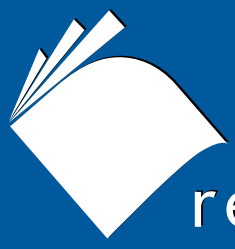


realtimepublishers.com™

The Definitive Guide™ To

Security Inside the Perimeter

Apani

Rebecca Herold

Introduction to Realtimepublishers

by Don Jones, Series Editor

For several years, now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Chapter 1: New Threats for the Same Security Issues

The need to secure information is a concern at the forefront of many executives' minds, and for good reason. Every day news reports document information security incidents that cost companies significant time and money to resolve, often at the expense of their brands and reputations:

- CardSystems Solutions Inc. is poised to go out of business as a direct consequence of a May 2005 security breach in which 40 million credit card numbers stored on their internal network were accessed by attackers who defeated the perimeter security. The company announced the breach May 22nd, and on July 19th, both Visa and American Express announced that they would no longer use CardSystems Solutions.
- An angry systems administrator—who alone developed and managed his company's network—centralized the software that supported the company's processes on a single server. He then coerced a coworker to give him the only backup tapes for the software. After the systems administrator was fired for inappropriate and abusive treatment of his coworkers, a logic bomb he had planted deleted the only remaining copy of the critical software from the company's server. The company estimated the cost of damage in excess of $10 million and as a result had to lay off 80 employees.
- The MyDoom worm made it past firewalls as an email attachment in January 2004. At the height of the outbreak, more than 100,000 occurrences of the worm were intercepted each hour. Cleverly disguised as an innocuous text file attachment, unsuspecting users opened the attachment and launched the worm inside their network perimeter. In 2004, MyDoom was estimated to have cost businesses $250 million (http://money.cnn.com/2004/01/28/technology/mydoom_costs/).
- An IT sector application developer who was downsized out of his job before the Christmas holiday launched an attack on his former employer's network 3 weeks after his termination using one of his former coworker's user ID and password to obtain remote access to the internal network. He modified many of the company's Web pages by modifying text and posting pornographic images, in addition to sending each of the company's customers an email message letting them know the Web site had been attacked. He also included within the message the customers' IDs and passwords for the Web site. A month and a half later, the developer attacked again through the remote connection, this time resetting all the network passwords and changing 4000 pricing records. He was sentenced to 5 months in prison, 2 years supervised probation, and ordered to pay his former employer $48,600 in restitution.

- An upset city government employee who did not get a promotion deleted files from office computers the day before the person who got the new position started. The subsequent investigation verified the disgruntled employee as being responsible for the incident. However, the city government officials did not agree with the police detective about whether all of the deleted files were recovered. No criminal charges were filed, and the employee was allowed to resign.

> 🕮 For more information, see the 2005 United States Secret Service and CERT Coordination Center/SEI Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors at http://www.cert.org/archive/pdf/insidercross051105.pdf.

Public attention has generally focused on preventing harm to networks by creating an impenetrable perimeter to keep unwanted outsiders at bay. Reality demonstrates, however, that the network is highly susceptible to threats that originate within the perimeter as well as threats that make it through a perimeter that is, in today's environment, highly vulnerable and porous and cannot feasibly be made impenetrable. Additionally, the human threats from trusted network users are increasing. For example, an authorized insider might be able to disable certain network security mechanisms to allow a collaborator on the outside to gain access. Alternatively, an insider might be able to transmit large volumes of sensitive information from inside the network to an outside destination without ever being discovered. Perimeter security has typically focused on keeping the bad things from entering the network—not preventing things from going out of the network.

Network Perimeters Are Now Like Sieves

The well-defined perimeter is disappearing, and your network is no longer like a steel fortress protecting against threats—instead it is like a stainless steel sieve. Mobile employees, wireless access, Web-based applications, remote workers, contractors, and business partners who have access to your network have put an end to the perimeter fortress. These factors can innocently or maliciously introduce attacks on the network and jeopardize confidential information and corporate assets. Attacks can come from anywhere at any time. There is no longer a well-defined perimeter.

Today, you need powerful, proactive security practices for all systems that connect to your internal network. New business demands and processes will continue to expand your perimeter, increasing the risks to your network. Without a plan to secure inside the perimeter, employee productivity, revenues, information, computing resources, and your company brand are highly susceptible to being greatly damaged. Internal security has become an obligation and a necessity. Customer confidence relies upon it, and worldwide laws and regulations require it.

Successful security requires the network to imbed security throughout the many network layers, applications, and associated devices as well as instilling effective security practices within the personnel who have trusted access to the network. Technology can be implemented to help discover when trusted network users are attempting to do damage. The time has come to pervasively secure inside the network perimeter.

Issues Are Nothing New, But the Threats Continue to Grow

Businesses have always faced numerous issues with regard to handling and protecting information. The primary issues have not changed much, but the number and types of threats created by computers and innovative technologies continue to grow. Threats to information include:

- Outsider fraud
- Insider fraud
- Employee abuse of trust
- Mistakes
- Poorly constructed applications
- Lack of due diligence resulting in protection gaps
- Lack of understanding and training
- Downsizing
- Outsourcing
- Natural causes (Earthquake, flooding, fire, and so on)

Outsider Fraud

Having swindlers try to defraud businesses is certainly nothing new; fraud has been around as long as history has been recorded. However, the techniques by which fraud now occurs is much more varied than ever before and takes advantage of new technology and human foibles. The Choicepoint fraud incident from February of 2005 is a perfect example. The fraudsters took advantage of technology to create identities based upon those of other legitimate persons, then took advantage of the vulnerabilities within the Choicepoint identity verification process to perpetrate a fraud against the company while compromising the security of 145,000 of the individuals within the Choicepoint databases. Phishing is another example of using technology (emails and Web sites) to commit fraud against people to whom bogus messages are sent.

Insider Fraud

The occurrences of employees with authorized access to network resources committing fraud are likely to continue to increase—although it's difficult to ascertain the current numbers for such crimes because they are under-reported to law enforcement and prosecutors (Source: National Research Council, Computer Science and Telecommunications Board, *Summary of Discussions at a Panning Meeting on Cyber-Security and the Insider Threat to Classified Information,* November 2000). Organizations are often reluctant to make such reports because of insufficient level of damage to warrant prosecution, a lack of evidence or insufficient information to prosecute, and concerns about negative publicity.

Employee Abuse of Trust

Employees with authorized levels of trust pose a great threat to the network when they become dissatisfied with their jobs or are otherwise motivated to take advantage of their extensive access capabilities and have a desire to cause damage on the network. Growing numbers of cases of disgruntled IT systems administrators modifying files and making business networks unusable have been reported.

Mistakes and Errors

Mistakes, errors, and omissions by insiders within the network perimeter are some of the most prevalent causes of information security problems. Accidentally sending email to the wrong person can lead to a loss of confidentiality if these messages are not protected, and loss of availability to the intended person. The most commonly cited example of this type of security breach is when an Eli Lilly employee accidentally sent an email to all Prozac users subscribing to a prescription service with all the names of the recipients clearly visible within the message heading.

Poorly Constructed Applications

A particularly common threat is through incorrectly configured or out of date security controls or exploitable software such as operating systems (OSs) and databases without up-to-date patches. Although these errors are usually accidental, programming errors can cause systems to crash. Application security cannot be delegated to the network administrator; it must be an integral characteristic of an application's overall architecture. A truly well-built application will inherently be secure. A poorly constructed application may be impossible to secure—effective security can't simply be tacked onto an application after it has been written. Application security must be addressed throughout the entire development process, not as an afterthought.

Lack of Due Diligence Resulting in Protection Gaps

Oftentimes in the rush to get a system or application into production, the implementation teams either inadequately test the security or assume someone else has performed testing for security issues. If errors or omissions are made during the software development, maintenance, or installation process, the integrity, reliability, confidentiality, and availability of the information processed could be threatened.

Using commercial off-the-shelf software does not guarantee error-free software. Hotmail had a bug that allowed anyone to read the accounts of their subscribers without a password. Microsoft Outlook and Outlook Express software had a bug that allowed malicious code to run on a computer without the knowledge of the user and cause Outlook and Outlook Express to fail. In addition, this bug allowed unauthorized individuals to utilize user access rights to reformat the disk drive, change data, or communicate with other external sites.

Lack of Understanding and Training

Many organizations do not adequately communicate their security policies and procedures to their personnel or train them for how to integrate security within their job activities. If personnel do not know how to properly implement security, they can easily perform activities in ways that put the network at risk. For example, if an employee does not know they need to secure the computer screen when away from the work area, an unauthorized person can access that system in the user's absence and commit fraud or maliciously delete or alter files—all under the authorized user's name.

Downsizing

After a company has reduced staff, it is common for people who have been laid off to be upset. Often they are given 2 weeks notice while retaining all the same rights to the network. When people know they will soon be unemployed, and are upset, they may maliciously use their access rights to wreak havoc on the network. For example, Omega Engineering suffered $10 million in losses after a network engineer, upset about being laid off, detonated a software time bomb that he had planted in the network he helped to build. The bomb made the Omega network unusable and brought the manufacturer of high-tech measurement and control devices used by the United States Navy and NASA to a standstill. When the bomb went off in the central file server that housed more than 1000 programs as well as the specifications for molds and templates, the server crashed, erasing and purging all programs. The incident resulted in 80 layoffs and the loss of several clients.

Outsourcing

The third parties to whom you give access to your network may not have the motivation or knowledge to adequately secure their activities. Also, if you connect an outsourced organization to your network, their security threats, vulnerabilities, and risks then become yours. You also risk having your information inappropriately used by employees who have no motivation to secure the information that comes from another company. For example, in 2005 a British newspaper, the Sun, reported purchasing credit card and other confidential details about hundreds of British citizens for just $5 each from an employee of an outsourcing organization in New Delhi.

Natural Causes

Environmental threats include natural disasters, such as floods, earthquakes, tornadoes and other environmental conditions. These threats result in the loss of availability of information that could lead to an inability to perform critical tasks, financial loss, legal liabilities, and even loss of public confidence or image. When these threats are coupled with inadequate physical security, there is also risk of loss of confidentiality of information.

Move Perimeter Concepts Inside

Organizations must focus on securing their internal network with the same vigilance that is applied at the perimeter. Organizations can apply similar information security techniques developed for the perimeter to their internal networks including the following:

- Defending against malicious code and worms and containing their spread
- Ensuring only safe devices and endpoints access the network
- Ensuring the privacy and integrity of data in motion
- Protecting critical applications from misuse and abuse
- Establishing an effective program for patching vulnerable systems
- Educating network users about how to apply security

Urgency to Address Old Problems with New Solutions

There is an increased urgency to address old problems with new solutions. Businesses have always had to face the problems of technology evolving faster than the associated security solutions. Keeping employees vigilant with their security practices as new computing devices become ever more mobile and affordable has been challenging business leaders since the introduction of the desktop computer. What used to work is no longer effective.

Financial Impacts Are Increasing

Security incidents are causing increasingly larger financial impacts. New destructive threats continue to emerge. For example, it is widely estimated that the Slammer worm alone caused more than US$1 billion in damage. Protecting against and containing worms is currently the most pervasive problem driving investment in internal security solutions. However, there are dozens of other problems that cause significant financial impact.

Vendor Communications Drive Security Exploits

Security vulnerabilities are now communicated much more proactively and quickly by vendors than ever before. As a result, the time from vulnerability announcement to active exploits has shrunk dramatically. It never seems as though the patches for security holes can be applied quickly enough. Businesses are continually trying to find new and better ways to protect their network resources while they are susceptible to the exploits until the software security patches can be applied.

Network Endpoints Are No Longer Managed Centrally

New types of technologies and devices are creating cavities within the network perimeter often without the notice of the organization. Organizations must realize that endpoint devices—such as personal computers, PDAs, Blackberries, and smart phones—must be secure on the networks as well as when they are connecting from outside the perimeter, such as through a VPN or wireless connection. If these endpoints are not secure, they can easily inadvertently introduce malicious code and other security threats to the organization.

Business Leaders Must Shift Their Security Approach

A June 2005 study inquired 140 top enterprise and government security executives about their approaches to network security and budget trends. This study revealed the need for tighter user access controls and continued concern about security threats and patching, even though the security budgets had increased in most of the organizations. Surprisingly, the study also found that more than half the respondents are still relying upon the perimeter as the primary way to protect the internal network, providing unmonitored access to the network resources once a user is authenticated. Sixty-two percent acknowledged that their organizations faced intrusions from internal sources that were authorized to be there.

It is essential that the network perimeter must be secured as much as possible. However, just relying upon perimeter security will not save organizations from costly security incidents, such as the attacks that have been widely reported against credit card processing centers and banks. There is an immediate need to make security a pervasive feature of all components of the network, inside and out. Access to the network must be pre-emptive as well as proactive and reactive.

Leaders Must Plan for Security Incident Response

It is also essential to plan ahead how an organization will react to internal security incidents and breaches. Many organizations are not prepared. The ways in which organizations respond to incidents and breaches typically fall into one of approaches:

- Locking down the affected sections of the network completely as soon as there is a significant security event
- Shutting down the entire network completely when an event occurs
- Turning on monitoring, quarantining, and blocking right away
- Reacting chaotically in an ad hoc manner with no clear direction or plan

Most organizations patch the perimeter and external servers much more quickly than the internal network resources. Because the resources are internal, most business leaders assume they can take much more time to apply the security patches because the perception is that the risks are much lower within the perimeter.

Leaders Must View Network Security Differently than in the Past

Organization leaders need to start thinking about network security from a perspective other than the old outside, perimeter, and internal way. Organizations need to take into consideration the following issues with regard to the components of their network:

- Which components are the high-value targets for an attack?
- Which components would have the most business impact if they were breached or made unavailable?
- What strategies should be used to efficiently and quickly respond to incidents?
- Is there information being stored or processed in inappropriate and insufficiently secured locations within the network?
- What human and managerial approaches should be used to defend against existing threats to all areas of the network?
- What changes in the security business model must be made to address the changes within technology that by their construct create new vulnerabilities, such as wireless, peer-to-peer, and mobile computing?
- Is the quality of the applications sufficient to help deflect attempted security breaches?

Information Security Market Immaturity Creates Challenges

Another challenging aspect of today's environments is that the information security market is still in its infancy. There are very few formal standards established for security products or services. Many vendors offer individual solutions such as firewalls that address only one type of security need. Organizations are challenged with making disparate and widely ranging types and qualities of security solutions work together, creating patchwork security across the enterprise. IT staff bears the daunting task of cobbling all these solutions together, constantly deploying an expanding list of products and spending inordinate amounts of time and money completing the integration work to ensure that these components are working together.

These immaturity issues create other significant challenges for IT staff:

- IT staff must absorb huge amounts of information to understand and manage the computing environment. Each product generates alarms, logs, and other information that they must review to determine whether something is wrong.
- The software industry places relatively low priority on security. Although some vendors garner a lot of press by announcing their concern and emphasis on security, most do not follow this example or go far enough with deploying security features. In fact, security is often sacrificed to make the software easier to use and less costly, resulting in growing numbers of vulnerabilities.
- Information security vendors will not offer mature solutions to adequately protect business any time soon. Businesses must develop strategies to mitigate risks for their own unique threats, risks, and vulnerabilities instead of depending upon a silver bullet solution to quickly provide resolution.

Scalability Issues

The nature of the internal network environment presents unique challenges when compared with perimeter security. Quite simply, when considering both, internal security requires significantly greater:

- Scale of the environment—Protection requires numerous networks, sub-networks and potentially thousands of systems.
- Scope of the environment—There are significantly greater, widely varying business applications and underlying protocols—not just HTTP, FTP, SMTP, and the handful of others associated with the DMZ.
- Numbers of users—The number of individuals and groups authorized to use the internal network is much more than with the external environment where there are typically very few defined groups with limited access privileges. Internally, the different roles can easily number in the hundreds or thousands, resulting in a much more complicated set of policies and controls.
- Speeds and volumes of traffic—Internet connections and associated DMZ resources rarely face more than 45Mbps, while internal networks and systems routinely operate at two to ten times that bandwidth. As a result, any controls that are implemented in the internal environment need to be capable of conducting the necessary inspections and dispositions at a much greater rate.

Table 1.1 compares the concerns of internal versus perimeter security.

Concern	Internal Security	Perimeter Security
Network Issues	Thousands of systems to protect	Small number of systems to protect
	Hundreds of thousands of Mbps of traffic to monitor	Tens of Mbps of traffic to monitor
Application Issues	Thousands of applications	A dozen or so applications
	Hundreds of thousands of protocols	Few protocols
	In-house applications	Standardized and well-defined applications
	Protocol compliance more lax	Strict adherence to protocols
	Client-to-client applications	Client-to-server applications
	Remote connections	
	Dependency on end users for many controls	
Management Issues	Hundreds to thousands of user and group roles	Few user and group roles
	Monitor the unknown or unusual	Block the unknown of unusual
	Decentralized coordination	Centralized coordination
Resource Issues	Large number of IT staff to support	Typically small IT support team
	Small ratio of security to network size budget	Large ratio of security to external IT components budget

Table 1.1: Internal vs. external security scalability.

Making Internal Security Scalable

How can an organization position network security solutions to accommodate change while not, or at least not noticeably, impacting network performance? What type of incremental cost for security must be accepted in order to adequately secure all components of the network according to their level of risk? Organizations need to consider the scalability issues involved with security when designing not only their security architecture but also their entire network infrastructure.

Let's look at a few examples of how architecture components within a business network impact the security scalability challenge.

Types of Routers

Most organizations buy the least expensive routers to meet their business and security needs of the moment. However, buying modular routers, even though more expensive up front, might be better than buying fixed-configuration routers because it is more efficient and easier to add and modify user and network interfaces, when needed, at a lower incremental cost. Security scalability is impacted by such issues as the type of router used, the size of the network, router configuration files, and the audit files generated.

Server Selection

Most organizations purchase servers to meet their current and existing business processing and security needs. Consider how well the server you choose will scale to handle your company's specific processes, such as online transaction processing (OLTP). It may be better in the long run to invest in a multi-processor-ready server even if you only need one processor for your current business. As your transaction load increases, you can then add more processors as necessary at a lower price. Security scalability is impacted by such issues as access control files and directory permission structures.

Network Design

Have you integrated all your organization's needs for voice, data, and high-speed dedicated Internet access across your network using an integrated service provider (ISP)? Determine whether the ISP is capable of adding bandwidth for both access and long-haul transport as your business needs change. Determine whether the ISP can support IP, Frame Relay, and ATM as required to meet performance objectives. Security scalability is impacted by such issues as firewall port configurations, instructions detection devices, audit files, and encryption configurations.

Zoning Helps Address Scalability Issues

Establishing enterprise-wide security zones helps to address the security scalability issues. Security zones not only support the effectiveness of layering security but also decreases the cost of enterprise technology infrastructure and create a scalable environment. Enterprise-wide security zones also support open architectures and encourage more collaboration and teamwork within and across the enterprise, addressing the management challenges of such collaborations. The significant movement toward embracing cooperation across organizations and sectors creates security problems. However, establishing security zones allows organizations to more successfully collaborate with one another while still protecting their valuable information resources.

Security Must Be Scalable as well as Support Business Goals

The challenge with creating scalable security architecture is building it effectively to allow the enterprise to function as it needs to meet business goals. The security solution must be scalable to give the organization what it needs for adequate security. Successfully scalable security solutions result from the security planners and implementers understanding both the business and the risk, threat, and vulnerability environments in detail. Many inefficient and rigid security solutions have been built because the organization did not consider the business and built the wrong security architecture.

The mix of security technologies used impacts scalability. Before implementing each separate security solution based solely upon the narrow scope of the task(s) it performs, you should ask some questions:

- What set of tools, technologies, and strategies comprise effective security practice for your specific organization?
- Is it possible to reduce this set of separate components into a set of business rules?
- Do these components support your existing security standards? Or, do you need to establish security standards?
- Is the technology you are considering mature? Is implementation or application within your environment going to be optimal compared with other technologies?
- What other security mechanisms are already deployed? How will the technologies under consideration interact with them? Will they conflict or enhance security?
- Is implementation of the security technology user friendly?

Business networks are often very limited in scalability because current tools are used with other tools that are not compatible, difficult to implement, a challenge to administer and maintain, and are poorly managed.

Multi-National Issues

Multi-national business drivers are prompting more focus on internal security than ever before, making security within the perimeter a priority. Companies must comply with world-wide regulations to ensure the privacy of their customer information as well as the security of the intellectual property that resides on internal networks. These global requirements drive an increased need for internal security.

There is also an increased awareness about malicious network attacks on internal networks that can be launched from anywhere in the world. Organizations in the past took an approach of not telling when incidents occurred to avoid the publicity and potential resulting negative business impact. However, now it is required by many international laws for organizations to provide proof that they are adequately protecting their entire network and the personal information stored within. This requirement is made even more significant as the number of internal attacks increases.

The Deloitte Touche Tohmatsu 2005 *Global Security Survey* shows internal attacks on information technology systems are surpassing external attacks at the world's largest institutions. The survey revealed that 35 percent of respondents confirmed attacks from inside their organization within the past 12 months, up from 14 percent in 2004.

There are many legal aspects to ensuring the security of information within the perimeter. Privacy and workplace surveillance issues need to be addressed when determining how, within an organization, to implement tools to decrease the possibility of insider malfeasance. Technology that produces data (audit logs, for example) that meet acceptable legal and forensic standards must also be addressed. In addition, monitoring and termination requirements for individuals suspected of internal network abuse or misuse must be addressed under the requirements of employment laws while also meeting the needs for systems security. Finally, sophisticated adversaries can take advantage of jurisdictional differences and route their attacks through non-cooperating jurisdictions. The jurisdictional challenges are complicated by the fact that under United States' law search warrants are geographical in nature. The restrictions on cross-border data flow impacts how a geographically dispersed world-wide network can share data among different network segments.

Controls Must Address International Requirements

International network controls must ensure that risks are reduced to an acceptable level by taking into account:

- Requirements and constraints of national and international legislation and regulations
- Organizational objectives
- Operational requirements and constraints
- Cost of implementation and operation in relation to the risks being reduced and remaining proportional to the organization's requirements and constraints
- The need to balance the investment in implementation and operation of controls against the harm likely to result from security failures.

Insider Attacks

Insider attacks might be difficult to prosecute in certain countries. For example, in Australia, an internal security breach occurs when an employee of a company uses the company's information system without authorization or uses it in such a way that exceeds his or her valid authorization. Consider a couple of related court cases:

- In the 1993 Victoria case *DPP v. Murdoch,* the defendant was prosecuted for computer trespass under the Summary Offences Act. The judge ruled that the relevant computer offense provisions of the act do not distinguish between persons who have no permission to enter a computer system and persons (such as employees) who have authority of some kind to enter the computer system, "If [an employee] has a general and unlimited permission to enter the system then no offense is proved. If however there are limits upon the permission given to him to enter that system, it will be necessary to ask was the entry within the scope of the permission? If it was, then no offense will be committed; if it was not, then he has entered the system without lawful authority to do so."
- In the 1995 New South Wales case of *Gilmour v. DPP,* the Supreme Court applied the above principle and held that an entry of data is made "without authority" when the employee is not authorized to make the particular entry, notwithstanding that the employee has general authority to gain access to the computer and make other entries.

Worldwide Legislation Spans Broad Areas

Because the Internet is easily accessible from any location in the world and most large organizations are now multi-national, it is important to understand and operate in compliance with worldwide regulations. Just a few examples of international legislation that is stricter with regard to data protection requirements than many United States laws include:

- The European Union Data Protection Directive
- Canada's Personal Information Protection and Electronic Documents Act
- Japan's Personal Information Protection Act
- Australia's Federal Privacy Act

An important consideration for business executives to remember is that laws and regulations are generally enacted on a country-by-country basis while electronic commerce is performed globally. As soon as your business uses the Internet to conduct business, you are doing business with the world. This consideration has the tremendous advantages of offering your products and services globally; however, you also need to comply with local regulations. These regulations are by no means consistent, and you could easily find yourself conflicting with one regulation by complying with another.

One major challenge with global electronic commerce and network sharing is that certain countries do not place a high priority on protection of personal information or intellectual property. They might have higher priority issues, such as food or medicine, and might be unwilling or unable to police individuals who are engaged in activities such as software piracy. Computer criminals typically operate freely in these countries without the fear of law enforcement agencies shutting down their operations. Unless business executives put strategies in place to protect their intellectual property and customer information, they run the risk of falling victim to these individuals.

Addressing Compliance Issues and Requirements

One example of a United States' Federal law is the Sarbanes-Oxley Act that went into effect in July 2002. It is intended to protect investors by improving the accuracy of corporate disclosures. All companies publicly traded in the United States must meet financial reporting and certification mandates for all financial statements. From an information security perspective, it is difficult to achieve compliance under Sarbanes-Oxley without having an effective information security program to protect your vital financial information.

- Adequate controls must be implemented to ensure that only authorized individuals are able to access this information.
- Change control processes must be in place to ensure that any changes to your financial systems are implemented in a controlled manner.
- A business resumption program must be in place to ensure that your organization can continue to operate in the event of a disaster.

Legislating State-Level Security

One example of state-level security legislation is California Senate Bill (SB) 1386, which went into effect in July 2003. It requires organizations that have customers or consumers in California to disclose any breach of security related to specific types of personal data, including Social Security numbers, drivers' license numbers, and account, credit, or debit card numbers. Security breaches include unauthorized access of computer data that compromises the confidentiality or integrity of that unencrypted personal information. Individuals who are affected by this breach of security must be notified. Most states now have pending similar legislation, and many have already signed similar bills into law.

Companies Need to Report Breaches

Public notification and reports to government of security breaches can be embarrassing to companies and can have a direct impact on their brand and revenue stream. However, penalties can be imposed on organizations that do not comply with the notification requirements. These regulations place additional importance on having an effective information security program, including comprehensive internal controls in place.

> ☞ With the growing number of e-commerce security incidents, the number of regulations will continue to increase. It is important to understand these laws and the restrictions that they can pose to your information security program. Successful business executives will develop strategies that turn these challenges into competitive advantages.

Businesses Must Be Prepared to Respond to Breaches

Organizations must have a plan for responding to such legal requirements for reporting and breach notification. They must also educate their employees about how to address such issues as well. Unfortunately, this communication does often not occur, although it is crucial, as evidenced by the 2005 E-Crime Watch survey conducted by *CSO Magazine* in cooperation with the United States Secret Service and the CERT Coordination Center, which reported "The respondents rated employee security training, education and awareness programs, and regular communication as the most effective strategies for deterring insider threats. These strategies create a culture of security in the organization, where all employees understand that security is a shared responsibility."

With more and more laws requiring breach notifications to impacted individuals, organizations must make it a priority now to plan on how to both identify when a breach has occurred and how the breach response will be handled. Organizations cannot simply hope that a breach will not happen to them.

> As of June 23, 2005 there were 12 states that passed breach notification laws (http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf), with another 20 states that were considering them. According to the ID Theft Center (http://www.idtheftcenter.org/breaches_0705.pdf), as of July 7, 2005 there had been at least 74 disclosed information security incidents within the United States alone in 2005, affecting more than 55.2 million people.

Business Is Impacted by Insiders Committing Security Breaches

Although an employee who commits an internal network attack will often face criminal prosecution, the organization might also end up being the subject of a civil lawsuit. A very significant danger exists to organizations regarding insider network security breaches committed by an employee who uses the organization's computer systems to commit electronic fraud or cause damage or loss to third parties. In these situations, it's possible that the company could be held liable for the acts of its employee. This risk is just one more of many reasons the network must be robustly secured within the perimeter.

All Security Incidents Impact Business

Many CEOs and CIOs are slow to invest in computer security because they do not think they will get a return on their investment. What they need to consider are the costs of *not* investing in computer security:

- The head of CardSystems Solutions, Inc., which was infiltrated by computer attackers exposing as many as 40 million credit card holders to possible fraud, told the United States Congress in July 2005 that the company is "facing imminent extinction" because of its disclosure of the breach and the industry's reaction to it. Visa USA and American Express announced after investigating the breach at CardSystems' Tucson, Arizona facility that they would no longer allow the firm to process transactions made with their cards.
- According to the Carlsbad, California research firm Computer Economics, the damage from Nimda is estimated at $635 million, while Code Red cost businesses a whopping $2.6 billion.
- In December, 1998 Ingram Micro, a PC wholesaler, had to shut down its main data center in Tucson, Arizona. Ingram's Internet business and electronic transactions were down from 8:00 AM to 4:00 PM. As a result of its one day of lost sales and system repairs, Ingram estimates that it lost a staggering $3.2 million (Salkeyer, Alex. "Who Pays When a Business Is Hacked?" Business Week Online: Daily Briefing, May 23, 2000. URL: http://www.businessweek.com/bwdaily/dnflash/dnfarch.htm). This figure is comparable to Forrester's projection that an auto manufacturer unable to get tires for a week would lose $21 million.

Security Breaches Are Expensive in Many Ways

The value of a security breach can be measured by both tangible and intangibles considerations. The tangibles can be calculated based on estimates of:

- Lost business as a result of unavailability of the breached information resources
- Lost business traced directly to lost customers
- Lost productivity of the non-IT staff who cannot work up to usual goals while the IT staff tries to contain and repair the breach
- Labor and material costs associated with the IT staff's detection, containment, repair, and reinstallation of the breached resources
- Labor costs of the IT staff and legal costs associated with collecting forensic evidence and prosecuting the attacker
- Public relations consulting costs to prepare statements for the press and answer customer questions
- Increases in insurance premiums
- Legal costs for defending the business in liability suits resulting from failure to deliver assured information and services
- Impact of breach disclosure on stock price

Intangibles refer to costs that are difficult to calculate because they are not directly measurable, but are still very important for business. Intangibles are often related to a loss of competitive edge that results from the breach. For example, a breach can affect an organization's competitive edge through:

- Customers' loss of trust in the organization
- Failure to win new customers because of the bad press associated with the breach
- Competitor's access to confidential or proprietary information

Forrester Research estimated the tangible and intangible costs of computer security breaches in three hypothetical situations (Howe, Carl; McCarthy, John C.; Buss, Tom; and Davis, Ashley. "The Forrester Report: Economics of Security", February, 1998). They found that if thieves illegally wired $1 million from an online bank, the cost impact to the bank would be $106 million. They estimated that if network compromises were used to prevent a week's worth of tires from being delivered to an auto manufacturer, the auto manufacturer would lose $21 million. They estimated that if a law firm lost significant confidential information, the impact would be close to $35 million.

Gumball Security No Longer Works

Historically, organizations have used the gumball approach to securing networks, making the perimeter like a hard outer impenetrable shell, while leaving the inside of the network soft and chewy with less vigorous security in place. Most organizations today still primarily use the gumball approach, protecting their networks from unauthorized access by implementing perimeter protection devices, such as screening routers and secure gateways.

The threat of attack comes from two major directions: attacks based outside the corporate network and attacks based from within.

The gumball approach, although at one time effective, no longer works. When the perimeter could be well defined, it addressed the "attack from without" scenario. However, the perimeter is now very porous, with mobile computing devices, wireless access, and peer-to-peer and business-to-customer network connections poking ever more holes into the once hard shell. Even if the perimeter was not so porous, such a model cannot address the attacks from within.

Existing perimeter security does not protect from an attack from within.

IT security administrators have long focused on securing the network perimeter. Focusing on the perimeter is indeed important. However, the internal networks must be secured with the same level of diligence to reduce the risks created from the sharp increase of worms and other attacks specifically introduced inside the network via mobile and wireless devices, in addition to attacks originating from trusted network users.

Although many of the same principles used to establish and implement perimeter security solutions also apply to internal networks, internal security is generally more complex, requires elevated performance, and has requirements completely unique from perimeter security.

Existing perimeter security solutions, such as patches, antivirus software, switch and router-based solutions, legacy firewalls, and intrusion detection and prevention systems, are inadequate for comprehensive security and leave huge gaps for securing internal systems.

Organizations must increase their efforts to improve the protection inside the walls of their organization. However, the struggle to balance decreasing budgets and personnel resources result in the persistence of reliance upon the gumball approach to securing networks.

Computer Evolution Has Changed Security Needs Greatly

In the late 1960s, networks only existed in the sense of huge mainframes and hundreds to thousands and millions of networked dumb terminals connected via hubs and concentrators to the huge central processing units (CPUs) in a central, air-conditioned, properly humidified windowless room. Network security was not really a significant issue. However, in 1973, business leaders started to take note when executives at the Equity Funding Insurance Company used computers to create 64,000 fake customers; a fraud that resulted in losses of two billion dollars, to commit what is widely still considered as the biggest computer crime that has yet occurred (Donn B. Parker, *Fighting Computer Crime*, pg. 65, Wiley, 1998). This incident illustrates the initial threats to network security, which at the time were strictly internal, but foreshadowed the nature of most threats to come. The environment for network security was evolving.

In 1969, the Defense Advanced Research Projects Agency (DARPA) along with four computer institutions started to design a network through which data could be passed and received. UCLA, the University of California at Santa Barbara, the University of Utah, and the SRI collaborated to create ARPAnet, which evolved to the Internet.

The 1980s introduced personal computers (PCs) and local area networks (LANs), laying the foundation for more network security threats than ever anticipated. The government addressed what they perceived as eminent security issues and created security guidelines published within *Trusted Computer Security Evaluation Criteria* that mainly dealt with security problems for standalone machines but not network security. In the fall of 1988, the Morris worm was launched, and all of the 60,000 computers on the Internet were crippled for two entire days.

Today Security Must Be Designed to Address Global Issues

Businesses typically design business infrastructure around network architectures. Global business requires networks that link multiple businesses together. The Internet has grown to connect easily more than two million computers on one massive and primarily uncontrolled network. Corporate networks are merging with the Internet to develop Internet businesses, Web-based business transactions, and much more. Consequently, the security matters are incredibly huge. Securing just the perimeter is not enough; internal security must be robust.

What is internal security? Internal security is a focused effort to appropriately secure all resources on internal networks. Examples of resources include applications, data, servers, and endpoint devices.

Internal security attacks can happen either maliciously or inadvertently. The impact of internal security events will have a negative result on an organization from both a technical and business perspective. Organizations must take the necessary steps to secure their internal networks, not just the perimeter.

Addressing Security Within the Perimeter

Attackers have new techniques for bypassing perimeter security barriers. This is often accomplished in many ways, a couple of which include:

- Tricking inside users and systems to execute code containing worms, which then spread to other systems behind the firewall.
- Tricking users of JavaScript and ActiveX to execute malicious code hidden in external Web sites.

These internal threats in many ways are more dangerous compared with external threats because they are difficult to detect and prevent.

What Are Internal Threats?

Network perimeter security mechanisms, although necessary and effective in stopping external attacks, cannot provide sufficient protection against all outside threats or internal threats. Several threat categories were described earlier—what specific types of threats are there to the internal network?

- **External email and Web browsing—**Attacking a user through email and Web browsing using a variety of security flaws in commonly used scripting languages. Users are often unaware when a script is being run because scripts can piggyback on most types of data files. Often, but certainly not always, such inside-out attacks rely upon a user performing an action such as opening an attachment. Attackers may create the malicious code themselves to ensure that it will not be detected by an antivirus tool.
- **External attacks using new vulnerabilities—**Attacking the software and servers that are visible from the Internet. The most recent attack might be used so that it will not be detected by intrusion detection systems. Attackers frequently target email servers, domain name servers, Web servers, routers, and computer security devices such as firewalls.
- **Application-layer exploits—**Examples include worms and blended threats such as Sasser, Blaster, Bugbear, Slammer, and SoBig. The majority of the SANS/FBI top 20 vulnerabilities to Internet security are categorized as application-layer weaknesses. Attacks against these vulnerabilities more easily bypass perimeter security, which is typically focused on the network layer.
- **Modem use—**Although not used as much as in the past, modems still create an entryway into networks and are still used as backdoors to the network.
- **Virtual private networking (VPN) technology—**VPNs are increasingly used to connect business partners, bringing with them all the security risks and vulnerabilities that exist on the business partners' networks.
- **Various user-friendly pervasively used computing technologies—**PDAs, Blackberries, laptops, wireless LANs, and other popular personal computing devices are often not adequately secured but create new pathways into the internal network.

- **Mobile and telecommuter solutions—**Such out-of-facility work arrangements have seen widespread and increasing deployment on the basis of reducing operational costs and improving employee satisfaction. However, establishing such remote work with connections to the internal network inherently puts the internal network at risk from the remote threats.
- **Code exploits—**Software flaws, noticeably buffer overflows, are often exploited to gain control of a computer or to cause it to operate in an unexpected manner. The code exploits often come in the form of Trojan horses, such as non-executable media files that are disguised to function in the application.
- **Eavesdropping—**Any data that is transmitted over a network is at some risk of being intercepted or even modified by an unauthorized network user.
- **Social engineering and human error—**Malicious individuals have often penetrated well-designed, technically secured computer systems by taking advantage of the carelessness or lack of knowledge of trusted individuals, or by deliberately deceiving them, for example by sending phishing type messages.
- **Denial of Service (DoS) attacks**. Although such attacks are not primarily a means to gain unauthorized access or control of a system, their design to overload the capabilities of a machine or network and make it unusable can have dramatic business impact.
- **Indirect attacks—**These are attacks launched from third-party computers that have been taken over remotely often referred to as "zombie computers." Such attacks make it very difficult to track the originator of the attack.
- **Backdoors—**These threats are typically programmed methods of bypassing normal authentication or giving remote access to a computer to someone who knows about the backdoor while remaining hidden to casual to others.
- **Direct access attacks—**Common consumer devices can be used to transfer data surreptitiously. When someone gains physical access to a computer, all manner of devices can be installed to compromise security, including OS modifications, software worms, keyboard loggers, and covert listening devices. The attacker can also easily download large quantities of data without notice onto storage devices, such as CDs, DVDs, USB keydrives, digital cameras, and digital audio players.

Identifying Internal Security Requirements

It is essential that an organization identify all security requirements in the context of how those requirements impact business with regard to existing risks, threats, vulnerabilities, and legal and contractual requirements. Alternative paths into organizations, along with application-layer attacks, are increasing the threats that emphasize the need to complement perimeter security with a comprehensive and pervasive range of internal security activities and tools. At a high level there are three main ways to identify security requirements inside the perimeter.

- Assess risks to the organization, taking into account the organization's overall business strategy and objectives. A risk assessment will identify threats to assets and network components and evaluate the vulnerability to and likelihood of occurrence.
- Identify legal, statutory, regulatory, and contractual requirements with which your organization, trading partners, contractors, and service providers must comply.
- Take into consideration the particular set of principles, objectives, and business requirements for information processing that your organization has developed, formally or otherwise, to support its operations.

Choosing Security to Address Internal Threats

Computer security solutions generally use prevention, detection, or response to address threats, reduce risks, and address existing vulnerabilities (see Figure 1.1).

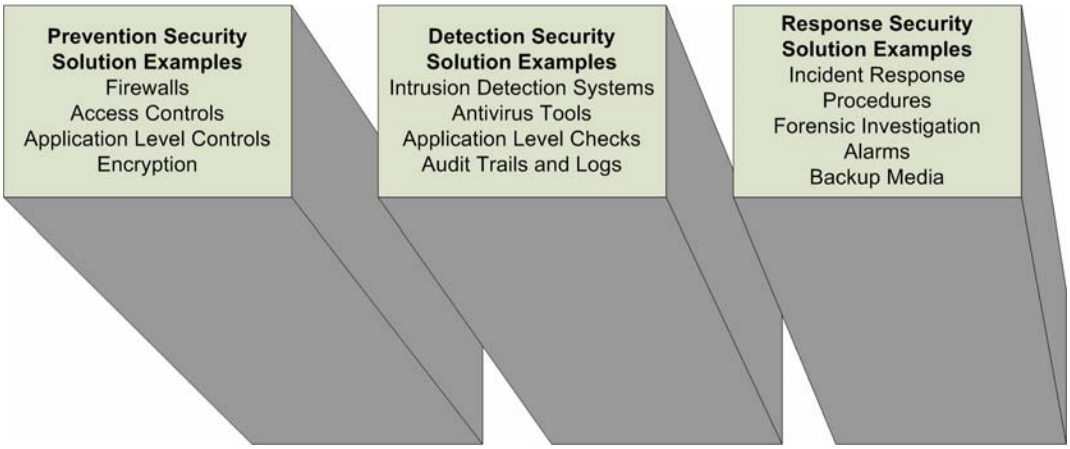
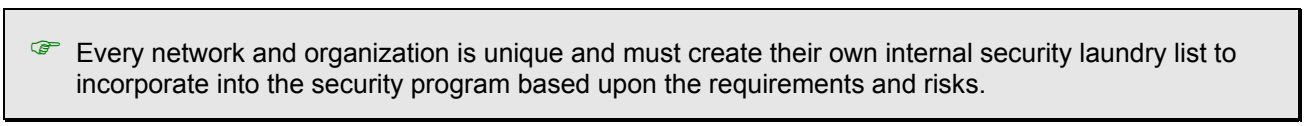


Figure 1.1: Example security measures.

The following is a laundry list of example actions that can be applied to address the security risks within the internal enterprise network:

- Maintain security on internal enterprise systems. Don't think that because the internal network is behind a firewall that it is implicitly safe. Keep up to date with security fixes for all systems.
- Protect critical infrastructure systems. Critical enterprise servers such as file servers, DNS servers, and antivirus systems must receive extra attention to keep them protected. Consider what would happen if your internal DNS servers became unavailable; would all of your applications also fail? Would you be able to access systems to perform remedial work?

- Use highly securable OSs for critical functions. If this is not possible, apply stringent security measures to harden the OSs you use.
- Don't allow all outgoing traffic through firewalls by default. As with incoming traffic, you should only allow those services that you need to go out.
- Run an intrusion detection system on your internal networks but don't rely on it to detect all problems. An intrusion detection system will help you identify the threats on your network but it won't protect your network by itself.
- Carefully use firewalls or other technologies to segment internal networks. Be sure you have considered the levels of protection and how much work it will take to maintain your segmentation. Be careful not to create a single point of failure within the internal network.
- Protect VPN endpoints with firewalls, and potentially with intrusion detection system monitoring as well. A VPN from outside should never terminate on an unprotected internal node.
- Utilize encryption inside the perimeter to protect confidential or sensitive information.
- Monitor to ensure system access is disabled completely and in a timely manner following an employee termination.
- Establish formal grievance procedures as an outlet for insider complaints.
- Create a reporting process when a colleague notices or suspects suspect behavior.
- Enforce comprehensive password policies and computer account management practices.
- Use configuration management practices to detect logic bombs and malicious code.
- Monitor system log activity.
- Establish and monitor procedural and technical controls for systems administrator and privileged system functions.
- Provide layered security for remote access.
- Monitor compliance with backup procedures and testing recovery processes.
- Ensure procedures are in place to disable temporary employee and contractor access as thoroughly as that of permanent employees.
- Establish security zones to help scale and manage security activities.



Summary

The assumptions used to improve the effectiveness of a perimeter-oriented security strategy can no longer be used to adequately secure the organizational network. This guide will look at the threats, risks, and vulnerabilities within the internal network and help you to identify the activities that will work best for your environment. To successfully manage these issues, executives need to understand and address the following seven significant challenges:

- E-commerce requirements
- Increased value of personally identifiable information (PII)
- Information security attacks
- Immature information security market
- Information security resourcing
- Government legislation and industry regulations
- Mobile workforce and wireless computing

This chapter discussion demonstrates there are many different security issues involved with securing the network, and they are generally unchanged from the past. However, the number and types of threats continue to grow dramatically. The network perimeter has become so porous it is a bad business decision to depend solely, or even primarily, upon perimeter security to protect your internal network resources and assets. There are many compelling factors to consider that will convince you of the need to secure your network throughout the enterprise and not just at the perimeter. This chapter highlighted these factors at a high level. The next chapter discusses these factors in depth.

Chapter 2: Factors Working Against Securing Just the Perimeter

Tribal thinking has existed for centuries within many different cultures in which members of a group, or tribe, were completely trusted to do what is right and good and those who were not members of the tribe were not trusted. There is a long history of organizations also trusting all their own members. Historically, organizations believed that trusting employees implicitly led to loyalty and better productivity. In fact, a study published by NFI in 2003 (http://www.nfiresearch.com/subpage/release/EmpLoyalty.html) stressed increasing trust, stating, "It isn't the monetary rewards that build loyalty—it is the feeling of adding value, making a contribution and being trusted that matter most in building an organization of loyal employees." This idea certainly reflects tribal thinking.

Tribal Thinking Must Change

According to the United States Department of Labor (http://www.bls.gov/news.release/tenure.nr0.htm), the median number of years that wage and salary workers had been with their current employer was 4.0 years in January 2004, and in January 1983 it was 3.5 years. Thus, the retention of employees in all industries has changed little in two decades. However, if you look at the statistics of employees who are actively searching for a new employer while with their current employer, you get a different view. A May 1976 Bureau of Labor Statistics survey (http://www.bls.gov/opub/mlr/2000/09/art1full.pdf) showed that 4.2 percent of all workers who had been at their jobs at least 4 weeks were interested in changing jobs. A 2005 survey conducted by the Society for Human Resource Management and CareerJournal.com reported that 81 percent of today's employees are interested in changing jobs within the next 12 months. This statistic seems to indicate that your corporate tribal members are loyal only until something better comes along.

Trust Where Trust Makes Sense

Trying to retain good employees certainly is necessary, but organizations must realize that the trust they impart upon their employees needs to have certain limits. Not only are security measures necessary to help protect against the malicious activities of those employees who cannot be trusted, such security measures are also necessary to help protect against the mistakes and lack of knowledge of well-meaning employees that could lead to business-closing incidents. This instinct of trusting everyone that is a part of your team, organization, or tribe, must be tempered with good business practice and establishment of due care processes.

Some of the most trusted positions within an organization are within the IT areas. Security administrators hold rein over your network. Making sure these folks are appropriately monitored, have appropriate controls applied, and receive adequate training is a demonstration of due care that your organization must take the time to implement. Although the vast majority of IT staff will do the right thing, there are still those that could be tempted to abuse their powerful capabilities and do wrong.

In August 2005 the Helsinki, Finland branch of global financing company GE Money had police investigate the theft in June of about €200,000 ($245,400). The police reported they believe the company's head of data security stole the money using banking software from the company along with passwords for its bank account. Accomplices then accessed the account from a laptop computer using an unprotected WiFi network at a nearby apartment building. Investigation revealed the laptop's MAC address (the unique identifier on the network card) belonged to GE Money, and the bank's security officer was soon implicated.

Preventing Crime by Insiders Is Difficult

It is difficult for companies to guard against crimes in which internal staff is involved, making it even more important to implement security measures internally. There are few reported incidents of computer crimes committed by insiders, but that definitely does not mean that there are few crimes that are actually committed.

In July 2004, Scotland Yard's Computer Crime Unit reported UK businesses typically only report 5 to 7 percent of all computer-based crimes to the police. "Around 93 to 95 percent of all cybercrimes go unreported because companies rate unwanted publicity as potentially more damaging to their business than the incident itself."

It is likely many of these unreported crimes are committed inside the network. It is also likely that many crimes go undetected.

New Technologies Make It Increasingly Difficult to Secure Networks

There has been an explosion in the creation of new technologies in the past decade that make it very easy to link networks. Staff members who do not realize the threats they present use new technologies widely inside the network, often without the knowledge of management. The availability of inexpensive technologies can be easily accessed by large numbers of people, employees, and outsiders alike. More and more employees are moving their business work to their home computers. Of course, this move can provide tremendous benefits to businesses. However, by increasingly putting powerful computing devices into the hands, and control of, employees, the businesses inevitably become more vulnerable to unauthorized network intrusion and abuse.

Consider What Insiders Can Do

So how vulnerable are businesses to the activities of their own tribe members? Considering virtually any computer system is susceptible to unauthorized intrusion, very vulnerable. Just consider a few of the types of authorized activities an insider can typically perform:

- Open the door of a computer room
- Dial into a computer network
- Obtain access to a direct-wired terminal
- Send email messages
- Supply or write a software program for a computer system
- Perform a computer maintenance or repair service

Your internal tribal members can do any number activities by exploiting their authority to wreak havoc on your network:

- Tamper with any service residing within the system
- Interfere with the work of systems administrators and operators
- Deny access to legitimate users
- Add false information
- Read, copy, or erase programs and data
- Enter other computer systems
- Change system instructions and protocols
- Introduce disruptive programs and applications

It only takes one person to corrupt a corporation's information network. Are you comfortable believing that 100 percent of your tribe members will always do the right thing?

Employees Have Wide Access Because they Are Employees

Employees, simply by virtue of their status as employees, enjoy wider access to a company's information assets and information equipment than outsiders do. Many, if not most, employees are now savvy computer users and, if they wanted, are better positioned to insert malicious code into a network than are hackers. They are also more able to steal passwords than any industrial spy. In fact, when it comes to leaking, copying, reading, stealing, altering or deleting information, employees participate in these activities far more than any external intruder.

Employees Often Breach Security

Why do employees want to deliberately fiddle with their organization's information? For many reasons, including greed, anger, frustration, and revenge, just to name a few. There are also hundreds of unintentional security lapses committed by employees daily as a result of carelessness, gullibility, and ignorance. Employee access to information is the greatest threat and greatest challenge to securing an organization's information infrastructure.

Employees Need Security Understanding

Organizations must instill a security mentality into their tribe members. This goal can only be successfully accomplished through careful planning and implementation. Such an awareness and training program must encourage employees to identify the need for information security and to willingly accept and follow the security controls and procedures in place. Such a program must implement constant communication, consistent reinforcement, audits for compliance, and investigations into non-compliance.

Trust is vital for successful business; it is also vital as part of the security equation. Security technology, controls and procedures are definitely essential in protecting information. Ultimately, however, the employees are critical to ensuring security.

If you explain clearly, consistently, and often to employees why security measures are established most will still feel trusted and understand the reasons why such measures are necessary. In fact, you *must* communicate that you trust your employees—this idea is a vital human factor in employee job satisfaction. However, letting employees know that they are trusted doesn't diminish the need to establish internal security controls—there are too many compelling reasons to do so, such as establishing accountability and to meet regulatory requirements.

Recent Studies Examine Insider Threats

In May 2005, the United States Secret Service in partnership with the CERT Coordination Center, located at Carnegie Mellon University's Software Engineering Institute, released their most recent Insider Threat Study (ITS—http://www.cert.org/insider_threat/insidercross.html). This study analyzed incidents from a behavioral and a technical viewpoint. The ITS examined incidents committed by insiders, defined as current or former employees or contractors, who intentionally misused their network access authorization in such a way that they impacted the organization's business operations, data, or networks. The 2005 ITS analyzed 49 insider incidents in which the insider's primary goal was to "sabotage some aspect of the organization (for example, business operations, information/data files, system/network, and/or reputation) or direct specific harm towards an individual."

The ITS revealed the majority of the insiders who committed acts of sabotage were former employees who had held technical positions with the targeted organizations. Almost all the insiders examined were charged with criminal offenses. Most of the charges were for violations of United States federal law.

The key findings of the ITS are the following:

- A negative work-related event triggered most insiders' actions.
- Most of the insiders had acted out in a concerning manner in the workplace.
- The majority of insiders planned their activities in advance.
- When hired, the majority of insiders were granted systems administrator or privileged access, but less than half of all the insiders had authorized access at the time of the incident.
- Insiders used unsophisticated methods for exploiting systemic vulnerabilities in applications, processes, and/or procedures, but relatively sophisticated attack tools were also employed.
- The majority of insiders compromised computer accounts, created unauthorized backdoor accounts, or used shared accounts in their attacks.
- Remote access was used to carry out the majority of the attacks.
- The majority of the insider attacks were detected only once there was a noticeable irregularity in the information system or a system became unavailable.
- Insider activities caused organizations financial losses, negative impacts to their business operations, and damage to their reputations.

These findings are corroborated by the findings of the 2004 Ernst & Young study (http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf) that indicates the damage from insiders is much greater than from outside the network. Most damage is from misconduct, omissions, oversights, or violating policies and procedures. The study reported one in five employees reported "personal awareness of other individuals stealing from the employer."

Many insider incidents are never discovered by organizations, so they are unaware that they are even being victimized.

Fraud Impacts Virtually Every Organization

The 1997 President's Commission on Critical Infrastructure Protection report (http://www.cert.org/pres_comm/cert.rpcci.abstract.html) reveals some primary issues related to the insider threat:

- Insider problems exist within the critical infrastructure, including the military, telecommunications, and energy sectors.
- There is a tendency for managers to settle insider problems quickly and quietly, avoiding adverse personal and organizational impacts and publicity. Because of this handling method, we cannot really determine how widespread the problems are. What actually gets reported is likely only the tip of the iceberg.
- Organizations are at risk from repeat offenders. As computer criminals migrate from job to job, typically without background checks and with constraints upon employers in providing references, no significant consequences result from their offenses.
- The range of potential perpetrators and their motivations is broad. Disgruntled employees who are angry about layoffs, transfers, and other alleged grievances have committed computer sabotage and extortion. Other cases involve employees who take advantage of their position of trust for financial gain, attackers who are employed within the critical infrastructure caught engaging in unauthorized explorations, and "well-motivated" employees who claim they are acting in the best interest of their organizations. Other perpetrators include *moles*, individuals who enter an organization with the explicit intent to commit espionage, fraud, or embezzlement. Overall, case investigators report that the number of computer-related offenses committed by insiders is rising rapidly each year.

The Association of Certified Fraud Examiners (ACFE—http://www.cfenet.com/pdfs/2004RttN.pdf) estimates that the typical United States organization loses 6 percent of its annual revenues to occupational fraud; in other words, fraud instigated by insiders. Using the United States Gross Domestic Product for 2003, this statistic amounts to roughly $660 billion in total losses.

Multiple other studies have examined various aspects of the impact of insider acts on businesses:

- In the 1996 WarRoom Research *Information Systems Security Survey*, 62.9 percent of the companies surveyed reported insider misuse of their organization's computer systems.
- The Computer Security Institute and FBI (CSI/FBI) 1995 *Computer Crime Survey* reported the average cost of an insider attack was $2.7 million. The 2005 CSI/FBI Survey reported that the average cost of an insider misusing the Internet was almost $6.9 million.
- A study conducted by the United Nations Commission on Crime and Criminal Justice surveyed 3000 sites in Canada, Europe, and the United States, and found that "By far, the greatest security threat came from employees or other people with access to the computers."
- An April 2000 study about the insider threat to Department of Defense (DoD) systems by the United States Office of the Assistant Secretary of Defense reports for one set of investigations that 87 percent of identified intruders into DoD information systems were either employees or others internal to the organization. Of 1004 criminal investigations associated with DoD information systems "87 percent were either employees or others internal to the organization."

The Perimeter is Porous

An explosion in outsourcing, mobile computing, wireless networking, business partner connections, and Web-based applications has created a spider web configuration of connections to virtually anyone, from anywhere, with any device. Perimeter-based security is no longer sufficient. It fails because there is no longer a clearly defined perimeter. With the large numbers of individuals with access to business networks who are not employees, it's difficult to determine who should have access to network resources and who needs to be blocked. Your "trusted" internal network environment is now likely connected directly to the Internet through a home or partner link or through an unapproved wireless connection.

The typical network perimeter is no longer like a steel fortress protecting against threats, instead it is like a stainless steel sieve.

Business to Business Connections

Most organizations now have business to business (B2B) relationships with business partners in which the partners' networks are connected through a variety of methods. Such relationships certainly enable efficient business communications and processing (such as supply chain management, lead-time reduction, and other business process automation) by transmitting transactions through these connections. B2B can also automate transmissions to reduce the level of human interaction that used to be necessary to achieve these benefits and efficiencies.

EDI Was the Forerunner of Partner Connections

Not long ago, organizations used Electronic Data Interchange (EDI) as the primary way to share information with their business partners. Of course, EDI is still used widely today. However, because of the complexity and costs involved with EDI systems and software, many companies used EDI only to share information with a small percentage of their partners. Most business partners do not need such complex systems to share information, so simpler, less-expensive solutions are implemented that leverages the ability to share information over the Internet, or to connect the trading partners directly to a company's network. A large amount of sensitive and competitive information is typically transmitted through B2B relationships, so security is a major concern. Not only the security of the transmissions but also the vulnerabilities that the multiple and varied connections present to the organization's network.

B2B Connections Are Typically Inconsistently Managed

B2B connection implementations often fall through the cracks with regard to consistently having one group to manage and monitor the connection. Sometimes the IT group may be responsible for doing something minor for the connection, such as opening a port on the firewall to enable communication between the business partners. Sometimes the business partner handles the bulk of the connectivity. In yet other cases, the business unit takes it upon themselves to make the connection without the assistance, oversight, or authorization of the appropriate IT area. Support issues are often handled ad hoc. All these ambiguities can lead to unsecured pathways into your network. Regardless of how the connections are made, your company is still ultimately responsible for ensuring the security of the company network.

B2B Connections Create Holes in the Perimeter

B2B connections can create an unbelievable number of holes into your network, providing compelling motivation to implement security at more than just the perimeter. The following sections explore some of these potential holes.

Lack of Security Policy Creates Security Holes

Often a good security policy does not exist to govern B2B connections. Without such a policy, personnel responsible for these relationships will not know the security requirements with which they must comply. There is also no accountability for personnel who create B2B connections if there is no policy. You need to have a security policy that outlines the minimum security requirements for each B2B relationship with your organization. The policy should outline security requirements related to architecture, transaction processing, monitoring, and the groups that must be involved from initial discussions to actual implementation and monitoring.

Lack of Due Diligence Creates Security Holes

Due care activities need to occur to ensure B2B connections and information exchanges are secured. If information security is not involved in the due diligence process, the business partner might not have adequate measures to secure the B2B transactions. If the business partner will access your company's data or systems, significant security concerns exist related to confidentiality and integrity of information. To mitigate this risk, information security must participate in due diligence activities to validate and confirm security specifications and requirements prior to signing the final agreement.

Lack of Audits Creates Security Holes

Audits need to be performed on B2B connections to find vulnerabilities and prevent unauthorized access to your information. If internal audit is not involved when forming a B2B relationship, the final B2B infrastructure may not meet your organization's audit and control requirements, including regulatory requirements. Internal audit should be involved in the B2B process from start to finish to help ensure that your organization's audit and control requirements are met.

Lacking Security in Partner Connections Creates Security Holes

Connections may be made with business partners when they are not needed, or may be made in ways that do not support the corresponding business process. It is important to understand the business process any connection to your network is supporting, along with the criticality of the process. Is the purpose just to share information or to perform business transactions? Considering such issues will help determine the appropriate way in which to make and secure the connections.

Lack of Assigned Responsibility Creates Security Holes

If no one officially owns the B2B relationship management activities, it is likely such partnerships are not managed appropriately, and no accountability will exist to ensure contract requirements are met. Once your organization has signed a B2B agreement, someone needs the ownership of that relationship. This role needs to ensure that the requirements are met (including security requirements), act as a single point of contact with the partner, and work with appropriate groups within your organization to manage the relationship.

Lack of Service Level Agreements Creates Security Holes

Without a Service Level Agreement (SLA), the partner may not be accountable for service levels required by your organization. Your organization's information may not receive an appropriate level of security, and may potentially be accessed on your network through the holes in the partner's network. An SLA obligates the partner to meet your security requirements. It should outline the scope of your organization's relationship with the partner, roles and responsibilities, performance metrics, and so on. Penalties should be incurred for being non-compliant with the SLA.

Some security-related issues to address within SLAs to help prevent incidents from occurring within the perimeter as a result of your relationship with the partner include:

- Allowable downtime
- Documented and tested disaster recovery plans
- Incident handling procedures and associated escalation lists
- Notification requirements for security incidents and information breaches
- Backup and recovery requirements for data
- Financial and non-financial penalties for SLA non-compliance
- Auditing provisions, including timing, notification, frequency, and so on
- Security requirements for the hardware and software used with the B2B connections, including such specifications as patch management and hardening standards
- Documented encryption requirements and standards

Lack of SLA Monitoring Creates Security Holes

If SLAs are not monitored, your organization's data may not be properly secured because the partner may not be meeting your SLA requirements. The person who owns the B2B relationship responsibility should also work with the appropriate areas in your organization to monitor the provisions of the SLAs.

Lack of Secure Information Exchange Creates Security Holes

If you are exchanging sensitive information that is not properly secured, it could be compromised and get into the wrong hands, and possibly result in detrimental impact not only to your organization, but also to your customers. Be sure to analyze and approve architectures for all planned partner connections. Important issues to address include, but are not limited to:

- Encrypting information during transmission
- Using digital certificates
- Establishing reasonable authentication measures

Lack of Network Traffic Analysis Creates Security Holes

If you do not establish security measures to ensure information coming from the partner network is valid and authorized, there is great risk of unauthorized access to your organization information and network. When your partner sends information to your organization, your partner must communicate with at least one or more of your systems. Your security considerations for these transmissions will vary based upon your organization, your partner, and the purpose of the transmission.

Lack of Business Partner Security Creates Security Holes

There is a wide spectrum of risks related to your business partner not having adequate security. They can range from minor impacts due to operations all the way to huge fines and penalties resulting form non-compliance with applicable regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and many others. Incidents on your partner networks could have significant impact to your organization's reputation, availability, and financial success (or failure).

Lack of Adequate Access Controls Creates Security Holes

Risks related to inadequate access control measures can have significant impact on the confidentiality of your data, potentially resulting in financial and/or reputation damage. Your partners should provide access to data and applications based upon a business need and as it relates to the kind of relationship and contract you have with the partner. Be very careful about providing blanket access to everyone within the partner organization or by having identifiers for your system shared by multiple business partner personnel; this setup results in lost individual accountability.

Lack of Employee Termination Procedures Creates Security Holes

Terminated partner employees could still have access to your organization's data and systems. They could wreak havoc on your network, making it inaccessible for business processing, surreptitiously take data from your network and give or sell to your competitors, or try to ransom it to your organization. When your partner employees are terminated, all their access to your organization should be removed. This is another good reason to not use group identifiers—it increases the likelihood terminated employees who used such an identifier will still have access to your systems.

Lack of Identifier Clean-Up Creates Security Holes

If you do not purge identifiers, individuals who no longer need access, including terminated employees, may still have access to the B2B applications and your networks. You should establish a procedure to periodically purge all identifiers from your systems that have not been used for a specific period of time, in addition to reviewing identifiers to determine whether they are still necessary, even if they have been used recently.

Business to Consumer Connections

Business to consumer (B2C) connections are those by which consumers purchase goods or services over the Internet, or some other public connection, from your company, or otherwise communicate or share information with you. Until recently, many organizations put up a Web site with information about their products and services so that consumers could learn about the company's offerings. However, organizations now overwhelmingly make services and products available for purchase, in addition to giving customers access to their account information, through public networks. Consumers use such connections extensively because of the convenience and often lower prices. However, many consumers still avoid making online purchases or accessing their account information through the Internet because of security concerns and the recent reports of identity theft, insufficient security on Web sites, reported attacker exploits, and concerns that Web sites are not legitimate. Such concerns are understandable.

If you have customers who look at your online catalogs, make purchases from your Web site, and supply information such as their name and address, they are participating in a B2C communication with your organization.

B2C connections create entry paths to your organization's systems and data.

Security risks related to B2C connections include:

- Unsecured transmission of customer information
- Unsecured storage of customer information
- Inadequate transaction integrity and legitimacy
- Insufficient security of the architecture supporting the B2C connections, such as the Web servers and the back-end systems
- Unavailability of the B2C systems components

The risks created by B2C connections could significantly impact your organization. B2C connections create a variety of pathways into your systems. Some of the potential impacts to your organization from a B2C connection security incident include:

- Your business operations could be delayed or even completely shut down through a Denial of Service (DoS) attack.
- If your customer information is stolen, your organization could face legal penalties, fines, and civil suits.
- Security and availability issues for your network can have immediate and significant financial impact on your organization. If your customers cannot make purchases, you lose money.
- If a breach occurs through a B2C connection, or any connection for that matter, and the incident is publicized, it will likely damage your organization's brand and reputation. The degree of damage will depend upon the nature of the incident and the severity.

B2C connections can create huge risks and an unbelievable number of holes into your network. The following sections explore some of the ways these risks and unsecured connections occur, providing still more persuasive reason to secure inside the perimeter.

Lack of B2C Security Policy Creates Security Holes

Without a policy to govern B2C processes, B2C architecture and applications will likely be developed with inadequate security. Trying to add security onto architecture and applications after deployment can be expensive and take much more time than if it was built in right from the start. Additionally, a policy provides a mechanism for enforcing effective B2C security practices.

Lack of B2C Knowledge Creates Security Holes

If organizations do not know the financial and brand impact of B2C connections, they will likely not plan appropriately to ensure the connections have the appropriate level of availability. Organizations need to determine the percentage of overall revenues the B2C connections generate as well as whether the Web site providing the B2C connection has had a security breach that would impact the organization financially or its brand.

Lack of Security Breach Documentation Creates Security Holes

If you do not know about past security breaches through B2C systems and how they impacted your organization, you cannot know how to prevent the same breach from occurring again. Knowing about past security incidents and how they were handled will help to implement measures to prevent them from happening again.

Lack of B2C Accountability Creates Security Holes

If no one owns the B2C connections responsibilities, there is no accountability—a dangerous situation for a revenue-generating activity. Lost or corrupted B2C connections have a significant impact, including lost revenue and lost customers. Ownership of the B2C connections must be established so that all associated activities can be consistently managed. Such a role should ensure updates occur, the content is appropriate, the network architecture for the connections is appropriate, and that customer Web sites are available, functioning appropriately, and are secured.

Lack of Database Ownership Creates Security Holes

If no one has documented ownership of the databases supporting the B2C operations, it's likely they will not be properly secured, resulting in unauthorized access and potential data integrity compromises. B2C databases are critical to the B2C infrastructure, and typically contain very sensitive and confidential information that falls under potentially multiple regulatory requirements for protection. This information must be adequately secured.

Lack of Access Restrictions Creates Security Holes

Without strict access controls on the B2C databases, unauthorized access to sensitive information in the database can occur or the integrity of the database could be damaged. Access to the database should be limited to only those who need it to perform their job responsibilities.

Lack of Due Diligence Creates Security Holes

If due diligence is not performed to ensure proper security of B2C processes, the application may not have the necessary security features. As a result, there could be unauthorized access to the application transactions or integrity loss to the B2C data. When purchasing a Commercial Off the Shelf (COTS) application, security is often overlooked. It is important to review the application package and consider access control capabilities, information flow with other applications and systems, and other security-related issues unique to the application.

Lack of Security for In-House Developed B2C Applications Creates Security Holes

If security is not built in from the beginning, there is a risk the application will not adequately ensure the integrity and confidentiality of the data. The costs associated with additional development and re-engineering of the processes when trying to add security as an after-thought could be significant. Implement policies and procedures to require security as part of the systems development and modification process. Consider automated tools to help developers build security into applications during the development process.

Lack of Web Server Security Creates Security Holes

If the Web server is not hardened or patched, vulnerabilities could be exploited to attack the B2C application. This attack could lead to Web site unavailability, defacement, access to internal systems, and so on, resulting in lost revenues, customers, reputation damage, confidential data breaches, and other significant business-impacting incidents. Best practices for hardening Web servers can be found on the corresponding vendor Web sites as well as on information security Web sites. Procedures should be implemented to perform hardening and patching activities on an ongoing basis.

Lack of Alerts Creates Security Holes

Without an intrusion management system in place, potential attacks could go unnoticed until after significant and potentially irreversible damage occurs. This could lead to lost revenue, lost customers, and damaged reputation and brand. Procedures must be in place to detect when something inappropriate is happening at the B2C Web sites. Consider using intrusion management systems, which can help detect potential attacks on a 24×7 basis. Some such systems also have the ability to stop certain types of attacks.

Lack of Segregation Creates Security Holes

If the B2C database and application sit on the same server, and the server is compromised or attacked, both the database and application could be compromised, resulting in customer and other sensitive information being exposed, permanently lost, or stolen. This risk is much greater if the application and database actually reside on the Web site server. To reduce risk, the application and database should not reside on the Web site server, but each on two separate servers behind your organization's firewall. Of course, the front end of the application will need to sit on the Web site server, but non-customer-facing functions of the application should sit in another network segment behind the firewall.

Lack of Firewalls Creates Security Holes

The lack of firewall, or an incorrectly placed or configured firewall, could result in unauthorized traffic into your organization's network. Oftentimes, the firewall is the only security feature of a B2C application. Implement policies and procedures to require firewalls to be used for every B2C application, and document the minimum requirements for establishing the firewall rules based upon the activities of the B2C application.

Lack of Cache Clearing Creates Security Holes

If sensitive B2C information is cached, another person could potentially log on to public computers or kiosks as the preceding person, leading to fraudulent activity. Client software should not allow authentication data, or other confidential data, to be cached. Additionally, cookies should not contain confidential information and should expire upon session termination.

Lack of Proper Logout Creates Security Holes

If an application does not logout properly, individuals could obtain unauthorized access to each other's accounts. Such is especially a risk in public places such as at kiosks or on public computers such as in libraries or in Internet cafes. Each B2C application should have a logout function to allow users to logout out of the application completely and disallow others using the computer from using an active session.

Lack of Secure Protocol Creates Security Holes

When information is sent in clear text across the Internet, it can be intercepted and used to gain unauthorized access to other accounts without any trace that this activity even occurred, let alone who captured the information. All sensitive information should be sent using secure protocols that encrypt sensitive information.

Lack of Password Masking Creates Security Holes

If they are not masked, the B2C passwords could be seen by others nearby and used to subsequently logon as another person, leading to fraudulent activity, loss of customer trust, and brand damage, not to mention potential regulatory non-compliance and resulting fines, penalties, and potential civil suits. All passwords should be masked on the end user's screen whenever they are typed.

Lack of Strong Passwords Creates Security Holes

Weak passwords can easily be exploited to gain unauthorized access to the B2C application as well as to customer account information. The B2C application must force users to create strong passwords and provide ways for legitimate, identity-validated customers to obtain or change their passwords if they forget them.

Lack of Logon Security Creates Security Holes

Without a lockout feature, malicious users could use brute force methods to gain unauthorized access to B2C applications and customer information. A lockout feature will help to prevent this from happening. The account should be locked until the account user contacts your company to reset the account, or otherwise provides valid proof of identity to unlock the account.

Lack of Identity Verification Creates Security Holes

If customer identity is not properly authenticated prior to resetting passwords and providing other account information, an unauthorized person could obtain this information then use it to gain access to the valid customer's account. Password resets should be performed only after following a consistent procedure to verify the customer's identity. Such procedures should also apply to responding to customers' requests for information about their accounts.

Lack of Administrator-Level Controls Creates Security Holes

If you do not limit administrator or root access to only those few who need it to administer the Web server, accidental or malicious damage to the Web site is a possibility. This is a significant risk if disgruntled employees have access. Administrator access to the Web server allows full access rights; an administrator can make any change or see anything stored on the Web server. Ideally, only one person should have this access as a primary responsibility, with another person serving as a backup. The person performing administrator activities should have a different personal account they use for all other activities that are not related to Web server administration.

Lack of Change Management Processes Creates Security Holes

Applications built in-house must go through a formal change management process before being put into production. Without formal change management procedures, vulnerabilities can be introduced to the B2C application as a result of inadequate testing and quality assurance. Vulnerabilities can lead to unauthorized use of the application or other types of security breaches. Formally documented change management procedures must be followed for all B2C applications, including those built in-house.

Lack of Information Access Controls Creates Security Holes

Access to product and service information offered on the B2C Web site must be strictly controlled. If such access is not controlled, critical service and product offering information and pricing could be changed inappropriately, resulting in customers placing orders with the wrong prices or the wrong descriptions. Formal policies and procedures must be in place to ensure service and product information cannot be modified without proper authorization. All edits should be logged and reviewed by quality assurance and management personnel.

Lack of Vulnerability Assessments Creates Security Holes

Vulnerability assessment of the B2C applications must take place. Without vulnerability assessment, significant vulnerabilities could be present and exploited when the application is moved to production. Tools are available that can be used to evaluate application code and security vulnerabilities. Code reviews can also be performed to identify faulty logic that creates vulnerabilities.

Lack of Logs Review

Someone must have assigned responsibility for reviewing the B2C Web server, database server, intrusion detection, and firewall logs. If logs are not reviewed, you will not know about potential security breaches in a timely manner, and will not be able to take proactive action. Periodic review of logs can help detect problems early while they are still manageable. Using automated tools for log analysis can help organizations that are short on human resources to perform the reviews. Another option is outsourcing log analysis.

Mobile Workers

An increasingly larger number of workers are becoming mobile. Personnel are carrying notebook computers, PDAs, smart phones, and Blackberries so that they can continue to work while they travel. More employees than ever are working from their homes. This increased mobility has enabled some individuals to be more effective in winning new business, transacting business on the spot, and delivering more timely and personal customer service.

An American Interactive Consumer report stated that there were 23.5 million teleworkers in the United States in 2003. The International Telework Association & Council (ITAC) and research partner Dieringer Research Group estimated there were 44 million United States teleworkers in 2004.

The nature of telecommuting inherently adds more work for an organization's IT and information security staff. According to Gartner, fewer than 30 percent of handheld computing devices are officially sanctioned or administered by IT. Support for such devices can take huge and unexpected amounts of time to address.

Large numbers of unauthorized personal computing devices are being used to perform business processing.

Securing the computing devices and storage media for mobile workers is dramatically more complex and difficult than securing a closed network. The more mobile workers an organization has, the more likely there are connections to their networks from external locations, and the more risks from each of these potential points of entry to the network. Recent studies from InfoBeads report most mobile workers work with information that is highly confidential and mission critical to the organization and has great impact on the business.

Mobile workers need to be well trained in the security requirements of computing while traveling and while working from their homes. They need to understand that they have ultimate control over the security of the business information while they are outside of organization facilities. Unfortunately, most mobile workers, especially those working primarily or exclusively from their homes, have notoriously lax security measures in place for their home-based business computers. A large majority now use cable and DSL modems for connections, effectively putting them online every hour of every day, subjecting them to the same types of attacks as the corporate networks but without the sophisticated firewalls and security tools in place to protect them.

ITAC and Dieringer Research Group reported the use of broadband by home teleworkers grew by 84 percent in 2004.

Think about how mobile workers actually work:

- Use telephone lines, DSL, and cable connections to link to corporate networks and business information
- Typically locate their home work areas where other members of their household and their houseguests can access their computing devices, storage media, and see their business printouts
- Often allow family members to use their business computing devices for school, other jobs held by household members, Internet access, volunteer work, and other activities
- Are vulnerable to the physical security hazards associated with children, pets, cleaning activities, roughhousing, and other common general living activities
- Have no one from the office ensuring they make backups or overseeing where the backups that actually get made are stored
- Can easily lose their computing devices and storage media that contain critical business information—often such losses are not reported or are reported only to the physical security office to write off as an asset loss for the depreciated value of the computer and associated software

This type of insider threat within your virtual perimeter can have dire consequences. Consider an exercise performed by Pointsec Mobile Technologies in 2004 (*Digital Secrets Up for Sale*, The Birmingham Post. June 15, 2004.) Pointsec purchased 100 laptop computers for pennies on the dollar over a 2-month period from Internet and public auctions. The amount of unsecured confidential business information contained on these computers was staggering:

- 70 percent of the hard drives (all of which were advertised as having been "wiped clean" or "reformatted") were readable.
- 77 Microsoft Excel documents were found containing customer email addresses, dates of birth, home addresses, telephone numbers, and other highly confidential information.
- A laptop purchased in Sweden contained confidential information from a large food manufacturer, including customer information, 15 PowerPoint presentations with "highly sensitive" company information, and more than 1500 private photos.

It is common practice at airports and mass transit facilities, such as Gatwick and Heathrow airports and on the Eurostar, for found items, including laptops, PDAs, and computer storage media, to be put up for auction if they are not reclaimed within 3 months.

Consider the damage not only to your organization's reputation, brand, and revenue, but also to your customers if your employees sold their computers containing business information. Consider also the potential serious legal ramifications of such an incident resulting in your company being charged with non-compliance with any number of regulations as well as potentially facing civil lawsuits.

It is critical for organizations to invest more time, attention, and resources in the security practices of their mobile workers and for the tools they use. Policies and procedures need to be implemented to effectively control the vast amount of business information processed outside of the network facilities.

Mobile Workers Create Holes and Entry Points into Your Network Perimeter

Organizations must make sure mobile workers:

- Process and access from their remote locations only the business information that they need to perform their business activities. They should not be able to access all the resources that they are able to access while logged onto the network from within corporate facilities.
- Use only business-owned computing devices to do work. When personnel use computing devices they personally own for business processing, the risks of having sensitive and confidential information mishandled and falling into the wrong hands increases dramatically.
- Receive the training and tools needed to maintain the security and confidentiality of business information while they are traveling and working from home locations.
- Have their remote computing devices configured in such a way as to allow information security and IT staff to be able to ensure the integrity of the information being transmitted from these multiple remote areas to inside the corporate networks as well as to ensure availability of the information when it is need within the business systems.
- Dispose of computing devices they no longer need securely, preferably through your organization's information security and/or asset management area. Such devices should never be donated to charities, given to family members to use, or auctioned off unless the storage media is first completely removed.
- Use hard disk encryption and access controls.

Mobile Computing Devices

The very nature of mobile computing devices puts them at a greater risk of theft than other types of computing devices. Your network hardware is typically located within secured facilities, but your mobile devices, which have access through your network perimeter, are typically located outside your organization's physical security perimeter. As previously discussed, mobile workers rarely work in an environment as secure as your business offices. Mobile devices are used in cars, airplanes, trains, and buses; stuck in purses, bags, and jacket pockets; and many times are forgotten and left in overhead storage compartments, restaurants, bookstores, and libraries.

What if your CEO's or security administrator's mobile computing device fell into the hands of a competitor, a criminal, or the news media? Would they be able to read confidential email, customer information, or access your internal network using the device?

What Is a Mobile Computing Device?

A mobile computing device is any device or medium that has computing capabilities, such as a PDA, laptop computer, or smart phone, or a device capable of storing electronic data, such as a CD, a USB thumb drive, a backup tape, and so on. Examples of mobile computing devices include:

- Notebook, laptop, and PDA computers
- Smart phones with storage, video, and/or computing capabilities
- Blackberries and other types of wireless email devices
- Laptop computer hard disks
- PDA memory drives
- Digital media cards, such as CompactFlash, SmartMedia, Secure Digital Memory Card, and MultimediaCard
- USB (or Firewire) storage devices
- Removable media such as CDs, DVDs, diskettes, and tapes
- Cell phone memory
- System Identification Module (SIM) cards for cellular phones
- MP3 players
- Digital cameras

Business Use Is Increasing

According to a 2004 IDC report, virtually all enterprise employees own cell phones and/or handheld computing devices. More than 22 million smart phones capable of running enterprise applications shipped in 2004, and IDC projects this number will reach 100 million by 2008. As the numbers increase, such handheld devices will become attractive targets for theft.

Frost & Sullivan research reports mobile professionals represent 75 percent of data users in the United States. The value of the business data and credentials stored on these devices has increased along with their ability to run critical business applications, ranging from email and instant/text messaging to field support and sales force automation. The top-tier executives are among those most likely to make extensive business use of mobile computing devices; they are also the personnel with the most critical and confidential business information.

Mobile Devices Store Increasingly Large Amounts of Data

Handheld storage capabilities were originally very limited, typically to just a few kilobytes of RAM. However, these devices are now capable of storing megabytes of information. Small removable compact flash devices and multimedia cards have tremendously expanded storage capacities. If a mobile computing device or memory stick falls into the wrong hands, it is likely to expose huge amounts of business information, potentially including customer information, business email, corporate plans and strategies, and so on.

A handheld device belonging to a power company employee in Japan containing confidential personal information for 665 families was stolen in 2005. In 2003, a Blackberry that had belonged to a Morgan Stanley executive was sold on eBay that contained dozens of business emails and other confidential information.

Easier than Ever to Compromise

The more advanced and feature-rich mobile computing devices become, the more ways there are to compromise them. With capabilities such as built-in cameras, text and media messaging, and always-connected Internet access, these devices are more versatile and usable than ever before, but they are also making it easier to download ring tones, images, games, malicious code, and shareware. When personnel use these advanced technology mobile devices without understanding the associated risks, it puts your business at increased risk to exploits from inside your perimeter.

Smart phones with Bluetooth connections can be victims of Bluesnarfing (remotely reading and writing the phone's address book, initiating calls, sending text messages, and so on.)

Easier than Ever to Lose Mobile Devices

Because of their increasingly small sizes and diminishing prices, mobile computing devices are often not handled carefully and end up being lost. People typically view such inexpensive devices as being easy to replace, and some almost treat them as disposable or in nonchalant ways. More and more vendors give away USB drives and PDA devices at trade shows as marketing gimmicks. It's no wonder the perceived value of such devices can tend to be negligible without giving thought to the value of the information contained within them.

A 2005 FusionOne poll revealed 43 percent of mobile users had experienced theft, loss, or damage of their mobile computing devices. Gartner estimates that 90 percent of mobile computing devices containing business information do not have security implemented, such as power-on passwords or encryption to protect the information.

Mobile storage media is often overlooked as a source of concern by organizations, but it contains some of the most sensitive and confidential business information. The risks are great:

- An information thief can quickly remove and potentially replace such media by an information thief with a dummy device so that the owner does not immediately realize the information was stolen.
- Small items such as these media devices can easily be misplaced, lost, or forgotten.

Dealing with Theft and Loss

An organization must immediately deal with a variety of issues when a mobile device is stolen or lost. The cost of replacement hardware is often insignificant compared with the potential financial costs from the primary security considerations:

- The information stored on the device is available to any third party who comes into possession of the device if the information was not encrypted. If the device contained proprietary or confidential information, this presents a serious risk to an organization.
- If the device holds credentials, such as unsecured digital certificates for use in accessing the corporate infrastructure, the device could be used to compromise corporate resources. Theft of credentials threatens data confidentiality.
- A lost device results in the user being without the ability to use it and the information it stores. They may now be incapable of performing their duties until the device and its data are recovered or replaced.

Your organization should have a documented policy for responding to the loss or theft of mobile computing devices. There should be a procedure to quickly report the loss, and device owners must be aware of this procedure. Information security must clearly and periodically communicate a clear message to the user community about the risks of mobile computing devices and stress the importance for users to report the theft or loss of a device immediately.

Mobile devices provide entry points to your internal network. Organizations must implement controls on mobile devices appropriate to the associated risks. When determining risks you need to review:

- The value of the data stored on mobile devices
- The specific vulnerabilities of the mobile devices in use
- The specific threats to the organization

Wireless Connections

Most mobile computing devices provide a wide range of wireless communications capabilities, such as Infrared, Bluetooth, Wireless LAN, GPRS, and even dialup over analog cell technology. All of these capabilities provide routes into your organization and network systems. They all are also vulnerable to communications interception in varying degrees. When mobile devices are used to transmit sensitive information, there are risks that the information can be inadvertently disclosed or intercepted. Virtual private networks (VPNs) are often deployed to address and control these risks.

Connections Made Outside the Network Perimeter

Wireless connections can easily, and are often, made to other outside untrusted networks. Such connections can be made from within your network or facilities. Mobile workers also often connect to untrusted networks using wireless in such locations as at an airport or using a broadband Internet connection within their own homes. Such devices are typically connected directly to the Internet without the protection of firewalls or intrusion detection systems (IDSs). This setup exposes the device, business information, and subsequently your organization, to a great range of threats, including direct attack from entities on the Internet, whether they are human or malicious code.

Wireless LANs Have Significant Risks

Businesses are jumping on the wireless network bandwagon in droves. However, there are a great number of risks inherent to wireless LANs for which business leaders are many times not aware. Some of these risks include unsecured default configurations, unsecured network architecture supporting the wireless LAN, encryption weaknesses, and physical security weaknesses.

> 🕮 An August 2005 CIO Insight survey reported that 83 percent of 357 IT executives indicated they use wireless networking.

War Driving

Most wireless networks are configured by default to allow any wireless system to access the network without authentication. Individuals can easily drive around with a wireless computing device and pick up many network connections, a practice called war driving. War driving is widely used to locate free Internet access or—even worse news to your business—to access information on corporate networks. Wireless LAN administrators may not know just how vulnerable they really are. If you have a wireless network, you must protect it against war driving.

> When someone gains access to your wireless network, the only things keeping the person from accessing unauthorized servers, applications, and information are strong internal security controls. If internal controls are weak or non-existent, an unauthorized individual could easily gain access to your corporate wireless LAN, then possibly take over control of your network by exploiting weaknesses.

DoS attacks are also a threat to wireless networks. If you have mission-critical systems running on your wireless network, an attacker doesn't even need to gain access to a system to cause damage or financial harm. All the attacker has to do is flood your network with transmissions to cause a DoS attack.

To help prevent the risk of inside attacks from occurring through wireless networks, you need to take two primary actions:

- Limit the network access to only authorized users
- Protect wireless traffic from sniffing

Legal and Regulatory Compliance

Regulations affecting the implementation of information security controls are becoming more common. For organizations in many sectors (such as healthcare, power generation, and financial services), there is specific legislation with which they must comply. These regulations do not focus on requirements for securing the perimeter of an organization's network. Indeed, they apply to all levels of an organization's information infrastructure. Relying upon securing the perimeter would likely lead to non-compliance with these regulatory requirements.

For example, consider the United States HIPAA regulation. The two sections within this regulation that impact information security professionals are the Privacy Rule and the Security Rule. Both require a variety of controls to be in place for ensuring the confidentiality and security of Protected Health Information (PHI). The Security Rule has very specific requirements for administrative safeguards, physical safeguards, and technical safeguards that must exist within all areas of the organization and network in which PHI is handled, accessed, or stored. Penalties and fines for non-compliance with these requirements can have huge impact upon an organization.

For noncriminal violation of the HIPAA rules, including disclosures made in error, civil penalties of $100 per violation up to $25,000 per year, per standard, may be issued. Additionally, criminal penalties may be applied for certain violations done knowingly as follows:

- Wrongful disclosure offense: $50,000 fine, no more than 1 year in prison, or both
- Offense under false pretenses: $100,000 fine, no more than 5 years in prison, or both
- Offense committed with intent to sell information: $250,000 fine, no more than 10 years in prison, or both

Also consider California's SB1386. This law requires any organization (state agency, person, or business) conducting business in California and processing personal information for California residents to disclose any information security breach to California residents whose unencrypted personal information was obtained by an unauthorized person. This legislation applies to information located anywhere, including inside the perimeter, on mobile computing and storage devices, and in any form. In 2005, 32 other states had proposed similar laws, with at least 19 states passing breach notification bills as of August 15, 2005. Different versions of the United States federal breach notification laws were also proposed. All these laws compel organizations to implement more security protection around personal information wherever it is stored.

Privacy Rights Clearinghouse has chronicled 82 different publicized personal information breaches that have occurred since February 15, 2005—starting with the ChoicePoint incident—through September 29, 2005. They estimate close to 51 million people had their personal information compromised within the accumulation of all these incidents.

Besides HIPAA and California SB1386, other regulations such as the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, the European Union Data Protection Directive, and Japan's Personal Information Protection Act require many companies to protect personal information from unauthorized access, regardless of where the information is stored or handled on the network. Companies are not compliant by merely taking actions to secure their network perimeters. Information must be secured and controlled throughout the entire enterprise, and access must be controlled within the workforce to only those who have a business responsibility for the information. Organizations often give little thought to the information stored on mobile computing devices, accessed by business partners, or through any of the numerous wireless, dial-up, or third-party connections.

The number of regulatory requirements enacted to address the security of financial and consumer information continues to grow. This increasing number of laws makes it necessary for business leaders to reassess the security strategies and goals for what they have historically considered their trusted network components; those components exist within the perimeter defenses where information has until recently always been assumed to be safe. This places more responsibility upon IT security administrators to meet regulatory requirements by performing more activities with the same amount of resources. The resulting stress upon these personnel not only lead to regulatory non-compliance because of lack of resources and time but also to unhappy workers, who in turn themselves become insider risks to your internal network.

Inappropriate Technology for the Purposes Being Addressed

Oftentimes in exasperation of having no all-encompassing security solution available, organizations try to apply other technologies to address the internal network security challenges:

- Inappropriate existing encryption solutions meant to be used with email are often tried as solutions to encrypt databases in storage.
- Systems and applications are developed with security added as an afterthought, at a much higher price resource time and dollar-wise than it would have been if security had been built into the project from the very beginning.
- Routers are used internally for access control solutions within the network.
- Home brewed security "solutions" are hard-coded into applications, resulting in applications working inappropriately, or security being easily compromised.
- If the technology is new, it may not be sufficiently strong or flexible to produce the desired results or adequately protect the intended resources.
- Departmental or application-specific firewalls are used within the enterprise network core.
- Access control for large populations of users is attempted by blocking individual IP addresses.

To be effective, security solutions must be appropriate to the risks, threats, and vulnerabilities being addressed. This security within the perimeter will be layered and will typically contain the following:

- Security policy
- Incident response plan
- Host system security
- Auditing
- Intrusion detection systems
- Router security
- Firewalls
- Vulnerability assessments
- Encryption
- Applications security

Increasing Data Value Increases Threats

Data is more valuable than ever before—another significant reason for protecting data everywhere it is located. In the past few years, there has been a dramatic increase in the value of data, particularly personal data, that has led to an explosion in the number of incidents for unauthorized access to and use of information.

> 🕮 The United States Federal Trade Commission reports the dollar volume of identity theft crime was $52.6 billion in 2004. Approximately 10 million Americans had their personal information misused, costing consumers roughly $5 billion and businesses around $48 billion. In addition, the United States Secret Service reported actual losses to individuals and financial institutions involving identity fraud totaled $442 million in 1995. This is an increase of 12,615% in 9 years!

There are large numbers of unscrupulous individuals who are more motivated than ever to obtain personal information to sell for profit. The black market for personal information is quite lucrative. For example, the June 21, 2005 *New York Times* reported change of billing (cob) account information is particularly valuable for information thieves; Discover Card cobs with any balance go for around $50 for each account, and American Express, a more exclusive and potentially more profitable account, line the pockets of the information thieves for around $85 each. There are even multiple sites, such as the now defunct sites iaaca.com and carderportal.org, that even provide lengthy tutorials to their subscribers about how to steal personal information and make massive profits.

The potential to make millions of dollars is strong motivation for many people to take advantage of the weak controls and security a company has implemented for the personal information it collects and processes. When motivated information thieves find vulnerability anywhere within a company that allows access to personal information, they take action to obtain the information. Trying to protect information only at the perimeter of a network is inadequate for trying to keep information thieves from getting to your data anywhere, any time, and using any means.

Summary

Protecting information resources within the perimeter is a business necessity. It is no longer possible to establish a network perimeter that can be a bastion of solid, impenetrable security to protect all the data safe and snug within. The perimeter is porous—this idea is no longer a debatable opinion, it is a fact. Tribal thinking must change. Smart business leaders can no longer blindly trust all their personnel; not everyone within your organization wants, or plans, to be a permanent member of your team. Mobile computing has expanded your information universe—you now have highly valuable information boldly traveling and going far beyond your perimeter to locations and storage devices like never before and like you never expected.

The time is now for business leaders to take a holistic approach to securing the entire enterprise that complements and supports regulatory requirements as well as protects each internal component of the network. Doing so in harmony will minimize costs and improve productivity.

Multi-dimensional security provides a holistic approach to securing your enterprise data. Multi-dimensional security protects information assets and associated resources within all areas of your enterprise and in compliance with all regulatory, policy, and contractual requirements. It places protection at not only the perimeter but also wherever information is stored, processed, or transmitted. Multi-dimensional security employs not only technology solutions but also operational, administrative, and human forms of protection to help reduce the risks to information wherever information can be found.

Organizations must change their thinking from a secure-the-perimeter-only perspective to one that is a multi-dimensional enterprise-wide security strategy. They must start viewing their organizations as being comprised of numerous islands of information, each of which must be appropriately secured. We will explore this strategy in the next chapter.

Chapter 3: Multi-Dimensional Enterprise-Wide Security

Multi-dimensional security involves protecting the information assets and associated resources within all areas of an enterprise and in compliance with all regulatory, policy, and contractual requirements. It places protection at not only the perimeter, as has historically been the norm, but also wherever information is stored, processed, or transmitted. Multi-dimensional security involves more than just technology solutions; it also utilizes operational, administrative, and human forms of protection to help reduce the risks to information wherever information can be found.

At a high-level, a multi-dimensional security program includes the use of:

- Protection strategies
- Risk analysis and assessment
- Security policies, procedures, and standards
- Education
- Audit and validation
- Simplifying complexity

Using multi-dimensional security reduces the risk of a security breach, secures data flows throughout the transmission path, reduces the impact and cost of compliance audits, protects against insider attacks, and demonstrates due diligence.

Protection Strategies

There is no magic bullet solution that, in and of itself, will secure all enterprise information assets and systems in compliance with all contractual and legal requirements. Multiple protection strategies must be used to most effectively reduce and manage the risks that exist within today's highly decentralized and widely connected systems.

As a starting point, the strategies can be visualized as a combination of protecting connection points and processing and storage locations as well as educating the people who utilize them. Figure 3.1 represents these multi-dimensional topics and examples of the underlying components.

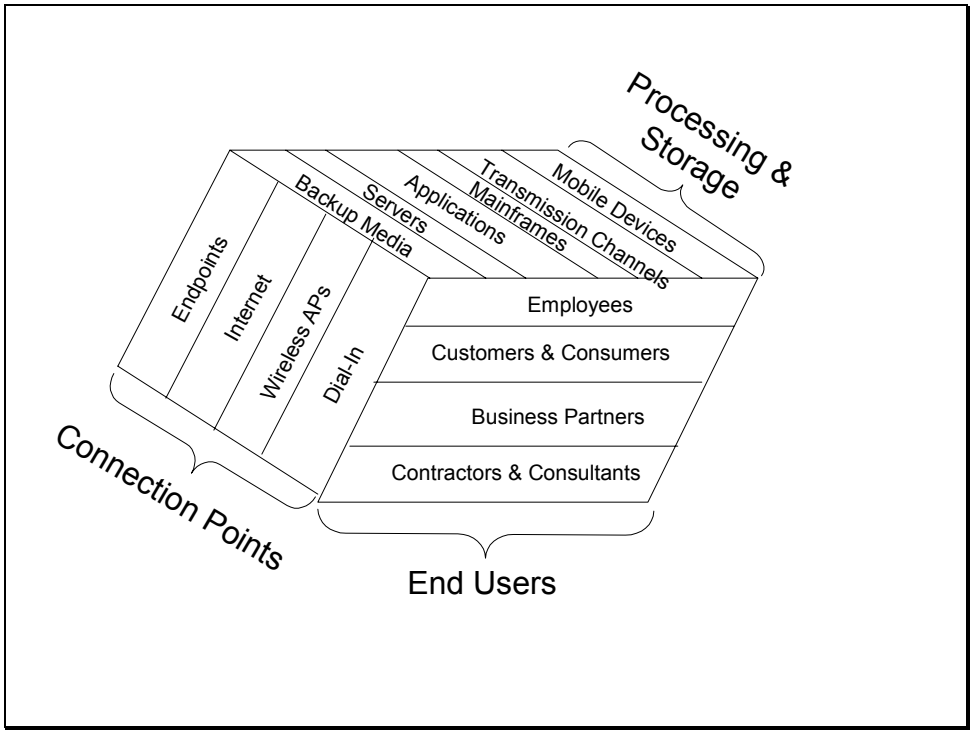


Figure 3.1: Illustration of multi-dimensional topics.

All these components are then working and handling information within the requirements outlined within policies, procedures, and standards, regulatory and legal requirements, education, and under the watch of audit and validation, as Figure 3.2 represents.

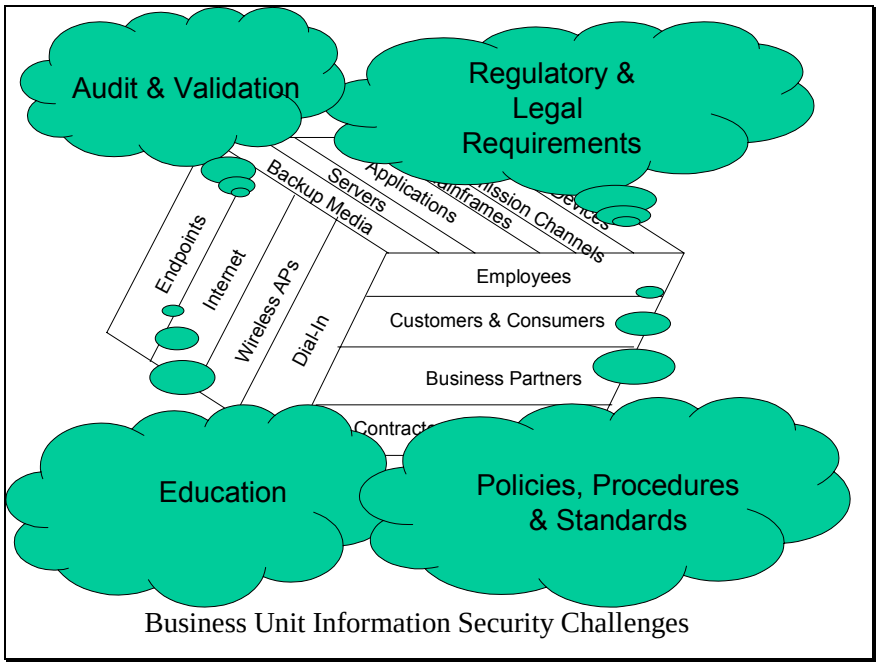


Figure 3.2: Multi-dimensional strategies within an organization's security requirements.

Each business unit must deal with these clouds of information security considerations. The typical organization will have many business unit information security clouds addressing these issues. Highly diverse multinational organizations will literally have information security considerations clouds covering significant areas of the earth, similar to the situation illustrated in Figure 3.3.

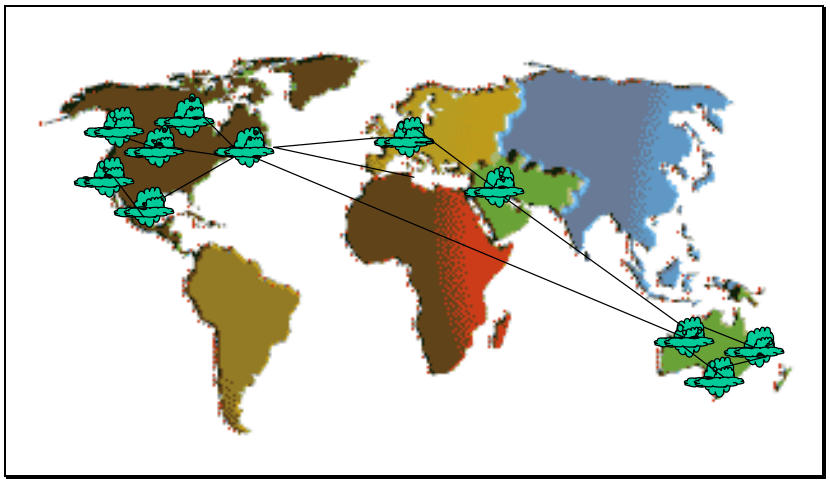


Figure 3.3: Worldwide processing locations and data flows.

The information components and issues within even the most seemingly simple organization can in actuality be quite complex. In a large organization, it can become almost overwhelming to information security practitioners to secure all these components and address all these issues. It is critical with so many components and issues to consider that organizations simplify the complexity as much as possible to be able to implement a successful information security program and subsequently help avoid dealing with information security incident storms that could result from all these volatile security considerations clouds crashing into each other. The first step in preventing your worldwide information security environment from experiencing destructive information security storms is to perform a risk analysis and assessment.

Risk Analysis and Assessment

It used to be that when businesses considered risks, they basically addressed the insurance coverage portfolio for the organization. Information security risk was not something at the top of business leaders' minds, or even in their thoughts, when the topic of risk management was mentioned.

As technology advanced, and as businesses became more decentralized and global, astute, forward-thinking business leaders realized that information was a cornerstone of successful business. As such, these leaders realized the need for appropriate protection to help reduce the risks to the confidentiality, integrity, and availability of the information.

Information security risk management evolved from the United States National Institute of Standards and Technology (NIST) Guidelines for Automatic Data Processing Physical Security and Risk Management (FIPSPUBs 31) and Guideline for Automatic Data Processing Risk Analysis (FIPSPUBs 65) in the mid-1970s. Because of the dramatic changes in the way information has been handled and processed since the introduction of what were then revolutionary documents, these FIPs were withdrawn in 2005 and 1995, respectively.

Risk Assessment and Analysis Methodologies

Since the introduction of risk analysis and assessment, there have been a wide range of methodologies and technologies developed for an even wider range of purposes. Some of the approaches are qualitative in nature, using metrics based upon information assets, threats, vulnerabilities, and safeguards and controls. Other methods are quantitative in nature, taking into consideration the monetary value of information assets, threat frequencies, threat exposure factors, and safeguard and control costs.

Risk Assessment and Risk Analysis…Defined?

First let us consider what is meant by the terms *risk assessment* and *risk analysis*. There has been much debate about these definitions over the years. NIST defines risk assessment and risk analysis within their Special Publication 800-30 as follows:

> Risk assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.

Note that NIST considers the terms to be one and the same in meaning. However, the International Organization for Standardization (ISO) defines these terms within ISO/IEC Guide 73:2002 as follows:

> Risk analysis: Systematic use of information to identify sources and to estimate the risk
>
> Risk assessment: Overall process of risk analysis and risk evaluation

Indeed there is room for interpretation. The goal of this guide is certainly not to argue for one term over another or to delineate the differences. For the purposes of this discussion, both terms will be used whenever discussing these types of risk management activities.

Most quantitative approaches are labor intensive and require the assessment/analysis facilitator to be a subject matter expert to most accurately determine the values of the risks. Unfortunately, a recurring weakness of risk assessments/analyses is that they usually fail to effectively communicate the discovered risks to business leaders, information owners, and decision-makers. Additionally, the accuracy of risk assessments/analyses is often in question, providing little value for business leaders and their decision-making process.

Automated tools can significantly reduce the labor and, to an extent, the inaccuracy of the monetary guesses associated with each risk. However, many businesses, frustrated with the cost and/or hard-to-use tools, have created their own in-house risk assessment/analysis methodologies and procedures. This process typically results in unstructured, uncoordinated methods for performing a risk assessment/analysis, and usually does not provide adequate consideration of all risks at all levels of the organization.

What Is Information Security Risk?

NIST defines risk in Special Publication 800-75 in the following two ways:

> Security risk: The level of impact on agency operations (including mission functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
>
> Investment risk: Risks associated with the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints.

Reducing information security risks is a necessity in today's business environment. Any type of internal or external threat, risk, or vulnerability can quickly impact a well-running organization in many ways, such as losing a competitive advantage, losing customers, missing deadlines or orders, bad publicity, regulatory noncompliance resulting in fines and penalties, or costly civil suit judgments. Performing a risk assessment demonstrates your company is demonstrating due diligence for the decision-making processes throughout your organization.

☞ A well-constructed risk analysis provides the documentation you need to prove that due diligence is performed.

To perform a risk analysis and assessment that will be useful to your organization, you must first define the risks. There are many professional and industry associations and government agencies that have published risk management and analysis guidance. Groups that have published risk management and analysis guidance include:

- The American Institute of Certified Public Accountants (AICPA)
- The Institute of Internal Auditors (IIA)
- The Information Security Forum (ISF)
- The American Society of Industrial Security (ASIS)
- The Information Systems Audit and Control Association (ISACA)
- The Information Systems Security Association (ISSA)
- The International Information Security Foundation (IISF)
- The International Organization for Standardization (ISO)
- The National Association of Corporate Directors (NACD)
- The Organization for Economic Cooperation and Development OECD
- The United States Department of Homeland Security Critical Infrastructure Assurance Office (CIAO)
- The United States President's Commission on Critical Infrastructure Protection (PCCIP)

Define Risks

Define risks for your organization and within each of the business unit areas. What does legal consider as information risk? What do your privacy and compliance areas consider as information risk? What do your auditors consider as information security risk? What do information security leaders consider as risk? To be successful with a risk analysis and assessment, you need to first define organization-wide risks that exist within your environment and come to a consensus. The subsequent results of the risk analysis and assessment will then be more readily accepted as being applicable for your environment. When your coworkers participate in making security decisions, they feel ownership for the resulting actions that are implemented and are more likely to make a conscious effort for compliance.

The United States Office of Management and Budget (OMB) has identified 19 areas of information security risk, which are highlighted in the following list:

- Schedule—Risk associated with schedule slippages, either from lack of internal controls or from those associated with late delivery by vendors, resulting in missed milestones.
- Initial costs—Risk associated with "cost creep" or miscalculation of initial costs that result in an inaccurate baseline against which to estimate and compare future costs.
- Life cycle costs—Risk associated with misestimating life cycle costs, exceeding forecasts, and relying on a small number of vendors without sufficient cost controls.
- Technical obsolescence—Risk associated with technology that becomes obsolete before the completion of the life cycle and cannot provide the planned and desired functionality.
- Feasibility—Risk that the proposed alternative fails to result in the desired technological outcomes; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.
- Reliability of systems—Risk associated with vulnerability/integrity of systems.
- Dependencies and interoperability between this investment and others—Risk associated with interoperability between other investments; risk that interoperable systems will not achieve desired outcomes; risk of increased vulnerabilities among systems.
- Surety (asset protection) considerations—Risk associated with the loss/misuse of data or information; risk of technical problems/failures with applications; risk associated with the security/vulnerability of systems.
- Risk of creating a monopoly for future procurements—Risk associated with choosing an investment that depends on other technologies or applications that require future procurements to be from a particular vendor or supplier.
- Capability of agency to manage the investment—Risk of financial management of investment, poor operational, and technical controls, or reliance on vendors without appropriate cost, technical, and operational controls; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.

- Overall risk of project failure—Risk that the project/investment will not result in the desired outcomes.
- Project resources/financial—Risk associated with "cost creep," miscalculation of life cycle costs, reliance on a small number of vendors without cost controls, or inadequate acquisition planning.
- Technical/technology—Risk associated with immaturity of commercially available technology and reliance on a small number of vendors; risk of technical problems/failures with applications and their inability to provide planned and desired technical functionality.
- Business/operational—Risk associated with business goals; risk that the proposed alternative fails to result in process efficiencies and streamlining; risk that business goals of the program or initiative will not be achieved; risk that the investment will not achieve operational goals; risk that the program effectiveness targeted by the project will not be achieved.
- Organizational and change management—Risk associated with organizational-, agency-, or government-wide cultural resistance to change and standardization; risk associated with bypassing, lack/improper use of, or non-adherence to new systems and processes because of organizational structure and culture; risk associated with inadequate training planning.
- Data/information—Risk associated with the loss or misuse of data or information; risk of compromise of citizen or corporate privacy information; risk of increased burdens on citizens and businesses because of data collection requirements if the associated business processes or project requires access to data from other sources (federal, state, and/or local agencies).
- Security—Risk associated with the security/vulnerability of systems, Web sites, and information and networks; risk of intrusions and connectivity to other (vulnerable) systems; risk associated with the evolution of credible threats; risk associated with the criminal/fraudulent misuse of information; must include level of risk (high, moderate, low) and what aspect of security determines the level of risk (for example, need for confidentiality of information associated with the project/system, availability of the information or system, or integrity of the information or system).
- Strategic—Risk associated with strategic- and government-wide goals; risk that the proposed alternative fails to result in achieving those goals or in making contributions to them.
- Privacy—Risk associated with the vulnerability of information collected on individuals or risk of vulnerability of proprietary information on businesses.

Risk Analysis and Assessment Challenges

Major problems exist with the language and use of risk analysis and risk assessment primarily because such activities did not evolve from academia or from a well-structured professional oversight body. Instead, information security practitioners have been forced to create their own risk analysis and assessment methodologies to meet their environments' needs. A significant number of information security professionals have performed what they label as risk assessments and skewed the results to meet their own agendas (for example, obtaining more budget or obtaining justification to remove systems they personally do not want to support). Such misuse of the risk assessment process has negatively impacted the perception of the usefulness of such risk review activities.

The language of results of the risk assessment/analysis is also typically vague or highly subjective. Such vagueness and subjectivity does not typically fit well within a business environment that is used to viewing risks in terms of dollars and cents. Unfortunately, most business leaders ask information security practitioners to quantify risks to determine budgets for information security expenditures. This requirement puts information security practitioners in the very difficult situation of losing the confidence of their management when they do not get the numbers exactly right.

Lacking a well-established taxonomy and terminology, even well-meaning, smart security practitioners discuss risk management in ways that can be misinterpreted or lead to poor business decisions. This misinterpretation results in confusion, frustration, and mistrust not only within an organization but also among the security professionals themselves. Inconsistent and misleading use of language results in inconsistent, misleading, and incorrect results of a risk assessment activity.

Risk assessment and risk analysis are not the only misused terms in this area. *Threats* and *vulnerabilities* are often used interchangeably within risk assessment/analysis reports and by information security professionals, leading to confusion on the part of the readers, which are typically business organization leaders.

Most insightful risk and security leaders realize that security risks cannot be accurately and specifically calculated. The reason is that there is no body of complete and valid information covering information security upon which you can base calculations (unlike predicting financial investment risks based upon actuarial tables and significantly large and well-established bodies of incident information). However, performing risk assessment/analysis is still necessary for businesses to be able to adequately understand information risks and to determine which controls and tools to use to prevent the risks based upon how many times similar incidents have occurred elsewhere. The most realistic way to do so is through the use of qualitative risk analysis, based upon regulatory requirements and the potential impact from non-compliance fines and penalties. The assessment/analysis should then communicate what the financial impact experiences for each risk have been in other companies.

Organizations must meet the conditions of the various legal and regulatory requirements for performing a risk analysis and assessment. Smart organizational leaders will maximize the process of performing a risk assessment/analysis so that the requirements of as many applicable laws and regulations are met as possible to eliminate the need to do multiple assessments and end up duplicating work and effort.

Risk Analysis and Assessment Must Be Part of a Multi-Dimensional Security Strategy

Business leaders must recognize two givens:

- Each information system and process has its own risk environment
- Each information system and process has its own unique inputs, outputs, level of activity, and associated costs

Because of these differences, each information system and process will have unique security requirements that are determined by the associated risk environments.

> ☞ The risk environment determines the possibility of harm and loss, and the inputs, outputs, level of activity, and associated costs determine the magnitude of harm and loss resulting from the exploitation of the risks.

An effective risk assessment/analysis will document information about risk exposures. This risk information will be used to make the most optimal risk mitigation decisions to result in the best overall performance. An effective risk assessment/analysis will allow the business to invest enough, but not more than what is necessary, to appropriately address information security risks.

> It is bad business and bad information security management to spend $10,000 to mitigate $1000 of potential losses. Information security expenditures should not cost more than the value of the systems, assets, and processes being protected.

An effective risk assessment/analysis will produce a measure of risk so that risks can be consistently and reliably compared with one another, and the risk mitigation costs can be correlated to the risks they are addressing.

> A common mistake businesses make is assessing a risk as “high,” “unacceptable,” or some other qualitative term, then not providing the quantitative information (such as estimated lost time, money, customers, fines, and so on) necessary to support a decision to implement risk mitigation measures. Risk mitigation measures should always have quantitative implementation costs provided to make the assessment/analysis useful.

Security requirements are identified using a methodical assessment/analysis of security risks. Expenditures for risk mitigation controls must be balanced against the business harm estimated to result from security incidents and failures. The results of the risk assessment/analysis will help to guide and determine the appropriate management action and priorities for managing information security risks and for implementing the controls selected to protect against these risks.

> ☞ Risk assessment/analysis should be repeated periodically to address changes that might influence the risk assessment results.

Security Policies, Procedures, and Standards

Information security policies, procedures, and standards are all important considerations organizations must formally document and implement to have an effective information security program. Each type of document serves a different purpose.

Information Security Policy

An information security policy establishes the framework within which the business rules and regulations for handling information and reducing risk are described. Effective policies are created to help bring the organization into compliance with applicable laws and regulations as well as to address how to secure the business information processing environments within the organization. Management should set a clear policy direction in line with business objectives and visibly demonstrate support for, and commitment to, information security.

Information security policies are mandatory; they should not be written in a way that implies they are merely suggestions.

Information Security Procedures

Information security procedures describe how to implement the policies. Procedures document the step-by-step detailed actions necessary to successfully complete a task that supports the policies. Procedures provide personnel with the information necessary to complete a task and provide assurance to management that the tasks are being completed in a consistent approved manner. Procedures improve efficiencies in employee workflow and assist in the prevention of misuse and fraud.

For example, a policy may require all information that leaves the organization to be encrypted. The corresponding procedure would define the tools and methods for encrypting the information, such as requiring the use of a virtual private network (VPN), along with details about each step to take to implement the software and hardware necessary to use the VPN in a way that is acceptable to the organization.

Information Security Standards

An information security standard is a detailed specification for hardware, software, and human actions to support the information security policies. Standards can detail the requirements for a wide range of issues, from the software to hardware that must be used to the remote access protocols that must be implemented to describing who is responsible for making information security approvals. Standards provide a documented way of ensuring that programs and systems will work together. By establishing standards, the enterprise limits the possibility of rogue applications systems, platforms, hardware, or software. There is less time spent in supporting non-standard activities or products. In short, standards define cost-savings processes that support the efficient running of the enterprise.

For example, a technical information security standard to support the policy requiring only corporate approved solutions be used to connect to the Internet might include a detailed description of how the transmission control protocol/internet protocol (TCP/IP) must be implemented, managed and used. A standard details the specific technical choices for implementing particular policies. For example, a policy may require strong identification and authentication be used when accessing information classified as confidential. The supporting standard might specify the specific brand and model of a microprocessor-equipped smart card to be used to enforce the access control restriction. Generally, those who are responsible for implementing policies use standards. Most standards do not need to be communicated to all personnel—only those responsible for the implementation of the policies. Standards also typically must be modified more regularly than policies in response to changing technologies and systems.

Regulatory Requirements for Information Security Documents

Many United States and international laws and regulations require organizations to document and implement policies, procedures, and standards. Additionally, business leaders must demonstrate that a standard of care exists within the enterprise. The implementation of these information security documents provides a demonstration of exercising due care.

Some of the laws and regulations that require organizations to document and implement information security policies, procedures, and/or standards include the following:

- The Gramm-Leach-Bliley Act (GLBA)
- The Health Insurance Portability and Accountability Act (HIPAA)
- Canadian Personal Information Protection and Electronic Data Act (PIPEDA)
- The European Union's Data Protection Directive

Additionally, the United States Federal Sentencing Guidelines for Organizations takes into consideration the policies implemented and clearly supported by executive management when they determine judgments for fines and penalties.

The Goal of an Information Security Policy

An information security policy documents executive management's direction on, and commitment to, information security. To be effective, you must communicate the security policy to everyone within your enterprise that handles your information or uses your systems.

> ☞ Executive management must communicate their direction on and commitment to information security within a high-level information security policy that applies to all parts of the enterprise.

An effective information security policy will

- Include a statement of direction from executive management supporting the goals and principles of information security.
- Communicate the business risks associated with information security incidents and accidents.
- Document information security, responsibilities, and the high-level principles personnel must observe.
- Specify key activities that must occur within the organization, such as carrying out security classifications and risk analyses, safeguarding important records, and reporting suspected security weaknesses.
- Require information to be protected in terms of its requirements for availability, integrity, and confidentiality.
- Emphasize the need for compliance with software licenses and other legal, regulatory, and contractual obligations.
- Prohibit unauthorized or personal use of the organization's information and systems and the use of obscene, racist, or otherwise offensive statements (for example, via email or over the Internet).
- Document that disciplinary action will be taken against individuals who violate policy requirements.

> ☞ An information security policy should be reviewed periodically and revised as necessary to reflect changes within the organization as well as technology changes.

Challenges of Policies, Procedures and Standards

The 2005 State of Information Security Study from CIO and CSO magazines includes results from interviewing 8100 IT security professionals from 62 countries. The survey results reveal that 8 percent of the companies have no documented security policy. The policy topics that occurred most frequently, as demonstrated by the accompanying percentages, within companies who had them included:

- User administration (69%)
- Appropriate use of email (56%)
- Systems administration (67%)
- Network security administration (55%)
- System security administration (52%)
- Appropriate use of the Internet (46%)
- Role-based access control (45%)

Twenty-four percent of companies had neither measured nor reviewed the effectiveness of their security policies and procedures.

These statistics reveal some of the challenges of creating and implementing policies, procedures, and standards:

- Organizations often do not base the policies upon existing leading practice frameworks and end up with a set of policies that have significant topics missing.
- Organizations often issue policies because they must, but then do not take any actions to verify the policies, procedures, and standards they have issued are effective or realistic in their environment.
- The majority of organizations are not addressing major security vulnerabilities, risks, and threats within their policies, such as mobile computing security and social engineering.

Policies Are Viewed as Business Inhibitors

In practice, information security seems to interfere with everyone's business. Network administrators work hard to make the networks as user-friendly and easy to use as possible, but then when security is applied—because of the mindset of the typical end-user—the security as implemented is very user-unfriendly and slows down users when they are trying to get their work done. Security policies challenge information and systems users to change the way they think about their responsibilities for protecting corporate information.

When you attempt to implement security policies on an unwilling audience, you will be met with resistance not only because the security is viewed as making jobs harder and more tedious but also because the typical worker does not like to be told what to do…especially by an information security expert, who they do not see as having any authority over them or as having a place in their chain of command.

A big challenge worth tackling is to present information security to everyone within the organization in a way that enables them to recognize that they, personally and professionally, are responsible for information security. To be successful, information security officers must involve all personnel from throughout the enterprise in developing information security policies. Personnel must justifiably believe that they own their security procedures that support the policies. Personnel with real involvement in policy development will become partners to advance information security instead of being opponents of security.

Education

Supplying your personnel with the security information they need and ensuring they understand and follow the requirements is an important component to your organization's business success. If your personnel do not know or understand how to maintain confidentiality of your information or how to secure it appropriately, you risk not only having one of your most valuable business assets (information) mishandled, inappropriately used, or obtained by unauthorized persons but also being in noncompliance of a growing number of laws and regulations that require certain types of information security and privacy awareness and training activities. You also risk damaging another of your valuable assets—corporate reputation.

Regulatory Requirements Compliance

There are an increasing number of laws and regulations that require some form of training and awareness activities to occur within the organizations over which they have jurisdiction. Issues under the United States Federal Sentencing Guidelines that impact the severity of the judgments include consideration of the types of training and awareness organizations provide to their personnel. The following list is not exhaustive but provides some of the laws and regulations requiring training and awareness:

- HIPAA
- 21 CFR Part 11 (Electronic Records/Electronic Signatures)
- Bank Protection Act
- Computer Security Act
- Computer Fraud and Abuse Act (CFAA)
- Privacy Act
- Freedom of Information Act (FOIA)
- Federal Information Security Management Act (FISMA)
- 5 U.S.C. §930.301 (for United States federal offices)
- Appendix III to OMB Circular No. A-130
- Digital Millennium Copyright Act (DMCA)
- GLBA
- Department of Transportation DOT HM-232
- The Sarbanes-Oxley Act
- The Organization for Economic Cooperation and Development (OECD) Security and Privacy Principles
- The European Union Data Protection Directive
- Canada's PIPEDA

Customer Trust and Satisfaction

Respect for customer security and privacy is one of the most important issues facing your company today. To gain and keep customer trust, your company must exercise good judgment in the collection, use, and protection of personal information. Not only do you need to provide training and awareness about this requirement to your personnel, but you also need to communicate to your customers (with whom you have a business relationship) and consumers (with whom you would like to have a business relationship, and who may have provided some information to you) what you are doing to preserve their privacy and ensure the security of their information through various awareness messages.

All workers (employee and contract) or companies who directly handle or impact the handling of your company information should take your security training before handling your company information, with refresher training every year, or more often based upon your business and the potential impact to your business if information is not handled correctly. You should provide training and awareness to ensure all your company activities comply with the company privacy policy as well as laws and regulations.

Compliance with Published Policies

Organizations need to educate personnel about their information security roles and responsibilities—especially in support of published policies, standards, and procedures. Awareness and training should be constructed to support compliance with security and privacy policies. Executive management act as role models for personnel; their actions heavily influence the level of employee awareness and policy compliance. Senior management should clearly and noticeably support, encourage, and show commitment to information security and privacy training and awareness activities.

> ☞ Implement a procedure to obtain a signed information security awareness agreement at the times you deliver the training to document and demonstrate that training and awareness activities are occurring, that the personnel acknowledge and understand procedures, and that the education efforts are ongoing.
>
> In addition, include evaluation of information security and privacy actions within the yearly job performance appraisal for all personnel.

Due Diligence

In general, due diligence means providing demonstrated assurance that management is exercising adequate protection of corporate assets, such as information and compliance with legal and contractual obligations. This requirement is a powerful motivator to implement a training and awareness program. Key provisions of the United States Federal Sentencing Guidelines and 2004 amendments include establishing an effective compliance program and exercising due diligence in the prevention and detection of criminal conduct. Any organization with some type of compliance requirements and/or plans (basically all public entities given the Sarbanes-Oxley Act of 2002) is directly impacted by the guidelines. One way such due diligence is demonstrated is through an effective, executive-supported information security education program.

It is no longer good enough simply to write and publish information security and privacy policies and procedures. Organizational leaders must now have a good understanding of the policies and the program, support the program, and provide oversight of the program as reasonable for the organization. This new requirement reflects a significant shift in the responsibilities of compliance and ethics programs from positions such as the compliance officer and/or committee to the highest levels of management. The guidelines require that executive leaders support and participate in implementing the program. To do so, an effective ongoing information privacy, security, and compliance education program must be in place.

Corporate Reputation

Reputation is another critical organizational business success asset. Without a good reputation, customers leave, sales drop, and revenue shrivels. Reputation must be managed well. A component of managing good reputation is ensuring personnel and business partners follow the right information security actions to lessen the risk of something bad happening to information; such incidents will likely lead to very unseemly news reports and media attention.

There are many issues that impact corporate reputation that can be addressed through effective ongoing information security training and awareness activities:

- Customer complaints
- Competitor messages and internal messages related to competitors
- Customer satisfaction levels with your organization's security and privacy practices
- Providing for customers with special needs and requests
- Number of legal noncompliance reports regarding security and privacy
- Perceived strength of posted security and privacy policies
- Marketing with what is considered as spam
- Number of staff grievances
- Upheld cases of corrupt or unprofessional behavior
- Number of reported security and privacy incidents
- Staff turnover related to training and communications
- Value of training and development provided to staff
- Perception measures of the company by its personnel
- Existence of confidential grievance procedures for workers
- Proportion of suppliers and partners screened for security and privacy compliance
- Proportion of suppliers and partners meeting expected standards on security and privacy
- Perception of the company's performance on security and privacy by consumers worldwide
- Proportion of company's managers meeting the company's standards on security and privacy within their area of operation
- Perception of the company's performance on security and privacy by its employees
- Perception of the company's performance on security and privacy by the local community
- Dealing with activist groups, especially militant groups, opposed to the organization

Accountability

Most personnel understand that if they are being measured for certain activities, they need to be accountable for those activities because those measures can impact their career with the company in some way. If an organization reports information security compliance and connects it with personnel performance, personnel understand more clearly their accountability and are even more likely to comply.

Accountability has more impact on a company, and corporate personnel, than ever before. There are a growing number of legal actions being filed by victims of inadequate information security and privacy practices against organizations that were not necessarily the perpetrators of an incident but whose systems and poor practices contributed to allowing the incident to occur. Such shifts in accountability start moving the enforcement of policy from management to individuals. Such shifts are also being supported by new regulations and government moves, such as requiring federal agencies to increase personnel accountability for breaches and requiring security to become standard in all network and computing products.

Implementing the use of signed information security awareness acknowledgements not only establishes personal accountability but also increases awareness and accountability for information security and privacy. Such signed acknowledgments document your organization's efforts and due care to ensure all personnel are given the information they need to perform their job responsibilities in a manner that protects information and network resources. Signed acknowledgments should be considered a facilitator for your awareness and training efforts. Signed acknowledgements could also provide valuable support for any sanctions you need to administer for policy noncompliance.

Your organization should expect all employees, officers, contractors, and business partners to comply with privacy, security, and acceptable use policies and protect your organization's information and systems assets.

Audit and Validation

Security audits and compliance validation reviews provide an in-depth examination of an organization's security infrastructure, policies, people, and procedures. When performed effectively and successfully, they will identify areas of weakness within the infrastructure. The auditor or reviewer can then provide recommendations for appropriate actions to address the weaknesses and reduce the accompanying risks.

Audits are important to ensure that corporate security policies are being followed and enforced. How can you ensure your access control policies are effective unless an audit is performed to review them?

Audits need to be performed to provide individuals who are responsible for particular IT environments, as well as executive management, with an independent assessment of the security condition of those environments and to validate that necessary controls are indeed in place and functioning as they should. The information security status of the enterprise environments should be subjected to thorough, independent, and regular security audits and control validation reviews.

Security audits and compliance validation reviews must include consideration of the business risks associated with the particular environment (the security clouds described earlier) under review and should be performed for critical business applications, information processing environments, communications networks, system development activities, and manual administrative and operational tasks.

Security audits and compliance validation reviews should be:

- Agreed upon and supported by the individual responsible for the environment under review
- Performed by qualified individuals who have sufficient technical skills and knowledge of information security
- Conducted frequently and thoroughly enough to provide assurance that security controls function as required
- Complemented by reviews conducted by independent third parties

Recommendations for improvement resulting from the audits should be discussed and agreed upon with the individuals responsible for the environment under review and should be implemented and reported to executive management.

> ☞ Information systems, processes, and practices security should be regularly reviewed. Perform the reviews against the appropriate security policies and the technical platforms and information systems for compliance with applicable security implementation standards, documented security controls, and regulatory and contractual compliance.

Audit requirements and activities involving checks on operational systems must be carefully planned and communicated to the audited area's management to minimize the risk of disruptions to business processes. You want information security to be viewed as a business enabler not as an obstacle to achieving business goals. To help enable the success of an audit, keep the following guidelines in mind:

- Obtain agreement with the audited area's management for the activities being performed
- Determine and document the scope of the activities
- Limit the audit checks to read-only access to software and data; if necessary for the audit, allow access other than read-only for isolated copies of system files
- Explicitly identify the resources that will be used to perform the checks
- Identify and agree upon with management the requirements for special or additional processing
- Monitor and log all access to produce a time-stamped reference trail for all critical data or systems
- Document all procedures, requirements, and responsibilities for the audit activities
- Ensure the person(s) carrying out the audit are independent of the activities audited

Planning

Senior management should establish a plan to perform regular and independent audits to evaluate the effectiveness, efficiency, and economy of security and control procedures in addition to management's ability to control information security function activities. Senior management should determine priorities with regard to obtaining independent audits within this plan. Auditors should plan the information security audit work to address the audit objectives and to comply with applicable professional auditing standards.

Challenges of Audit and Validation

Organizations must integrate their information security goals within business strategies to reach their overall enterprise objectives, get the most value out of their information, and capitalize on the technologies available to them. As computerized applications are penetrating nearly all business functions and processes, organizations are mixing hardware platforms from different vendors with a combination of commercially available software and in-house developed software. Issues such as IT governance, international information infrastructure, e-commerce, security, privacy, and control of public and enterprise information have driven the need for self-review and self-assurance. These issues combined make the audit and validation process much more challenging and complex than in the past when information processing was generally limited to a large mainframe computer.

As a result of this increasing complexity, business risk increases. Audits and reviews are needed to evaluate the adequacy of information security to address the adequacy of all the information security and controls used by all the people, places, and processing systems. Recent situations such as those at Enron, WorldCom, and others have clearly shown the need for audit and independence.

The Sarbanes–Oxley Act of 2002 is one example of a regulation providing the needed support for organizations to address their organizational policies and controls and use the capabilities of their internal audit and information security teams.

Legal Implications

In the years preceding the Sarbanes-Oxley Act, limited liability partnerships formed following the result of a Big Five audit organization that was taken to court by a client. The client selected a support system based on the firm's recommendation. However, the support system failed to perform in the manner recommended and caused the company financial loss. The courts held the Big Five firm liable for failing to exercise "due professional care" in the conduct of their work performed. The Big Five company sought the protection of a limited liability partnership with its audited client.

With the fall of Arthur Andersen LLP during the Enron scandal, there is now a Big Four. Arthur Andersen LLP was the first major international accounting firm taken to court and successfully convicted for a lack of due professional care in the destruction of client documents and obstructing justice. After a month-and-a-half trial and 10 days of deliberations, jurors convicted Andersen for obstructing justice when it destroyed Enron Corp. documents while on notice of a federal investigation. Andersen and their lawyers had claimed that the documents were destroyed as part of its housekeeping duties and not as a ruse to keep Enron documents away from the regulators.

The Sarbanes-Oxley Act regulation is not the only law that serves to compel organizations to perform regular information security audits and compliance reviews. A few of the others include HIPAA, GLBA, 21 CFR Part 11, the Bank Protection Act, the Computer Security Act, the Computer Fraud and Abuse Act (CFAA), the Privacy Act, FOIA, and the Federal Information Security Management Act (FISMA).

Simplifying Complexity

The beginning of this chapter discussed the many different components and multiple dimensions of addressing information security. Many organizations find themselves trying to fight fires and tackle all the related information security issues without first taking the time to create a thoughtful information security strategy. The strategy needs to simplify the complexity resulting from such highly diverse, dispersed, and dimensional environments.

Organizations must simplify the complexity of information security management by taking the large number of technology, human, and compliance issues and making them understandable to the business. At the same time, organizations must implement solutions to integrate these issues throughout all business processes so that information security is built-in to all products and services from the beginning of a business idea right through until the resulting service or product is no longer offered.

These complexities can be simplified using a common framework of information security disciplines and by getting the support of the information security efforts by the leaders throughout the organization rather than focusing on each individual issue at a time. The first step in simplifying information security complexity is by appointing an enterprise-wide information security officer to oversee and coordinate information security activities and decisions for the entire enterprise. This oversight will not only be the first step in simplifying complexity but also lead to consistency in addressing information security issues throughout the enterprise.

Challenges in Simplifying Complexity

Information security practitioners have been struggling with how to simplify the complexity of information security management for years. To many of them, it seems as though for every step forward they take with progress, they take two steps back because of how swiftly technology changes, how swiftly new connections are made to their networks, and how swiftly more and more employees and business partners are mobilizing their business information processing. Most also focus on just one business unit issue at a time, resulting in the information security function hop scotching back and forth between different services and products, and not coordinating efforts or maximizing the benefits of rolling information security controls out to all enterprise areas at the same time. Information security leaders end up constantly fighting security fires as each business unit information security cloud lightning strikes.

Divide and Conquer

To be effective, information security leaders must implement an information security strategy to simplify their efforts. To do so, consider each of the components within the multi-dimensional information security issues, divide your security responsibilities throughout the organization, and use automation to simplify and conquer your information security activities and challenges.

Too many times information security practitioners try to take on all the information security tasks themselves. This undertaking is not only unfeasible in most situations but also does not foster the need for all personnel to take responsibility for information security. When everyone is part of the development of information security, as a whole, organizations can then identify tools to address those activities that can be automated. There will be many areas where you can automate some of your information security activities throughout the enterprise (for example, through the use of centralized intrusion detection systems, access logs, antivirus solutions, and so on).

Address Information Security Components Using an Enterprise-Wide Action Plan

Dividing and distributing the information security responsibilities throughout the entire enterprise can accomplish simplification of complexity. One way to do so is by implementing the following:

- Assign overall responsibility for enterprise information security oversight.
- Establish an information security oversight board consisting of management representatives from each business unit and corporate functional office.
- Assign responsibilities for each of the governance categories:
  - Education through training and awareness
  - Regulatory and legal requirements
  - Audit and validation
  - Policies procedures and standards

- Assign responsibilities to representatives from each corporate and business unit for each of the security dimensions:
  - Connection Points
    - Endpoints
    - Internet
    - Wireless
    - Dial-In
  - End users
    - Employees
    - Customers and consumers
    - Business partners
    - Contractors and consultants
  - Processing and storage
    - Mobile devices
    - Transmission channels
    - Mainframes
    - Applications
    - Servers
    - Backup media

Figure 3.5 provides an illustration of an example distribution of security responsibilities.

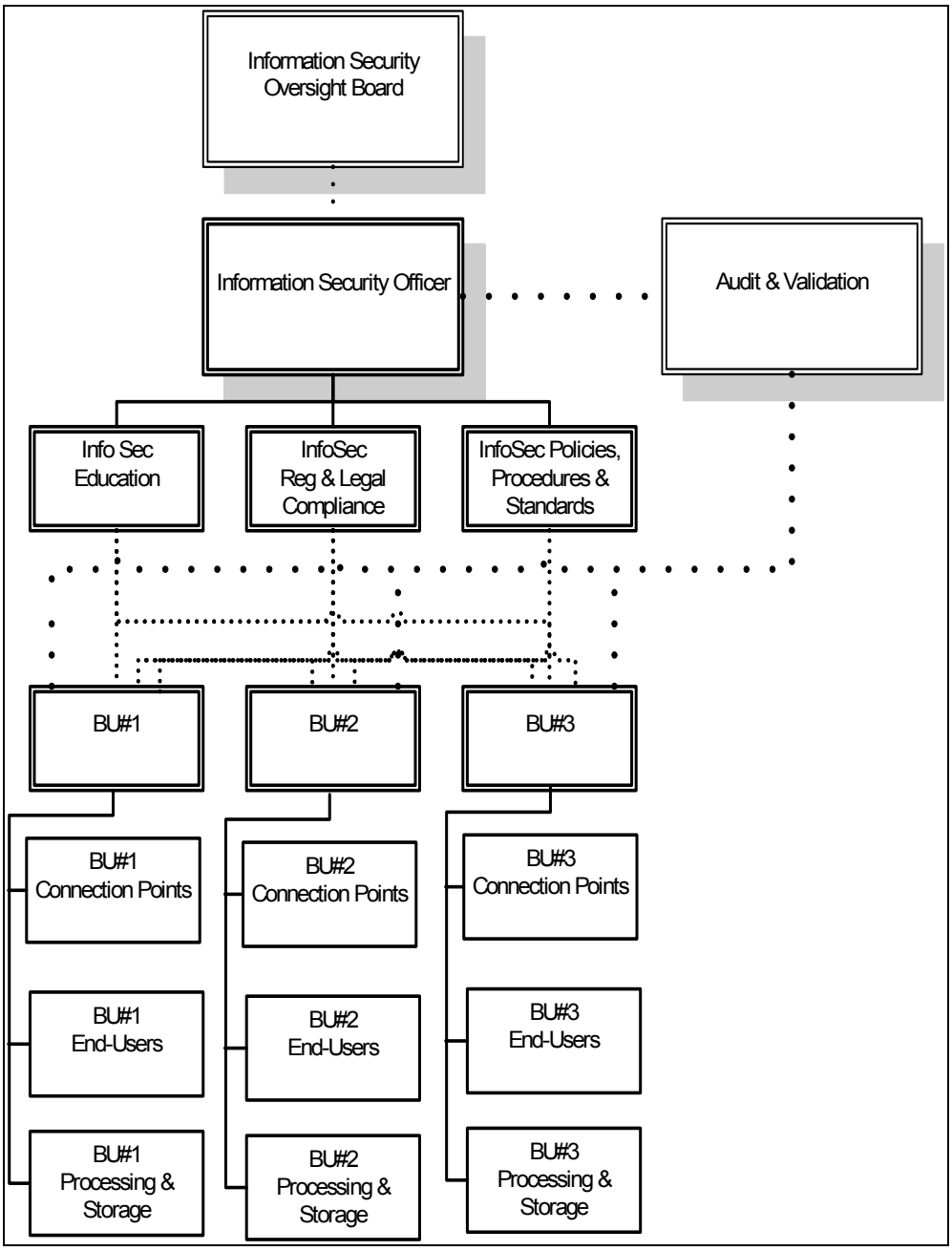


Figure 3.5: Example distribution of enterprise information security responsibilities.

Each role with information security responsibilities should use proven technology tools to automate as much as possible their responsibilities.

Challenges to Simplifying Complexity

Even when dividing and distributing information security responsibilities throughout the enterprise, information security leaders will still face challenges to simplifying the accompanying complexity of information security management. Some of these challenges include:

- Communicating the need for information security effectively so that it is not seen as just a technology issue.
- Making information security seamless to end users.
- Staying abreast of new regulatory and legal requirements for information security activities.
- Making sure business partners are adequately securing the information that you have entrusted to their care.
- Keeping up-to-date with new information security risks, threats, and vulnerabilities.

Summary

For an effective information security program, a business must implement a multi-dimensional security program that includes the use of:

- Protection strategies
- Risk analysis and assessment
- Security policies, procedures, and standards
- Education
- Audit and validation
- Simplification of complexity

Establishing a thoughtful information security strategy based upon identified risks and managed by one enterprise role with responsibilities distributed throughout the enterprise help to simplify the complexity of addressing security and help to ensure an effective information security program. The next chapter will discuss the value of zoning to address these complex multi-dimensional information security issues and challenges.

Chapter 4: The Value of Zoning

Zoning to secure valuable resources is nothing new. The concept of creating security zones has been around for centuries. For example, countries have divided their lands into regions and applied military security protection to each region based upon the regional characteristics, value, population, and other various factors.

Security zones are also used to help protect valuable resources against acts of terrorism or other targeted violence. For example, airports mitigate their risks through the use of security zones. They divide the airport grounds, airspace, and facilities into specific zones in order to protect the critical sections of the airport from unlawful interference and to more easily manage the zone areas. Certain security controls apply within each zone. These may include actions such as establishing and maintaining barriers to protect the zoned area, restrictions on entry, and so on. Typically, an airport has an airside area and a landside area. The critical aviation operations are generally included in the airside area, where security is more tightly regulated. These zones may be established for a range of reasons, including the control of people movement, prevention of interference with aircraft, and restriction of access to critical facilities.

Using security zones in these ways not only makes management of security more effective and efficient but also helps to decrease the overall cost of security by creating scalable protection for zones based upon the risks of each zone. Organizations can learn from these practices and apply these same concepts of creating security zones to their own enterprises to protect their information and network resources more efficiently, effectively, and economically. As discussed in earlier chapters, securing only the perimeter will not provide defense against new attack methods and threats such as:

- Social engineering
- Zero-day vulnerabilities
- Malicious email and Trojan horses
- Worms
- Insider attack and fraud
- Rogue wireless and modem connections

Regulatory Implications for Zoning

Recent surveys reveal that most customers still do not trust companies to handle their personal information responsibly. An October 2005 Ponemon Privacy Survey indicates the customer and opportunity losses associated with information breach events cost a company significantly more than the actual breach events themselves. A March 2005 Ponemon Privacy Trust Survey of more than 2300 adult Internet users in the United States reveals that customers who have a high level of trust in their banks are more likely to do online banking tasks and to remain loyal to the bank they trust. Fifty-seven percent indicated that they would stop using online services if a single privacy breach occurred.

Reflecting consumer mistrust, several governmental regulations have emerged that legislate security and build consumer trust. The laws are complex and failure to follow regulation can result in huge fines, penalties, and even prison time for offending executives. Business leaders must not only be aware of but also strive to be in compliance with the multitude of regulations that are applicable to their companies. This complexity can be made more manageable and companies can more clearly provide demonstration of due diligence by tackling the requirements in zoned chunks across the enterprise. Table 4.1 highlights a few of the regulations and high-level requirements as well as the implications for zoning to make compliance with multiple regulations more manageable.

Regulation	General Requirements	Implications of Zone Security
United States Gramm-Leach-Bliley Act	Administrative, technical, and physical safeguards to protect personal information Privacy notices and opt-out provisions Safeguards and monitoring against future threats Responsibility for ensuring secure outsourced security solutions	Increased storage volume and secure backup storage as well as increased network and storage security Data encryption at source Company-wide policies, risk assessments, and reports Enterprise-wide monitoring
United States California Senate Bill 1386	Disclosure of security breaches in which unencrypted (clear text) personal information may have been accessed by an unauthorized person Procedures to identify and contact persons affected Due diligence in protecting customer information from unauthorized access	Data encryption at source and throughout data life cycle Network and storage security at information repositories Quick and comprehensive identification of personal information storage locations Intrusion detection for access to personal information storage locations
United States Sarbanes-Oxley Act	All documentation used for financial reports and audits as well as all transactions and meeting minutes must be saved Data must be retained for 5 years Ability to locate and recover documents in a few days	Increased storage volumes and distributed storage locations Indexed document retrieval from primary and backup media Secured Write-Once, Read-Many (WORM) storage Restricted access for only personnel with a business need Disaster recovery including geographically dispersed and/or isolated synchronized storage
United States SEC Rule 17a (Books and Records Rules)	Non-rewritable, non-erasable, time-stamped, duplicate message storage Third-party download and storage service Fully indexed and searchable messages Data retention for 6 years, with the first 2 years being in faster storage Ability to provide a copy of any message upon SEC request Collect certain account records and customer information and verify the information with customers	Increased primary and WORM storage volumes Improved indexed message retrieval from primary and backup media, with query/report tools Third-party security Customer access to their corresponding information

Canada Personal Information Protection and Electronic Documents Act (PIPEDA)	Consent before disclosing personal information Well-planned and documented privacy policies made known within the company Information sensitivity and security levels Data retrieval on demand by customer or law enforcement Data retention only as long as required by law	Company-wide policies, risk assessments, and reports Procedures for gaining customer permission to disclose private information Increased secure storage volume Indexed document retrieval from primary and backup media Security based on levels of sensitivity
European Union Data Protection Directive	Personal data must be processed fairly and lawfully and obtained only for specified purposes Data subjects must be told how their personal information will be used and with whom it will be shared Personal data must be accurate, adequate, relevant, and not excessive for the purposes for which it was collected, and not be kept for longer than is necessary Appropriate technological measures must be taken to stop personal data being hacked, lost, damaged, or stolen Personal data cannot be transferred outside the European Economic Area unless the country to where it is transferred provides an adequate level of protection	Company-wide policies, risk assessments, and reports Information and network intrusion detection and prevention Improved indexed message retrieval from primary and backup media with query/report tools Provide access to individual's information upon their request Isolate personal data within only approved countries
Japan Personal Information Protection Law	Take measures to prevent personal data from being accessed or stolen Provide consumers with specific notices, obtain consent, provide information regarding their corresponding information in a timely manner, and allow information subjects to request corrections Cannot handle personal information beyond the stated scope Controlling access of personal information to third parties except as specifically indicated and allowed by the information subject	Company-wide policies, risk assessments, and reports Information and network intrusion detection and prevention Improved indexed message retrieval from primary and backup media with query/report tools
United States Health Insurance Portability and Accountability Act (HIPAA)	Administrative, technical, and physical safeguards to protect health information Privacy notices Safeguards and monitoring against threats Responsibility for ensuring security with third parties	Information and network intrusion detection and prevention Increased storage volume and secure backup storage Increased distributed network and storage security with internal firewalls Data encryption throughout life cycle Company-wide policies, risk assessments, and reports Enterprise-wide monitoring

Table 4.1: Regulations with zoning implications.

Why Network Security Zones?

The quality of a network's security is an essential component of the security posture; it connects applications, systems, and users. The network should provide a solid first layer of defense against outside attacks, complementing operating system (OS) and application-level security. Separating the network into virtual compartments, or zones, allows security managers to consolidate resources in a cost-effective manner and control user access to each application and related information. The network then creates a secure environment not only at the perimeter but also in security zones throughout the enterprise.


Security zones can contain the spread of an attack and provide strong access controls.

Original Zoning Simply Protected the Enterprise Network

The concept of network security zoning really became widely critical in the 1990s when exploding numbers of organizations began connecting to the Internet. In doing so, they realized, sometimes through brutal business-impacting results of security incidents, that security was needed between the corporate network and the wild and untamed Internet. This realization resulted in the widespread use of demilitarized zones (DMZs) at most security-conscious organizations. The DMZ protected the organization's information and network assets by connecting through them through a firewall. Basically, the network became one large security zone, and the DMZ became another, less-trusted filtering security zone, as demonstrated in Figure 4.1. The connections to business partners largely were made without any additional security applied, creating huge vulnerabilities that were by-and-large unbeknownst and/or unconsidered within the organization.

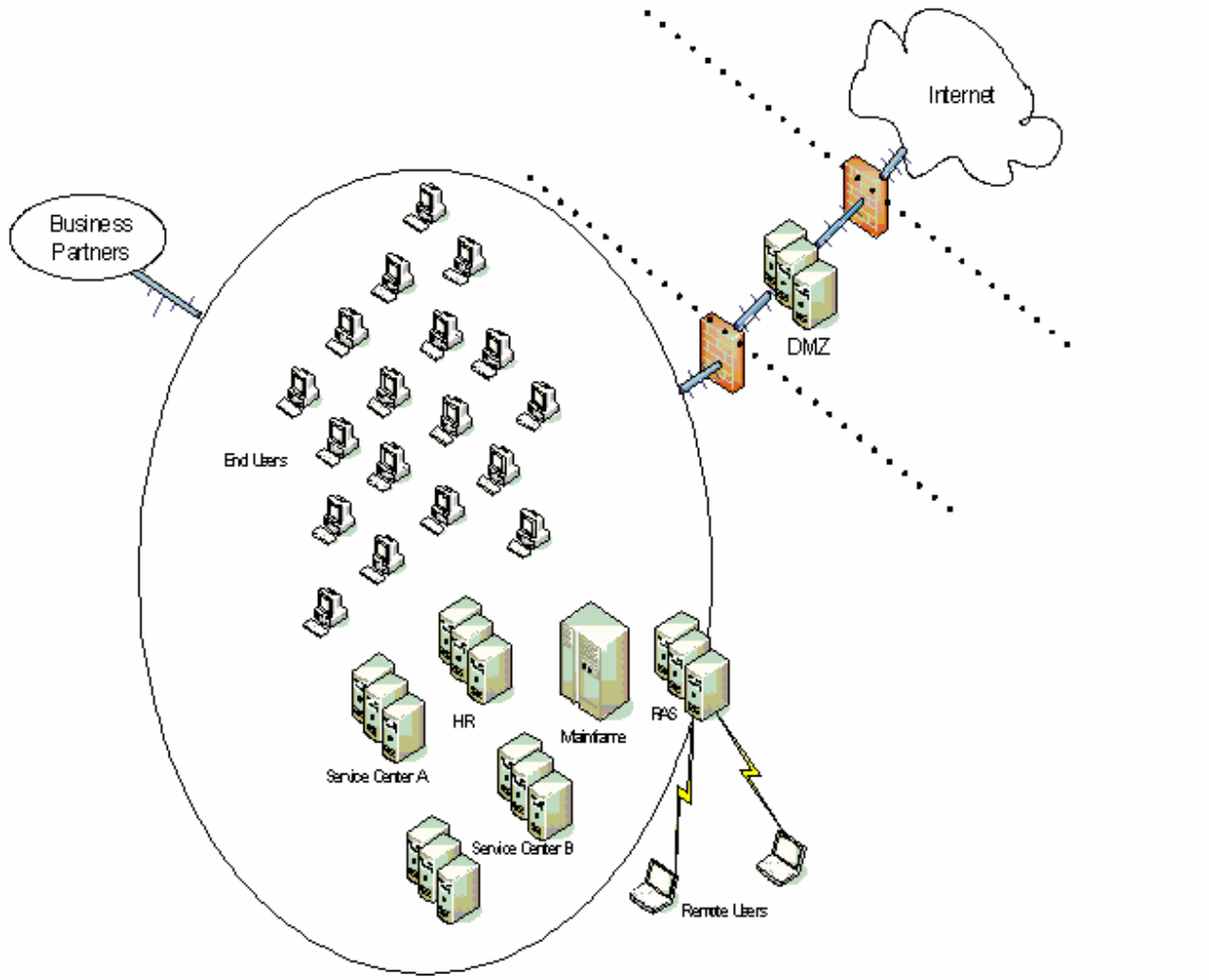


Figure 4.1: Typical early zoning with the internal network all in one zone.

Security Zones Should Now Be Built to Fit the Business

As zoning has evolved, it is increasingly used for creating security defenses between departments or other logical divisions of services and products. For example, the marketing department typically has hosts and subnets with many security and access controls in common. These hosts and networks can logically be grouped into their own zone simply called Marketing.

When there is a need for exceptions or other special cases, perhaps when one or more hosts belonging to the zone needs specific or more restricted access, explicit policy rules can be created within the host or subnet level, again without compromising security. Security zones allow for easy consolidation of environments in which multiple distributed security defenses are currently used for security segmentation. This consolidation offers significant cost savings, reduced administrative burden, policy enforcement, and clearly defined trust domains—all of which are the primary drivers behind consolidation.

So why isn't network security zoning more widely embraced if it is such a good idea? The most common reason IT analysts give is that up until recently the only way to employ security zoning was with hardware—by either installing firewalls or VLANs and subnets throughout the network. These methods alone were cumbersome to manage and created a certain level of inflexibility. As the internal threats, risks, and vulnerabilities were not fully understood, they felt that as long as the perimeter was secure, the inflexibility wasn't worth the perceived gains. However, with an increasingly porous perimeter, and more knowledge and understanding of insider threats, the value of establishing internal network security zones is being recognized as valuable. There are also many new and emerging products to allow the network to be zoned from a software point of view instead of just a hardware standpoint, effectively addressing the inflexibility of the older hardware-only solutions.

Enterprise Management Implications for Zoning

Over the years, within the typical organization, the network grows and security is deployed within various departments as it is needed. This network growth often accompanies rapid company growth, disparate geographies, and numerous new technologies, usually with no combined effort to consolidate the varying security components and layers into a single enterprise strategy. Dependence on the network along with functional enhancements to the business systems increases the importance of security and dependable accessibility to information. This uncoordinated application of security whenever it is needed, without any forethought to support or management, results in extremely costly and difficult-to-manage systems with gaps in security throughout the network. Implementing network security zones can help organizations achieve their goals of scalability, availability, security, manageability, performance, supportability, and geographic distribution, while realizing savings at many levels throughout the enterprise.

Zoning Streamlines Business Processes

Creating effective security zones throughout the enterprise will not only decrease the total cost of ownership (TCO) for the IT infrastructure by eliminating wasteful redundancies and establishing consistent standards but also has the added benefit of creating an efficient management layer of protection through thoughtful and effective network and systems segmentation.

Security zones enable organizations to:

- Allow for more efficient audits and compliance reviews
- Decrease operating costs
- Ease the challenges for security policy enforcement
- Enable better geographic security distribution
- Improve network security manageability
- Improve network security scalability
- Improve physical security defenses and management
- Increase network performance
- Increase overall network availability
- Optimize resource allocation
- Provide more efficient security systems supportability
- Reduce software and hardware requirements for security tools and systems
- Respond more quickly to network and systems threats

Zoning Mitigates Risk Within the Network Perimeter

Providing compartmentalized security throughout the enterprise through the use of security zones is a tried and true way to mitigate risks within the perimeter. Security zones proactively defend against vulnerabilities, minimizing unauthorized access, intentional and unintentional.

Zones Lessen the Impact of Zero-Day Attacks

Consider the impact of "zero-day" malicious code attacks. "Zero day" refers to an attack, usually through a malicious code exploit, such as a worm or a virus, that makes use of previously unknown vulnerabilities. Zero-day exploits typically start attacking systems at the same time as, or even before, the public announcement of a vulnerability in a computer system. Reactive defenses, such as signature-based virus scanners and automated patching systems, are still necessary, but they are ineffective against zero-day attacks.

By using security zones, such zero-day attacks can be more successfully contained within the zone of origination, isolating the attacks and the compromised device. Confining an attack to one or a few zones allow other network security zones to continue to support business as usual.

Zones Lessen the Impact of Insider Attacks

As discussed earlier in this guide, there is great threat to information resources from insiders who have authorized access. Insiders may threaten an organization's interests by disclosing sensitive or classified information, making decisions that have a negative impact on the business, or exacting a network attack. Establishing security zones throughout the enterprise can help to contain the impact of any insider attack to only the zone within which they are located.

Authorized users with privileged access may attempt to access unauthorized resources, perform Denial of Service (DoS) attacks on shared resources, or delete or modify shared data sets. Establishing security zones throughout your enterprise network will prevent such attempts from going beyond the security zone into another where the user has no authorization.

The situation is particularly dangerous when a legitimate user's authentication credentials (password or keys) are stolen, allowing an attacker to masquerade as a legitimate user. Such masquerade attacks can lead to further damage beyond the initial compromised account and there is little indication of a problem to security systems administrators. Establishing security zones will help to limit the damage to only one zone within the enterprise and save the rest of the enterprise zones from the destructive impacts.

Zoning Saves Organizations Time, Money, and Human Resources

When considering the deployment of security zones, wise business leaders must consider how the implementation of what at the onset seems to be a huge investment, in reality will save the organization time, money, and human resources in the long run.

According to a 2005 Gartner Group study, the average downtime cost for businesses across all industries is more than $1 million per hour. In addition, according to a 2005 Wall Street Journal report, more than 83 percent of all critical data lost is due to some form of human error, 64 percent from human mistakes and 19 percent from internal sabotage within an organization.

So where can savings be realized? Measure the gains in IT staff and user productivity from deploying the solution as well as the revenue recaptured from reduced downtime, the cost savings from increased IT staff efficiency, fewer security incidents and associated response costs, and lower capital and operating expenses. The following list provides examples of ways in which network zoning will save organizations time and money resources:

- IT productivity savings—Zoning can help improve IT staff productivity by allowing security to be managed and addressed on a zone-by-zone basis as opposed to the common way of managing on a server-by-server and node-by-node basis. Besides reducing operations costs, gains in IT productivity can free up staff to implement new initiatives more rapidly, helping to create a competitive edge.
- User productivity—When users are unable to access network resources, their productivity is likely to be severely impaired. Users often are able to move to other business applications when service interruptions or performance degradations occur. Zoning will improve system uptime and user productivity by confining problems to as few zones as possible while allowing other zones to remain in full production mode, providing areas for those affected in one zone to continue their work in another unaffected zone.
- Recaptured revenue—Higher system availability contributes to businesses' top lines because less revenue is lost due to downtime and potential service penalties are avoided. Downtime can also be costly in terms of diminished customer satisfaction and possible loss of a customers' business. Security zoning can contribute to recaptured revenue by isolating security problems to one part of the enterprise to more efficiently be responded to while allowing the other zones within the enterprise to continue providing service and products.
- IT efficiency—IT staff efficiency can be described as a measure of how well the IT management organization can achieve economies of scale and scope of work with its people, tools, and practices. Companies must be able to grow their systems and networks at a faster rate than the IT staffs required supporting them in order to remain competitive. Experienced and knowledgeable IT professionals continue to be scarce, resulting in existing staff taking on more work and responsibilities, including more and more security management activities. Establishing security zones helps IT departments to achieve economies of scale and scope to better manage with fewer staff and resources, while at the same time gaining a competitive advantage.
- Other cost savings—Additional cost savings may be realized by eliminating other security management tools that have historically be used on a server-by-server and system-by-system basis, and instead use tools designed to effectively manage security within established security zones.

Security Zoning Reduces Operational Risk

Security controls must be in place to safeguard all operations of enterprise information facilities and systems. Operational security controls must ensure that risks to information integrity, availability, and confidentiality are minimized in the operational environment, in online service delivery, and in exchanging information by any means in the internal or external information environment. Zoning can enhance and improve the efficiency of security and risk reduction for these operations. The following sections provide examples of operational activities that can be enhanced by security zones.

Zoning Protects Against Viruses and Malicious Code

Organizations must ensure that security controls are in place for the protection of information and systems against viruses and other malicious code. Controls must include prevention, detection, removal, and reporting of attacks of malicious code on the information environment. Incorporating zone-based virus and malicious code prevention can help improve the effectiveness of the controls and help protect zones when outbreaks occur in other zones on the network.

Zoning Improves Systems Maintenance

Organizations must develop processes to ensure the availability of information and information systems, networks, and applications in the event of failure or unforeseen loss of information. Processes must be established that include comprehensive information backup procedures. Operator and fault logs must be implemented to monitor the integrity and availability of information, information systems, networks, and applications. Efficiency is improved by implementing logs and maintenance within zones. This task is accomplished by limiting the scope of the logs and, as a result, making maintenance less labor intensive, allowing multiple groups to focus just on their areas of responsibility.

Zoning Improves Network Management

Organizations must establish security controls to protect networks and infrastructures from unauthorized access and to safeguard information confidentiality and integrity. To ensure the integrity of networks, privately owned devices (for example, home computers) must not connect to enterprise networks unless detailed risk assessments are conducted to determine all security impacts and any additional security measures are in place to ensure the highest level of information security. Assessment must include all aspects of information security (for example, authentication measures, access controls, virus and malicious code protection, physical and personnel security). Establishing such measures and controls and performing such assessments within identified security zones helps to streamline the security process and limit the scope to only the area of the network for the management process.

Zoning Enables Secure Exchange of Information and Software

Methods for exchanging information between an organization and business partners or third parties must be consistent and secure to meet legal and regulatory requirements. When network information is exchanged, it must be protected according to the level of classification. By creating security zones, an organization can more easily and efficiently manage the information within each zone as well as ensure each piece of information is appropriately classified. This setup then enables the information to be shared with third parties and business partners in the most appropriate way. For example, a zone can be established to exchange information with a high-risk third party so that the accompanying risks to rest of the network will be minimized as much as possible.

Zoning Makes Reporting Security Incidents More Efficient

Formal processes must be in place to report security incidents and weaknesses as quickly as possible to appropriate positions, such as the corporate information security officer and/or corporate privacy officer. Dividing the enterprise network into security zones can allow for more efficient and timely monitoring of security incidents on a zone-by-zone basis and report to the most appropriate position based upon the zone within which the incident occurs.

Zones Physically Protect Information Assets

Physical and environmental controls are also an important component to protecting enterprise information and systems. Without sufficient physical and environmental controls, you could experience a complete network failure. To help prevent network interruptions and inappropriate access to information resources you need to:

- Ensure adequate climate control, such as monitoring temperatures and humidity of information systems equipment
- Store all backup media at a secure offsite location
- Protect network equipment and information media from water, fire, and other environmental hazards
- Use power interruption controls to ensure continuous, consistent electricity
- Control physical access to computing equipment
- Ensure only authorized persons can enter areas in which sensitive information and network components are located

Environmental failures and physical events can cause considerable damage to information systems and business processing. Such threats can be natural or man-made. Mitigating the risks from these threats can be approached using zoning techniques in the same way that zones can be established within the network.

Implementing a strategy for physical protection is an important step to include within any effective enterprise information security plan. Zoning can be used to establish efficient and effective physical information protection.

Traditionally, organizations considered zoning to basically consist of installing fire alarms and fire suppression systems within each room. However, physical zoning to complement network security zoning efforts goes beyond this. Physical zoning can facilitate the simplest to the most detailed security model. The components of security devices implemented within each identified security zone may include:

- Smoke and fire alarms
- Motion detectors
- Physical intrusion detection alarms
- Closed circuit television (CCTV) systems
- Physical barriers
- Locks and safes
- Break-proof glass
- Temperature and humidity control
- Halon and other waterless fire suppression systems

Physical security zones can be based upon similar requirements as network-based zones. For example, physical zones can be role-based. In such a plan, users are assigned to access physical areas, systems, data, and other components based upon their job responsibilities and assigned roles. Figure 4.2 provides a basic example of using role-based physical security zoning for access control. In this example, the zones are labeled 1 through 7. Each zone has unique threats, risks, and vulnerabilities. Zone 1 is the least restrictive, being open to the public. Zones 5 and 6 are the most restrictive, containing the operations equipment and all the customer data. Everyone within the building has access to the areas within Zone 7. Only authorized personnel have access to Zone 3, the executive office. Zone 4 is restricted to only personnel performing test and development activities.

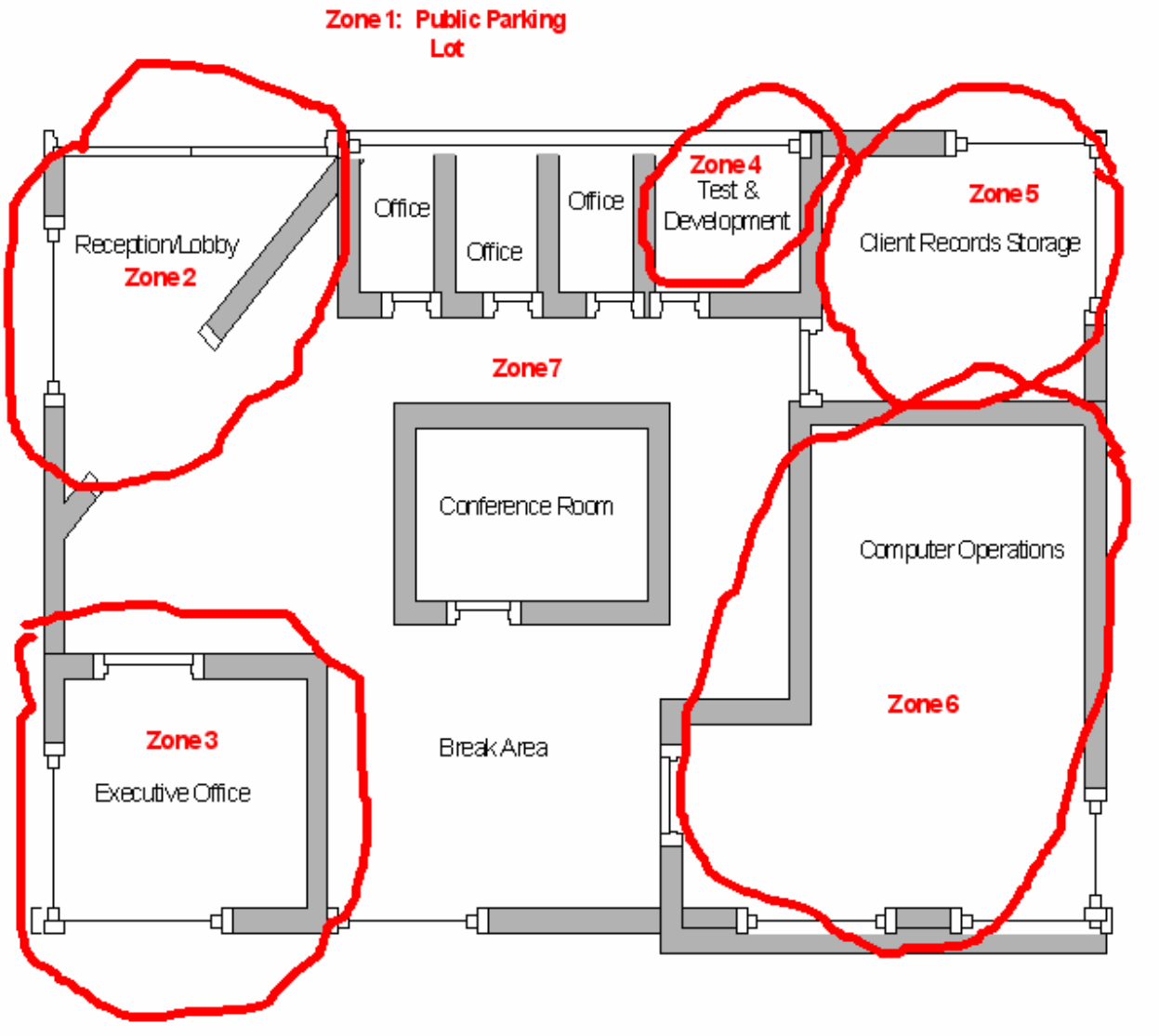


Figure 4.2: Example of physical security zoning.

Conduct a risk analysis to understand the physical threats, vulnerabilities, and risks, then use this information to build a risk mitigation strategy that includes identification for where physical security zones are needed. Once you have decided where your physical security zones should be located and how restrictive access to each should be, you then need to determine the controls to support the security zones.

> ☞ The more restrictive the zone, the stronger and more reliable the controls should be.

By combining physical zones with network security zones, organizations can create an effective centrally managed defense to protect information and assets.

Start to Think About Zoning

Business leaders can translate the broad concept of using security zones as discussed within enterprises at a very high level by:

- Identifying relationships between departments and determining how they share information and how they trust each other
- Identifying critical enterprise information and network assets
- Creating an inventory of these assets
- Identifying security zones by grouping the assets and identifying key processing areas
- Creating a road map to implement the security zones, based upon criticality, over a practical period of time
- Determining and implementing zone-specific protections

The following sections explore at a high level the concepts of creating and implementing security zones to help guide enterprise leaders in overseeing such activities within their organizations.

Identify Critical Enterprise Information and Network Assets

Create a list of critical enterprise information and network assets, then document the ones essential to the reliable and necessary operation of the enterprise. Follow a documented, risk-based process for your identification methodology. Establish risk-based criteria that correspond to the unique environment, requirements, services, and products of your organization.

> ☞ Most organizations have a control center and backup control center that are considered critical enterprise assets.

The computers and networks that provide the data and information to drive decisions made in the control center will typically be considered critical assets. Some organizations will have a very long list of critical assets. They will often be based within business units and critical corporate activity centers.

> ✎ Identifying critical information and network assets will require the participation of personnel from all facets of the organization.

The following list highlights examples of critical information and network assets:

- Customer information
- Web servers
- E-commerce applications
- Firewalls, routers, and other network security components
- Employee data
- Business transaction logs

As of September 2005, the North American Electric Reliability Council (NERC) is currently drafting wide-ranging cyber-security guidelines to replace their temporary precautions adopted as NERC Cyber Security Standard 1200 in 2003, renamed NERC Cyber Security Standard 1300 in 2004. This new set of guidelines, NERC CIP, will be finalized in Spring 2006 and establishes standards in eight key areas:

- Provisions for identifying critical cyber assets
- Developing security management controls
- Implementing training
- Identifying and implementing perimeter security
- Implementing a physical security program for the protection of critical cyber assets
- Protecting assets and information within the perimeter
- Conducting incident reporting and response planning
- Crafting and implementing recovery plans

Create an Asset Inventory

Creating an inventory and corresponding classification of critical enterprise information and network assets is a critical step in creating security zones. It is also an activity that should have been done already to facilitate business continuity processes and comply with various regulatory requirements for identifying and protecting certain types of information.

Typically, such an inventory and classification of criticality is created during a business impact analysis during the creation or update of a business continuity plan.

The types of resources typically included within a business impact analysis include:

- Personnel
- Facilities and associated specific locations
- Technological platforms, including traditional, e-commerce-related and network management systems
- Applications and systems software
- Data networks and equipment
- Voice networks and equipment
- Wireless networks and equipment
- Vital records
- Personally identifiable information
- Supply chain partners and associated data and network components
- Business processing outsourced vendors and associated data and network components

The 2004 TechRepublic State of IT Asset Management study of 497 organizational responses revealed:

- 10 percent do not have an IT asset inventory
- 51 percent use the most rudimentary asset management tools (spreadsheets and discovery tools) to maintain an IT asset inventory
- 19 percent use a repository integrated with discovery tools to manage inventory
- 13 percent manage the IT asset life cycle with defined processes, automated workflow, and integration
- 7 percent use a mature IT asset management model

Asset inventory and categorization will also help auditors and compliance regulators to better understand how the security threats on a low-priority system or zone are different and require different levels of security than the security threats on a high-priority system or zone. Not only will such an inventory and categorization improve the reviewers' understanding, it will also help to reduce the time necessary for the review, which will then result in a positive impact on your organization's bottom-line.

The information within a zoned area of the enterprise network for development systems will likely be lower priority than the customer information located within the zoned area of the enterprise network for production ecommerce systems.

Identify Security Zones by Grouping Assets

Divide the data center into areas that are logically separated from one another based upon their associated critical assets and revenue areas to contain an attack at minimal impact to the overall business. Zones can support individual applications or application tiers, groups of servers, database servers, Web servers, e-commerce zones, and storage resources.

Examples of security zones created through grouping assets include limiting user access to Web servers, such as through the use of a Web front-end, protecting the application and database tiers from accidental or malicious damage. In addition, communication between applications can be limited to specific traffic required for application integration, data warehousing, and Web services.

Security zones can provide logical separation of each application's storage environment across a scalable, consolidated storage network. To achieve this setup efficiently, firewalls can be integrated and virtualized to provide secure connectivity between application and server environments

Zone Development and Production Environments

Segregate business-critical development and production facilities to reduce the risk of accidental changes or unauthorized access to production software and business data. Development and testing activities can cause unintended changes to software and data sharing the same computing environment. Use zoning to manage these risks.

When creating zones take into consideration that

- Development and production applications should run on different processors or in separate domains or directories \
- Development and test work should be separated at a logical level
- There are (or should be) rules governing the transfer of software from development to production
- Software version controls may reside in different zones
- System utilities (such as compilers and editors) should not be accessible from production systems

Zone Business Partners

The risks of using external service providers, connecting to business partners, and otherwise sharing information and network resources with third parties should be assessed and documented. Connecting to or using third parties for managing or processing computer or network facilities increases the risks to an organization's information security. Just look at the number of incidents that have occurred through third parties in just the past 12 months, as described in previous chapters.

Appropriate information security measures, both technical and non-technical, should be incorporated into contracts before a third party connects to an organization's network or starts processing an organization's information. Use this contract information to create security zones for the business partners that address the unique risks presented by each.

Zone by Business Units

Many organizations find after identifying critical information and network assets that it is most advantageous and efficient for security management to create security zones based upon business unit services and products.

Create a Road Map to Implement Security Zones

After the security zones are identified, a road map needs to be created to ensure the efficient and effective implementation of the security zones into the enterprise, based upon criticality, over a reasonable period of time. Integrate the security zones into the existing enterprise network. Define the access and security requirements for every service so that the network can be divided into security zones with clearly identified security and access levels.

Work with each security zone separately. It is likely each zone will have a different security model necessary to address the identified risks. Security controls should be implemented so that security breaches and incidents can be confined to a particular zone or part of the network as much as possible.

> ☞ Implement security zones in such a way so that they will limit the damage a security breach or incident has on the entire network.

In addition, security zones should take into consideration the network security architecture defining common security services that are implemented across the network. The following list highlights typical services:

- Password authentication, command authorization, and accounting
- Virtual private networks (VPNs)
- Access control systems
- Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs)
- Encryption systems
- Third-party application service providers (ASPs)

Recognize the optimal varying levels of control within the security zones to identify clients and zone users, protect your zone perimeters as well as network perimeters, protect confidential information from eavesdropping or tampering during transmission, and ensure the integrity of your system and applications. Such decision making will involve not only IT staff but also information security, business unit contacts, and internal audit. After you have made the difficult decisions for the types of security to deploy within the zones based upon the risks within each of the zones, deploy the security architecture in phases, addressing the most critical zone areas first.

Implement Zone-Specific Protections

The road map for establishing and maintaining security zones will likely include a diagram representing the zones. For example, Figure 4.1 from earlier in this chapter may now look like Figure 4.3 after the decisions have been made about where to establish the zones.

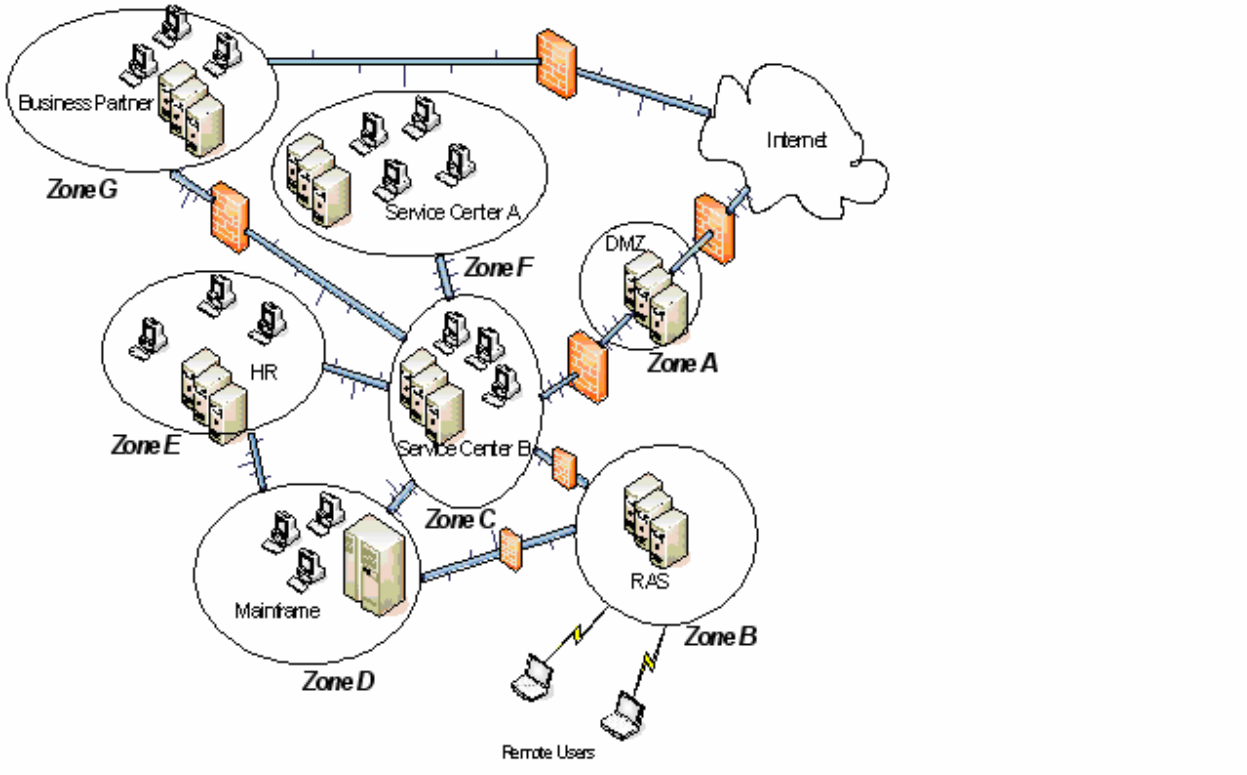


Figure 4.3: Example of zoning within the network.

Each of the identified security zones need to have controls and protections implemented based upon the risks specific to that zone. It is likely all zones will have similar protections, such as virus control systems. However, it is also likely that zones will have unique controls that no other zones may have, such as a zone with a remote access server (RAS) or a zone that houses a credit card processing system. There will probably be zones that have firewalls protecting them, and other zones that have no firewalls.

Steps to building a security zone include:

- Asset identification and classification
- Business impact analysis
- Asset prioritization
- Creation of manageable security zones (compartmentalization)
- Hardened security zones based on criticality using firewalls, filters, and access controls
- Deployment of in-depth and diverse defenses
- Security zones monitoring
- Assessment then remediation of vulnerabilities

☞ The key to successful zoning is thoughtful analysis of the risks within and to each zone, then the application of the most appropriate security controls for each zone's risk.

Integrate Security Zones Within Your Layered Security Strategy

By implementing security zones, an organization will shift reliance from perimeter security to an asset-centric model that protects the enterprise assets from the most likely threats with the most efficient measures. Security zones allow assets of greater organizational criticality and value to be held to higher security standards and protected by additional layers of defense. If possible, they should be compartmentalized, or zoned, into their own networks and segments. By doing so, the perimeter will be considered an asset.

Do not stop at just zoning alone, though. Zoning is just one of the layers to use within an organizational security strategy. To successfully defend against the multiple and varied types of threats and address the numerous and diverse vulnerabilities, organizations need to create and implement a layered security strategy. Perimeters, infrastructure devices, OSs, applications, and data must be assessed and appropriately fortified to mitigate the risks that threaten your organization. Use multiple complementary approaches for security enforcement and defense at various points in the network, which will remove single points of security failure.

Chapter 5 will discuss the need for a layered security strategy in detail. For now, the following list outlines at a high level a layered security strategy, including security zones:

- Obtain executive management support—An information security program must have the visible backing of upper management to be successful. Personnel follow the example of their leaders; if they clearly see upper management supporting information security efforts, they will also do so.
- Address legal and contractual requirements—An information security program must include activities that support privacy and information assurance requirements that exist within the wide range of enterprise contracts and are required by applicable laws and regulations throughout all the locations where the organization has offices and does business with partners and customers.
- Include personnel and processes into enterprise security planning—Effective security policies and procedures, security awareness and training, and consistent policy enforcement ensures a stronger, more efficient security program. You cannot expect security policies and procedures to be followed effectively, efficiently, or consistently unless the people using information resources have been told what they are and truly understand how to follow them.
- Clearly define user roles within security zones—Use both technical and non-technical security tools and control mechanisms—such as firewalls, IDSs, filters, access control capabilities, physical barriers, and alarms—to enforce access policies between security zones, giving only those with a business need access.
- Implement strong authentication methods to protect network and physical zones from unauthorized access and entry.

- Implement processes to maintain the integrity of the resources located on the network, servers, and end-user systems by doing such activities as
    - Hardening the OSs within the enterprise network and implementing ways to harden mobile computing devices
    - Disabling unused services
    - Applying patches as soon as possible, but only after testing and waiting for a timeframe when the risk of the change is reduced
    - Continuously protecting against malicious code, such as viruses, worms, Trojan horses, and spyware
- Secure endpoint computing devices that are connected, or sometimes connected, to the enterprise network—Create an inventory to account for all end-user computing devices, including wired and wireless. For instance:
    - Securing WLAN/Wi-Fi or Wireless Mesh communications using VPNs and WPA2
    - Securing devices that are often forgotten with regard to security, such as handheld computing devices (PDAs, Blackberries, and so on), smart phones, and mobile storage devices, such as USB thumb drives; such devices can contain a huge amount of personal information, intellectual property, and sensitive data, and are highly prone to loss or theft
- Protect the network administration and management information—Establish virtual LANs (VLANs) in conjunction with other security tools (such as IPsec, SNMPv3, SSH, TLS, and so on) to separate traffic between zones, allow only authorized access, and protect network resources, devices and applications, management and systems components. Be sure to implement backup processes for systems and device configurations and use a change management process to ensure only appropriate changes are implemented, in addition to tracking changes.
- Stay aware of your network traffic trends and the corresponding threats, risks, and vulnerabilities within each of the security zones—Monitor for threats, both outside of the perimeter and within the perimeter. Block invalid network activity and traffic using a variety of tools, such as DoS prevention, anti-spoofing, and logon blocking implemented at the security zone perimeters.
- Implement a wide range of security tools to create a blanket of protection against threats and protect mission-critical systems and applications—Keep your firewalls up to date to support new systems, applications, and protocols, such as SIP and H.323.
- Monitor the network security health by creating appropriate and sufficient logs—Analyze the logs and associate them with audited events to help ensure the most effective security management based upon current and relevant information. Summarize logs and events to create a network security health report with identified threat activity.
- Evaluate all established security zones to ensure they are still effective—Update the zones whenever necessary to improve upon security by addressing new threats, risks, and vulnerabilities.

Summary

Organizations should use security zones to more effectively and efficiently help protect valuable information and network resources against the multitude of threats within the perimeter as well as the increasing amount of threats from outside. The following checklist identifies considerations for security zone implementation:

- Identify critical assets and create an inventory to know and understand where necessary information and network resources are located.
- Perform a security assessment to identify vulnerabilities and risks, with specific breakdown by host, OS, application, data, network devices, and links. The assessment will provide information necessary for determining appropriate risk levels for each asset and the requirements for maintaining each one to the desired security level; this information should be incorporated into the security policy.
- Define security zones and set security levels for each zone. Use security zones to divide the network as well as the data center into areas that are logically separated from one another to contain an attack at minimal impact.
- Employ zones that support individual applications or application tiers, groups of servers, database servers, Web servers, e-commerce zones, and storage resources.
- Limit user access to and within security zones to specific servers, protecting the application and database tiers from accidental or malicious damage.
- Limit communication between applications to specific traffic required for application integration, data warehousing, Web services, and so on.
- Use security zones to provide logical separation of each application's storage environment across a scalable, consolidated storage network.
- Implement endpoint protection for critical servers and hosts. This protection can be used to discover attacks in progress, protecting not only the zone being attacked but also the OS and applications and sending alarms to the management console when an exploit is detected. Implement network IDSs for critical network segments and zones, analyzing traffic streams to identify DDoS and other attacks as well as hacker activity. Implement IPSs to stop attacks, but do so thoughtfully so that you reduce the risks that false-positives will kill a legitimate session.
- Control access between zones with firewalls and routers. Firewalls provide control for outbound connections from a zone and allow legitimate responses from the remote host.
- Implement VLANs to enable containment within security zones. When each host or segment has its own VLAN, security managers can quarantine attacks and prevent their spread to other hosts; hosts on each VLAN can communicate only with the default gateway, not with other hosts.

Chapter 5: Layered Security

Using just one tool or performing just one activity will not accomplish an effective information security program. An effective information security program consists of many layers. Using many different layers of many different types of security will most effectively protect the enterprise from the attacks and threats that exist from all directions and in all ways, both malicious and accidental, to information resources. This layered defense is often compared to the layers of an onion, creating many different types of security layers that must be penetrated before the target at the core of the onion (your critical information infrastructure) can be reached. Such layering establishes a more reliable security posture; if a failure or breach occurs in one layer, it will not compromise the other concentric layers.

Chapter 3 discussed the need for a multi-dimensional security program that includes the use of

- Protection strategies
- Risk analysis and assessment
- Security policies, procedures, and standards
- Education
- Audit and validation

Implementing security within these multi-dimensional layers appropriate to each of the zones discussed within Chapter 4 will provide a comprehensive enterprise information assurance framework within which organizations can then apply the appropriate tools and establish appropriate corresponding management activities. Taking the time to establish this framework may seem overwhelming at first, but doing so in a thoughtful way will truly result in simplifying the complexity of managing security and will distribute and incorporate security responsibilities throughout the enterprise.

Effectively layering security will incorporate security activities into all business layers throughout the enterprise.

The layers that comprise an effective information assurance program will consist of at least the following elements, in addition to any other elements an organization needs for its own unique and specific risks, threats, and vulnerabilities, as well as industry, regulatory, legal, and contractual requirements. These elements are essential because they cover logical security (networks, hosts, and programs), physical security (things that can be touched), personnel, and preventative and reactive measures:

- Security program management
- Application security
- Network security
- Node-level security
- Physical security
- Human resources security
- Monitoring and evaluation
- Disaster preparedness
- Incident response

When implementing these layers, organizations must carefully plan and implement to

- Make security as transparent and tolerable as possible
- Plan for effective enterprise-wide security integration
- Implement an effective information security education program
- Balance the activities for security with the business processes to achieve optimal security to address risks, but no more than is necessary

Always remember that information security should be implemented to most effectively support and protect the business, not to unnecessarily inhibit or disrupt the business.

Security Program Management Layer

The information security program is an information security layer that permeates multiple levels of the enterprise and benefits the organization in many ways. Every level enhances the entire information security program by making use of various types of expertise, authority, and resources. Generally, as a result of this layered security program management

- Executives will better understand the organization as a whole and have better knowledge to most appropriately and effectively use their authority to protect the enterprise information assets.
- Managers within each of the business and operational units will be more familiar and cognizant of the specific security requirements, including technical and procedural requirements and the associated challenges of the systems and information users.

Security initiatives are only effective when a framework exists that controls and manages information security activities throughout the organization.

Information security program management layers, when implemented most effectively for each enterprise's specific needs, will be complementary. Each layer will help the other be more effective for information security assurance.

Effectively layering the security management program will generally involve two levels of information security management:

- Centralized enterprise information security management with ultimate accountability and oversight responsibilities.
- Distributed information security management with various information security accountabilities spread throughout the enterprise business units, operations areas, and geographies.

Centralized Security Management

Establishing a centralized security management area with ultimate enterprise-wide security oversight will result in distinct benefits to organizations. It will increase the efficiency of security throughout the organization, allowing security to be implemented with an economy of scale that is more resource efficient than having security assigned independently to different groups. In addition, it will allow the organization to enforce security requirements centrally as well as to centralize monitoring, evaluations, and updates to the enterprise security program. Centralized security management should include the following components:

- **Clearly defined and documented accountable security program management responsibility**. The security program management function must be clearly defined and supported by enterprise management as being the area ultimately responsible and with the authority for instituting information security initiatives and enterprise requirements. This area must consist of stable resources and personnel who have the responsibilities and can perform the necessary tasks.
- **Enterprise information security charter**. An effective program must be based upon a documented enterprise security charter that clearly defines the function of the information security program and defines the responsibilities for not only the information security area but also the related enterprise programs and departments.
- **Enterprise information security policies, procedures, standards, and guidelines**. An effective program must include information security policies, in addition to standards, procedures, and guidelines as appropriate to address the information security needs of the enterprise and support the documented charter.
- **Information security strategies**. Effective information security management must have both short-term and long-term strategies to incorporate information security into the enterprise business functions as well as existing, new, and emerging technologies.
- **Compliance**. Effective information security management must address how non-compliance with the security requirements will be discovered and how the program requirements will be enforced.
- **Inter-departmental partnership**. Information security activities overlap with other operational areas such as physical security, quality assurance, internal audit, safety, and legal, just to name a typical few. Effective information security management will include established communications and partnerships with these areas to more successfully integrate information security into the management of the enterprise as a whole.
- **Liaisons with external entities**. Effective information security management must be knowledgeable and up to date on the latest trends and issues. This function should participate in outreach activities to obtain information from external sources to access more comprehensive information, ultimately resulting in more comprehensive knowledge and more resources to contact when situations arise that are new or particularly challenging to the organization.

Distributed Information Security Management

The enterprise information security management program will address the entire range of information security issues for the enterprise. Distributed information security management programs will help to ensure appropriate and cost-effective security is addressed within each of the organizational business and operations areas. Distributed information security management will incorporate security into their respective areas in the following ways:

- **Area-specific security procedures and guidelines.** Distributed information security management personnel will address the specific activities within the business area while at the same time support the enterprise information security program.
- **Manage incorporation of information security into the systems development life cycle**. Distributed information security management personnel will ensure appropriate and cost-effective security by ensuring security is built-in to their associated business processes from the very beginning, through systems launch, update, and retirement.
- **Manage integration of information security into the business unit operations.** Distributed information security management personnel will understand their areas, mission, technologies, and operating environments better than any corporate area. They will be able to most effectively integrate information security activities into the daily management of their departments and activities.

Application Security Layer

Information security controls built-in to business process applications are another important enterprise information security layer. Examples of how to build information security into applications include programming checks and controls for

- Completeness
- Accuracy
- Validity
- Authorization
- Data encryption
- Segregation of duties

Although the design and implementation of application security controls is typically the task and responsibility of the IT and engineering areas, the chosen controls must be based upon business requirements. The centralized and distributed information security management areas must define the requirements clearly and effectively to allow the IT areas to deliver and support the appropriate applications security services in addition to including successful links to the corresponding security within the supporting databases and infrastructures.

The centralized and distributed information security management areas should understand the following types of application control objectives in order to work most successfully and efficiently with the IT areas while they are creating and updating applications:

- Data authorization and origination controls
    - Data preparation—Procedures that IT follows to ensure consistency and completeness in data preparation activities; for example, input forms can be provided to help minimize, or perhaps even eliminate, errors and omissions
    - Source document authorization—Procedures to appropriately prepare source documents and sources and to adequately segregate duties between origination and approval of source documents
    - Source document data collection—Procedures to ensure appropriately authorized source documents are complete, accurate, accounted for, and transmitted for timely entry
    - Error handling—Procedures to ensure the detection, reporting, and correction of source document errors, problems, and irregularities in data collection
    - Retention—Procedure to ensure the original source documents are retained to the required and appropriate amount of time to meet regulatory contractual and litigation requirements, in addition to allow for retrieval or reconstruction of the data within a reasonable time following transactions
- Data input controls
    - Authorization—Procedures to ensure that only authorized personnel perform data input
    - Accuracy, completeness, and authorization checks—Procedures to ensure that the data entered for business transaction processing (whether it is generated by people, systems, or through other interfaces) are checked for accuracy, completeness, and validity; the procedures should ensure that such checks are performed as close to the data origination point as possible and produce accuracy metrics for each source to identify problems.
    - Data input error handling—Procedures to correct and then resubmit erroneously input data
- Data processing controls
    - Data integrity—Procedures to ensure separation of duties is maintained during data processing, along with verification procedures to appropriately update the control totals, master file, and other application resources
    - Validation and editing—Procedures to ensure processing, authentication, and editing validation (manual checks should be performed whenever automated checks cannot); it is also a good practice to sometimes perform manual and automated checks (manually checking a sample of data will confirm that the automated checks are valid)
    - Error handling—Procedures to identify bad transactions before they are processed and without unnecessary interruption of other transaction activities

- Data output controls
  - Handling and retention—Procedures to handle and retain output from applications; such procedures must incorporate privacy and security requirements from applicable laws, regulations, and contractual requirements
  - Output distribution—Procedures governing how to distribute applications output; to be effective, these procedures need to be clearly documented, communicated, and enforced
  - Balancing and reconciliation—Procedures to balance output and relevant control totals; use audit logs to enable transactions processing to be traced, along with reconciling data disruptions
  - Review and error handling—Procedures to ensure that the area generating the output and appropriate persons using the report check the accuracy of the information; the procedures should include how to identify and handle the errors
  - Securing output—Procedures to ensure output reports are appropriately secured and maintained during the distribution period as well as after they have been delivered to the appropriate persons
- Boundary controls
  - Authenticity and integrity—Procedures to appropriately check the authenticity and integrity of all information that originates outside the enterprise such as that received by telephone, within papers documents, and via fax or email
  - Transmission (via electronic methods) and transport (via physical methods) protection—Procedures to ensure appropriate and sufficient security to ensure accidental or unauthorized access modification or misdirection of sensitive information does not occur during information and report transmission and transport (for example, blocking out sensitive data on hardcopy that will be sent to an auditor, when the auditor does not need that sensitive data, using encryption, and so on).

Node-Level Security

Another important information security layer is node-level security. Leading practices to accomplish node-level security implementation use a combination of identification, authentication, and logical access controls. The current hot topic of identity management focuses on integrating these activities into the business environment.

Identity Management in a Nutshell

Identity management seeks to ensure that all types of network users, and their corresponding activities and capabilities on systems and applications, are uniquely identifiable. Identity management processes work to ensure user access rights to network resources and information are in line with each user's documented business responsibilities and needs. Identity management implementations usually involve a formal process implemented by information security personnel of assigning user access rights following requests by management and approval by systems owners. In addition, a central repository is maintained that defines user identities and access rights. Both technical and procedural methods are used to establish and keep user identification, authentication, and access rights up to date.

Identification and Authentication

Identification and authentication are important for preventing unauthorized user and process nodes from being able to access networks, systems, applications, and information. Access control mechanisms are used to differentiate between these users and processes to allow only those authorized to perform the activity they are requesting.

> It is not only a leading information security practice but also required by many laws and regulations to grant system users access to only those resources, information, and applications necessary to perform their job responsibilities. This setup is commonly referenced as access control based upon "least privilege."

Identification

Identification is the information the end-node user or process provides to uniquely distinguish their activities and capabilities. The most common form of identification is the user ID. However, there is also a need to identify devices, especially inside the perimeter where there can be a large number of headless servers, which Chapter 6 will discuss in more detail. Certificates are also frequently used to provide identification for users and devices.

> To create accountability for activities, organizations should not allow user IDs to be shared.

Authentication

Authentication is used in conjunction with identification to validate the entity using the identifier as truly the associated user or process it claims to be. There are three ways in which identification can be authenticated:

- Using something the user knows, such as a password or PIN
- Using something the user possesses, such as a token or smart card
- Using something with biometric characteristics, such as voice patterns or fingerprints

Network devices also need to have their identity validated. Certificates are the primary method used to authenticate the identity of network devices.

> The method of authentication is strengthened when more than one authentication method is used.

Logical Access Control

Logical access controls are system-controlled ways for a node (end user or process) to be explicitly enabled or restricted to do something with a computer resource—such as view, update, and delete. Logical access controls not only allow the user or process to have access to a specific network or system resource but also provide the specific type of access to the resource. Organizations should implement logical access controls based upon the information security policies that cover the corresponding systems, networks, and applications. Logical access controls should be based upon business processes and goals, with information security, operational requirements and ease of use incorporated into the control decisions.

Establish logical access controls upon the principle of least privilege, granting access to only the information resources necessary to perform business activities.

Network Security Layer

Although the Transmission Control Protocol/Internet Protocol (TCP/IP) is an important part of the network security layer, it is also important for business leaders to understand that security within the network information security layer goes beyond TCP/IP.

The open nature of TCP/IP complicates security implementation and makes it more challenging.

Security within the network layer must be incorporated into, and addressed, within many different components and using many different techniques. Networks can span many organizational and business partner boundaries. Organizations must understand and take into account the risks associated within the data flow as well as ensure that legal and contractual issues exist in harmony with the business services and practices. There will be the need for additional security to be applied within the network to protect sensitive information that passes through public and business partner networks and zones that are not trusted.

Organizations must have layers of security that are implemented within the appropriate network zones to ensure appropriate and effective security techniques and related management procedures are used to authorize access and secure and control information flows from and to networks.

Examples of network security tools and techniques include:

- Firewalls
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Network segmentation
- Malicious code prevention
- Remote access controls
- Encryption

Network Security Controls

Networks must be sufficiently and effectively managed and controlled using the following tools and techniques to protect the network and associated components from a multitude of threats and to provide security for the systems and applications that depend upon the network for business processing. There are a wide range of security controls within the network layer that business leaders must carefully consider:

- **Separation of duties—**Separate operational network responsibilities from the other computer authorization responsibilities. No single person should be able to access, modify, or use network assets without the separate authorization or detection from another distinct position or area. The initiation of a network change must be separated from the authorization of that change. When designing network controls, this collusion possibility must be considered.
- **Remote network access—**Clearly document and communicate the responsibilities and procedures for managing remote systems and how they connect to the network.
- **Data transmission protection—**Establish controls to protect and safeguard the confidentiality, availability, and integrity of data that is sent over public, shared, and wireless systems. Encryption, discussed in Chapter 6, is one example of an effective tool to protect data transmissions. The endpoint systems and applications must be protected from the threats these open networks present.
- **Logging and monitoring—**Determine the appropriate logging and monitoring necessary to record relevant security and network activities to enable successful security incident investigations, in addition to providing other necessary evidence for business processing. Logging and monitoring is also mandated and restricted by laws, regulations, and contractual requirements and aids troubleshooting. Audit trails created from logging and monitoring are becoming more important, not only for regulatory compliance but also to enable the correlation of multiple network activities throughout all security layers.
- **Management coordination—**Network security activities must be carefully coordinated with network operational management activities to ensure security is applied consistently throughout the network and information-processing infrastructure. Without effective communication and coordination, there could easily be conflicting activities taking place or the failure to accomplish necessary tasks because one area thinks another area is performing specific security activities. For example, without coordination, a system may never get backed up because two groups assume that the other is performing the backup.

Securing Network Services

Identify, and include within networks services agreements as appropriate, network security features, service levels, and management requirements for all network services. This task should be done with not only outsourced services but also the services provided in-house. Network services can range from simple to complex and include such things as:

- Provisioning network connections
- Private network services
- Value added networks
- Managed network security solutions such as firewalls and IDSs

Well-documented security agreements and requirements make it very clear the expectations the organization has for network security activities. Consider defining the following network services and security requirements:

- Monitor the management of the network security services
- Periodically and regularly audit the management and success of the network security services
- Implement technology—such as authentication, encryption, and network connection controls—based upon risk
- Specify technical parameters for secured connections with identified networks services to support the security and network connection policies and requirements
- Enable procedures to restrict access as appropriate to specific network services and applications
- Implement node-level security where appropriate, including the use of identity authentication and logical access controls

Physical Security

The physical information security layer is a very important component of information security that is often overlooked by information security practitioners. This aspect of information security is commonly left solely to the facilities security personnel. However, it is important in preventing unauthorized physical access, damage, and interference to information assets and resources to consider the physical security risks, threats, and vulnerabilities. Then work in partnership with physical security departments, end users, business partners, and other identified areas to ensure adequate physical security is implemented to protect mission-critical and sensitive information processing facilities. These information processing facilities and systems should be located within secure areas and protected by defined security perimeters; in addition, appropriate security barriers and entry controls should be applied. Data and processing centers need to be physically protected from unauthorized access, damage, and interference. Mobile information systems must be appropriately physically secured using a variety of methods.

> ☞ All information security physical protection methods need to correspond with the identified risks threats, and vulnerabilities as well as the corresponding potential business impact.

The following physical security controls can serve as a checklist to help you determine the types of controls to be considered and implemented as appropriate to the organization's industry, size, geographic locations, and regulatory and contractual requirements.

Site Selection and Physical Security

- Account for the risks of natural and man-made disasters
- Consider applicable laws and regulations, such as the United States Occupational Safety and Health Act (OSHA)
- Establish physical security perimeters (using things such as walls, card controlled entry gates, and manned reception desks), physical security zones (discussed in Chapter 4), location of critical equipment, and shipping and receiving areas to control physical access to information processing sites and buildings, restricting access to only authorized personnel.
- Establish responsibilities for monitoring and procedures for reporting and resolving physical security incidents.
- Ensure information processing building and site perimeters are physically sound.
- Put alarms and monitors on all fire doors on the security perimeter and test them regularly.
- Install physical intruder detection systems on all external doors and accessible windows, in addition to unmanned areas containing information processing resources.

Give special consideration to physical access security within buildings where multiple organizations are located.

Public Access, Delivery, and Loading Areas

Control the areas and access points where unauthorized persons could enter organization premises, such as in delivery and loading areas. If possible, isolate these areas from the information processing facilities to further avoid unauthorized access. Implement appropriate controls in the public access areas:

- Restrict access to a delivery and loading areas on the outside of facilities to properly identified and authorized persons.
- Design delivery and loadings areas so that supplies can be unloaded without obtaining access to any other parts of the building.
- Put alarms and surveillance cameras on external delivery and loading area doors. Keep the video according to applicable laws and contractual requirements, and store for analysis in case of an incident.
- Implement procedures to inspect incoming packages and materials for potential threats.
- Physically segregate incoming shipments from outgoing shipments.

Physical Entry and Access Controls

Access to organization premises, and often specific buildings and rooms, should be restricted to only those with a business need to enter:

- Justify, authorize, log, and monitor access to organization premises, buildings, and areas for all persons, including personnel, temporary staff, clients, vendors, visitors, and all other third parties.
- Record the date and time of visitor entry and departure. Supervise all visitors unless their access has been previously approved, and grant them access according to specific, authorized purposes.
- Ensure only authorized persons can access areas where sensitive information is processed or stored. Use authentication controls (such as access control cards with PINs) and keep an audit trail of all access.
- Require all personnel to wear some form of visible identification.
- Do not allow third-party support personnel access to secured areas or areas where sensitive information is located unless absolutely necessary for them to perform their job responsibilities, under which circumstances access should be authorized and monitored.
- Regularly review access rights to secured areas and update appropriately.
- Maintain a list of who has access control devices, such as keys and access control cards.
- Implement policies addressing how to protect the access control devices. For example, keys must not be kept in locks or hanging on the wall, and key cards must not be left unprotected on a desk.

Securing Offices, Rooms, and Facilities

Physical security for offices, rooms, and facilities should be designed and applied based upon the risk to the particular facilities and to the accompanying legal and contractual requirements. Consider applying the following controls:

- Implement applicable health and safety regulations and standards
- Site key rooms and facilities to avoid public access
- Do not make directories and internal telephone books identifying locations of sensitive information processing facilities accessible to the public
- Give only personnel with a need to know information about the existence of, or activities within, secured areas
- Avoid unsupervised working in secure areas not only to prevent opportunities for malicious activities but also for safety reasons
- Physically lock and regularly check unmanned secured areas
- Do not allow photographic, video, audio, or other recording equipment such as cameras in mobile devices into secured areas
- Document requirements and procedures for employees, contractors, and third parties to work within secured areas
- Use clean rooms when outsourcing processing of confidential and mission-critical information to third parties

When discussing protection of information processing that has been outsourced, a clean room typically means that all the computer machines and output devices—except for terminals—used by the third party are disabled. This does not allow for information to be copied, hard drives and handheld devices cannot be used to get information, and hard copies of information cannot be obtained. The servers are physically located in a completely different geographic area, so there is no way to get data from a clean room facility. In addition, personnel are physically searched when entering and leaving.

Environmental Security

Avoid as much damage as possible from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters. Information security activities must include the design and implementation of measures to protect facilities and processing equipment against these adverse environmental conditions:

- Install equipment to monitor and control the environment, including temperature, humidity, and power within processing areas.
- Design and apply physical protection to help protect against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters.
- Implement protections from security threats presented by neighboring premises, such as a fire in neighboring buildings, water leaking from the roof or in floors below ground level, or an explosion in the street.

- Store hazardous or combustible materials at a safe distance from secured areas.
- Do not store bulk supplies, such as stationery, paper clips, or other types of supplies that are commonly needed on a daily basis, within a secured area.
- Locate fallback equipment and back-up media at a safe distance from the facility, within a secured site, to avoid damage from a disaster affecting the main site.
- Install and appropriately place fire-fighting equipment. Periodically test or inspect the devices to ensure that they are functional.

Computer Processing Equipment Security

Organizations cannot depend upon facilities security alone to adequately protect computer-processing equipment—too many vital computer devices are mobile. Appropriate controls must be implemented to help prevent loss, damage, theft, or the compromise of assets and interruption to the organization's activities. The following controls should be considered:

- Protect all types of computing equipment from physical and environmental threats.
- Implement policies for computer equipment siting (placing in appropriate locations) and disposal.
- Implement special controls as necessary to protect against physical threats and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.
- Position information processing facilities that process sensitive data to reduce the risk of information being viewed by unauthorized persons during their use, and secure all types of storage facilities and areas to avoid unauthorized access.
- Isolate computing equipment that requires special protection to reduce the general level of protection necessary.
- Implement controls to minimize the risk of possible physical threats, such as theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.
- Establish policies addressing eating, drinking, and smoking in proximity to information processing facilities and equipment.
- Monitor environmental conditions, such as temperature and humidity, for conditions that could adversely impact the operation of information processing facilities.
- Install lightning protection to all buildings and lightning protection filters to all incoming power and communications lines. Be sure to include remote processing areas, such as home workers.
- Consider using special protection methods, such as keyboard covers, for computing equipment in industrial environments.
- Protect equipment processing sensitive information to minimize the risk of information leakage due to emanation.

Supporting Utilities

Organizations depend upon power to keep information processing and computing facilities going. Protect processing equipment from power failures and other disruptions caused by failures of supporting utilities:

- Regularly inspect support utilities and test, as appropriate, to ensure proper functioning and reduce risk from their malfunction or failure.
- Provide electrical supply that conforms to the equipment manufacturer's specifications.
- Use an uninterruptible power supply (UPS) to support orderly close down or allow for continuous running of equipment supporting critical business operations.
- Consider using a back-up generator if processing is required to continue in case of a prolonged power failure.
- Regularly check UPS equipment and generators to ensure adequate capacity and test in accordance with the manufacturer's recommendations.
- Consider using multiple power sources, particularly for large facilities.
- Locate emergency power off switches near emergency exits in equipment rooms.
- Provide emergency lighting in case of main power failure.
- Ensure stable and adequate water supply for air conditioning, humidification equipment, and fire suppression systems (where used).
- Install an alarm system to detect malfunctions in the supporting utilities.
- Connect telecommunications equipment to the utility provider by at least two diverse routes to prevent failure in one connection path.
- Ensure adequate voice services are available to meet local legal requirements for emergency communications.
- Protect power and telecommunications cabling carrying data or supporting information services from interception and damage.

Equipment Maintenance

Information processing equipment must be properly maintained to ensure the continued confidentiality, availability, and integrity of the information and systems processed on it:

- Maintain equipment in accordance with the supplier's recommended service intervals and specifications.
- Allow only authorized maintenance personnel to make repairs and service equipment.
- Keep records of all suspected or actual faults and all preventive and corrective maintenance.
- Implement controls for situations in which equipment is scheduled for maintenance. Consider whether personnel onsite or external to the organization perform the maintenance. Remove sensitive information from the equipment before allowing outsiders to perform maintenance, or obtain sufficient clearance and appropriate confidentiality and non-disclosure agreements from them.
- Comply with all insurance policy requirements for the processing equipment.
- Implement appropriate security for offsite equipment taking into account the unique and existing risks of working outside the organization's facilities premises.
- Implement policies to prevent equipment and media being taken off the premises to be left unattended in public places.
- Require mobile computing devices to be carried as hand luggage and disguised when possible when traveling.
- Implement policies and procedures for personnel who work from home or other locations off the organization's premises. Determine appropriate controls through risk assessment and apply as appropriate.
- Obtain adequate insurance coverage to protect off-site computing equipment.
- Implement physical security controls for all kinds of mobile computing devices, such as personal computers, organizers, mobile phones, smart cards, paper, smart phones, PDAs, Blackberries, storage media, and all other types of mobile computing and storage devices.

Securely Decommission Equipment

Check all types of processing equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal, re-use, sale, or donation to outside the organization:

- Either physically completely destroy the devices containing sensitive information or use procedures and tools to ensure the complete removal of information from the storage devices using techniques to make the original information non-retrievable. Such techniques should go beyond just using the standard delete or format function; they should include using software that will permanently wipe data and degaussing.
- Assess the risk of damaged devices containing sensitive data to determine whether the items should be physically destroyed rather than sent for repair or discarded.

Taking Computing Equipment Off Premises

- Do not allow equipment, information, or software be taken off-site without prior authorization.
- Maintain documentation of the employees, contractors, and third-party users with authority to permit off-site removal of assets.
- Establish and implement time limits for equipment removal and returns. Establish procedures for ensuring compliance.
- Where appropriate based upon risk, log computing equipment as it is taken off-site and when it is returned.
- Perform spot checks to detect unauthorized removal of property in addition to detecting unauthorized recording devices, weapons, and other equipment presenting a threat to the organization and premises. Be sure to perform such spot checks in accordance with applicable legislation, policies, contracts, and regulations.

Human Resources

The most vulnerable of the information security layers, as discussed in Chapters 1 and 2, truly are the human resources that organizations depend upon to follow information security policies and procedures. It is vital that individuals know and understand how to appropriately handle and safeguard the information and associated computing resources that they use while performing their job responsibilities.

Organizations must invest time and resources to help ensure personnel do the right things by:

- Hiring qualified and appropriate individuals
- Providing effective training and awareness
- Motivating with clear career paths and incorporating security into job responsibilities which are used for job appraisals
- Establishing a defined compliance review process
- Mitigating risk of overdependence on key resources by using more than one person for a role in addition to cross training

To help reduce the human risks involved with information security, organizations should consider the following controls within the human information security layer.

Recruitment, Competencies, and Retention

- Implement procedures for recruiting information security personnel, and other personnel with information security responsibilities, to ensure they are appropriately qualified with the skills and experience necessary to achieve information security goals.
- Motivate personnel by incorporating information security as part of the annual job appraisal process.
- Regularly verify personnel remain competent to fulfill their information security responsibilities and continue to receive the appropriate education, training, and/or experience to stay up-to-date with changing technologies and threats.
- Define core information security competency requirements and verify they are being maintained, using qualification and certification programs where appropriate.

Roles

- Define, monitor, and supervise information security roles, responsibilities, and compensation frameworks for personnel. Such responsibilities should include complying with policies and procedures, along with the code of ethics and professional practices.
- Include within the terms and conditions of employment personnel responsibility for information security, internal control, and regulatory compliance.
- The level of supervision over roles should be in line with the sensitivity of the position and corresponding information handled, along with the amount of responsibility assigned.

Training and Awareness

Provide personnel with information security orientation when hired and ongoing training and awareness messages to maintain their knowledge, skills, abilities, and internal controls and security awareness at the level required to achieve organizational goals:

- Provide appropriate ongoing awareness messages, targeted group training, and regular updates to policies and procedures, as relevant for roles and job functions.
- Provide ongoing training specialized to the groups that handle information or support information processing systems. Such training should include security requirements, legal responsibilities, and business controls as well as training in the correct use of information processing facilities, such as log-on procedure, use of software packages, and information on the disciplinary process.
- Make information security awareness, education, and training activities suitable and relevant to the different organization roles, responsibilities, and skills
- Include information within training and awareness on known threats, who to contact for further security advice, and the proper channels for reporting information security incidents.

Personnel Clearance Procedures

- Include background and criminal checks, according to applicable laws, regulations, and union agreements, during the personnel recruitment process.
- Periodically perform background and criminal checks for positions with the most impact to business with regard to information handling and network support.
- Perform background and criminal checks not only for employees but also for contractors, consultants, vendors, business partners, and anyone else who will have access to the organization's information and systems. Periodically re-check personnel backgrounds to discover any events that may have occurred since hire that would put the organization at risk.

Job Performance, Change, and Termination

- Regularly perform job performance evaluations that include consideration of information security requirements and procedures.
- Establish procedures to expediently remove systems and information access and retrieve all equipment and information as soon as personnel terminations occur.
- Ensure that when personnel terminations occur, knowledge transfer is arranged, responsibilities reassigned, and access rights removed to minimize risks and provide for continuity of the personnel functions.

Monitoring and Evaluation

The monitoring and evaluation layer of information security is one that, unfortunately, is often only marginally addressed. Organizations must establish methods for monitoring and evaluation to maintain operational assurance and information security. There are various methods for monitoring and evaluation, including performing scheduled audits; implementing ongoing monitoring of key applications, systems and network components; and performing evaluation activities.

Audits

Both self-administered and independent third-party audits provide important information about the technical, operational, procedural, and regulatory compliance status of an organization's information assets. A variety of tools are used to perform audits:

- Automated tools—These can be used to identify a wide range of vulnerabilities, such as inappropriate or inadequate access controls and access control configurations, bad passwords, systems software weaknesses, and necessary patch updates.
- Performing an internal controls audit—An internal or external auditor can review the controls in place and evaluate their effectiveness. A comprehensive audit will address both automated and human-based procedural controls.

- Security checklists—Checklists can be used to compare leading standards, baselines, or the organization's own policies and procedures with the existing information security environment.
- Penetration tests—Penetration testing, when performed correctly and appropriately, will use multiple methods to attempt to access a system or network. Automated tools can be used within penetration tests to automate the attempts and make the test more efficient. Penetration tests should be performed after security controls are implemented, which will test the effectiveness of some of the controls. Many organizations make the mistake of engaging in a penetration test before they have improved their information security program. Penetration testing can cause adverse impact to business operations if not performed properly; these types of tests should only be conducted with the knowledge and cooperation of systems and network management.
- Social engineering tests—Social engineering tests, such as trying to get a password from the Help desk, is an effective drill for ensuring personnel follow policies and procedures, and can help to reveal where additional training and awareness is needed.

Monitoring

Like audits, there is a wide range of methods that can be used for monitoring.

However, be aware that some methods of monitoring could be illegal based upon applicable laws, regulations, and contractual obligations. Always check with legal counsel before implementing monitoring to ensure it is being done within all the legal boundaries.

- Review logs—Periodically review systems- and applications-generated logs to detect security problems, such as attempts to perform unauthorized activities. Ensure inappropriate information and information under legal restrictions, such as certain types of personal information, is only logged when necessary.
- Utilize automated tools—Virus scanners, checksums, IDSs, and integrity verification programs are just a few of the types of automated tools that can be used for monitoring.
- Configuration change management—Monitoring configuration changes helps to ensure that the correct version of a system or application is being used and that changes are reviewed prior to being placed into production to consider security implications.
- Mail lists/vendor announcements/industry membership groups/publications—Monitor sources outside the organization to keep as current as possible with new and emerging security concerns and issues.
- Accreditation—Formally examine the security of systems and applications periodically to discover whether security is still sufficient and identify necessary changes and other high-level information security management issues along with the implementation status.

Audit and monitoring data can be used as business performance indicators as the following examples highlight:

- Business contribution including, but not limited to, financials, marketing, and customer service
- Performance within strategic business unit, information security, and IT plans
- Compliance with applicable laws and regulations and the associated risks and deficiencies
- Internal systems user satisfaction
- External customer satisfaction
- Key IT processes, such as development, service delivery, and patch management
- Activities to reach long- and short-term goals, such as the use of emerging technology, reusable infrastructure, business and IT personnel skill sets

Disaster Preparedness

Historically, the most unglamorous of the information security layers is disaster preparedness. However, events of the past decade demonstrate the importance and criticality of the components, which include contingency plans, business continuity plans (BCP), and disaster recovery (DR) activities. It is vital for organizations to have such plans in place to support the business goals for continued operations as much as possible under the circumstances.

Hurricane Katrina, which hit the United States' Gulf Coast at the end of August 2005, is an example of a significant natural disaster that had been a possibility for many years, but yet the effects for which were drastically underestimated. The destruction in primarily New Orleans, but also within the Florida Panhandle, Alabama, Mississippi, and Louisiana resulted in federal disaster declarations over a 90,000 square mile area. The total damage estimates at the beginning of December 2005 exceeded $100 billion. This situation compellingly illustrates how crisis management and continuity planning are of increasing concern to public and private sector executive decision makers.

Contingency Plans

Contingency planning addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. Contingency plans integrate the results of business impact analysis. Effective contingency planning will result in a plan for each critical business process and infrastructure component. Contingency plans should describe the implementation resources, staff roles, procedures, and timetables. Contingency planning involves five key components:

- Assessment of the cost and benefits of identified alternatives and selection of the best contingency strategy for each identified business process
- Identification and documentation of the contingency plans and implementation methods
- Definition and documentation of the triggers for activating contingency plans
- Establishment of a business resumption team for each identified business process
- Development and documentation of "zero day" strategies and procedures

The term *zero day* used in the information security context refers to having a security vulnerability exploited on the same day that the vulnerability becomes generally known.

Business Continuity Plans

Organizations need to develop BCPs to minimize the interruptions to business activities in addition to protecting critical business processes from the effects of major failures of information systems or disasters. In addition, BCPs must ensure the continued functionality, or in worst cases, timely resumption of critical business processes.

Implement a BCP to minimize the impact on the organization and recover from loss of information assets to an acceptable level by using a combination of preventive and recovery controls. The time to recover a business process must be within an acceptable time interval.

An effective BCP will identify critical business processes and integrate the information security requirements of business continuity along with the other continuity requirements relating to such activities and areas as staffing, materials, transport, and facilities.

A critical element of creating an effective BCP is to perform a business impact analysis (BIA) to clearly document and consider the consequences of disasters, security failures, loss of service, and service availability as well as to identify the most critical business processes. Organizations that do not perform a BIA will find they are likely woefully unprepared to react in the most optimized manner when business disruption occurs.

BCPs should include not only controls to identify and reduce information security risks but also actions resulting from performing a general risk assessment to limit the consequences of damaging incidents. In addition, BCPs should ensure that information required for business processes is readily available.

Disaster Recovery Planning

Every organization can experience a serious incident that can prevent it from continuing normal operations. This can happen any day and at any time. The potential causes are infinite and widely varied. An organization that cannot recover business processes in an acceptable time can easily go out of business. Every organization is fundamentally responsible for maintaining a DR plan.

> Many regulations require covered organizations to develop and maintain some form of DR plans. Such regulations include HIPAA, GLBA, the United States PATRIOT Act, the European Union Data Protection Directive, Canada's Personal Information Protection and Electronic Documents Act, ad Japan's Personal Information Protection Law.

The concept of disaster recovery planning (DRP) is nothing new. Traditional DRP addressed the recovery planning needs of the organization's IT infrastructures, including centralized and decentralized IT capabilities as well as voice and data communications network support services. As DRP evolves, practitioners have found it apparent that more is necessary beyond just the recovery of IT. Timely recovery of the necessary IT components is useful only if the organization's business units are also able to continue functioning in some manner during the recovery process. The business must be prepared to communicate with customers, business partners, stakeholders, personnel, personnel family members, and others associated with the business. The entire organization must take into consideration in what ways they will be able to continue with basic business processes, such as receiving and entering orders, producing goods, providing services, collecting payments and revenue, and so on.

Incident Response

An information security incident can result from a number of events that can range from a computer virus, other malicious code, a system intruder, and denial of network services to a lost laptop computer or lost backup tapes. The definition of an information security incident is what an organization determines it means to its own particular environment.

Incident response is sometimes included as a part of contingency planning because of the component to quickly and efficiently respond to business disruptions and get back to normal processing as soon as possible. However, there are specialized activities within incident response that are compelling reasons to make this a separate information security layer within organizations.

An organization should address information security incidents by developing an incident handling team or functional area. The incident handling team should be used to quickly and effectively respond to defined incidents by performing activities such as containing and repairing damage from incidents and preventing or minimizing damage from future incidents. The basic components of an information security incident response function will include:

- Service desk function to receive, log, communicate, dispatch, and analyze incident calls, incidents, service requests, and information requests
- Monitoring and escalation procedures based upon the specific type of incident
- Procedures to log and track all incident calls, incidents, service requests, and information needs
- Escalation procedures to ensure incidents are escalated according to predefined limits and to allow for workarounds
- Procedures for monitoring customer, consumer, and personnel queries regarding the incident
- Trend analysis reports to allow response actions to be measured and to identify trends and recurring problems

All personnel, contractors, and other third-party users should be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of organizational assets. They should be required to report information security events and weaknesses as quickly as possible to the designated point of contact. The information security awareness and training program should include teaching personnel how to recognize and properly report incidents.

When follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence as required by the applicable jurisdictions. The rules for evidence generally cover:

- Admissibility of evidence—Whether or not the evidence can be used in court
- Weight of evidence—Quality and completeness of the evidence

Organizations must ensure information systems comply with any published standard or code of practice for the production of admissible evidence to ensure admissibility of the evidence in court actions.

It will often not be obvious when an information security incident is first detected whether the event will result in court action. This ambiguity creates the danger that necessary evidence is destroyed either intentionally during clean-up attempts or accidentally before the seriousness of the incident is realized. This situation illuminates the need for clearly documented and closely implemented incident response plans.

Information security evidence may go outside organizational and/or jurisdictional boundaries. Be sure to include legal counsel to advise how the organization can collect the required information as evidence. Consider the requirements of all the applicable jurisdictions to maximize chances of admission across the relevant jurisdictions.

Summary

All the layers of security defenses and controls discussed previously need to be applied throughout the enterprise. The specific controls within these layers will vary from zone to zone within which they are implemented, as described in Chapter 4. In effect, these security layers will exist in all the zones, as represented and applied, using the zoning diagram discussed in Chapter 4. However, because the chosen controls are based upon risk, they will not be identical throughout the enterprise.

The chosen and implemented controls need to be based upon risk, and each security zone will have different risks.

Within each security zone, apply only the amount of security needed to maximize the benefit of information security to the business. Do so by assessing the risks within each identified security zone. However, do not think that this means that "less is more" when it comes to information security! In fact, the most efficient information security activities will utilize a wide range of information security tools and procedures that will comprise a multi-layered blanket of information resources protection for the organization. Chapter 6 will delve into a discussion of these security tools.

Chapter 6: Tools in the Zones

Organizations must manage information security in multiple ways throughout the enterprise and as appropriate within each of the identified security zones. Network security management must effectively manage access to information assets and establish rules that network users must follow, limit access to network information resources to only those that have a business need for the access, and create notifications whenever incidents and inappropriate actions occur.

Powerful security safeguard tools must be implemented within established security zones to make the zones effective. When determining the security tools to implement, keep in mind that most reported information security incidents basically stem from three business weaknesses:

- Poorly implemented security measures revolving around improper access controls
- Lack of encryption
- Trusted insiders purposefully or accidentally accessing, using, or damaging information resources

A common perception regarding network security tools is that such tools are different from others within your organization. If you ask seasoned information security practitioners to list network security tools, you will get a wide range of diverse answers. This variation is understandable because what are considered important information security tools depends upon the roles and responsibilities for each information security practitioner within each unique organization and its accompanying threats, risks, vulnerabilities, geographic locations, and applicable laws, regulations, and contractual requirements.

An informal survey of five highly seasoned information security practitioners—each with 15 to 30 years of security management experience—asked the professional to list what popped into their minds when thinking about network security tools. Their combined responses resulted in a list of 32 tools, which the following list highlights:

- 802.11X WLAN controls
- 802.1x authentication
- Access control lists (ACLs) between network zones
- Application system controls
- Awareness and training for network users
- Centralized security management
- Database system ACLs
- Deep packet inspection devices
- Digital certificates
- Firewall appliances
- Firewalls between network zones—stateful inspection, application firewalls, proxies
- Identity management

- Intrusion Detection System (IDS) monitoring tools
- Kerberos
- Network partitioning
- Network segmentation
- One-time passwords, such as those used with the RSA SecurID
- Operating system (OS) controls
- Physical access control cards
- Physical separation of high-risk computers from the network
- Physically protecting network devices (employing data center physical access controls, protecting cables from tampering, and so on)
- Policies and procedures
- Quarantining tools that check a host when it connects to the network for a baseline configuration (current antivirus, patch level, and so on) and, if the baseline is not met, does not allow the host access or allows only limited access
- RADIUS, TACACS+, TACACS, DIAMETER
- Role-based access controls
- Single-Sign On (SSO) tools
- Traditional passwords
- Two-factor authentication tools (smartcards, tokens, and so on)
- Screensavers and other endpoint security actions
- VLANs
- Software tools such as those from BindView and Arbor Networks
- Content monitoring and data leakage prevention tools, such as NetIQ WebMarshall and Vericept monitoring solutions

All their responses are valid for each of their own situations and business environments. There was some overlap, but there were clear differences between the lists based upon the primary concerns for each practitioner.

Each organization must determine the risks to their own unique organization, create the security zones as explained in Chapter 4, then identify the best tools to address the threats, risks, and vulnerabilities within each of the identified zones.

There isn't one list of network tools that will provide the magic solution for securing network information resources.

The wide range of network security tools that will give organizations the most bang for their buck and help to provide the most effective security to their enterprise information resources can be generally discussed within four categories:

- Access controls
- Encryption
- Monitoring
- Awareness and training

> ☞ To be effective and meet the numerous legal and regulatory requirements that now apply to basically all organizations, these tools must be used in accordance with established, formally documented, and executive management supported policies and procedures.

Access Control

Problems will quickly emerge if proper access controls are not implemented throughout the enterprise and appropriate to each of the zones within which the controls are applied: Authorized users within the zones will download and install mobile code from the Internet onto the organization's computers, carry in problems on their mobile computing devices, or introduce problems from their remote locations. As this guide has emphasized, it is no longer sufficient to simply apply security at the network perimeter. Workstations and endpoints within the network perimeter must now be viewed as hostile territory and potential threats. Desktop access controls must be managed centrally, including such controls as desktop firewalls, malicious software prevention tools, security policies for the zones within which they reside, and user authentication and authorization. Information and network asset protection success relies on the measures implemented close to the IT resource, within multi-tiered applications, and on active security management.

Changing access controls from perimeter-based to zone-based will require changing the security architecture, and it will require careful planning and resources. Use the people and skills within the organization to leverage the time, effort, and costs involved. Structure the network architecture to consolidate resources and leverage security zoning. Tighten internal access controls by restricting access appropriately to support and facilitate business processing within the identified security zones. Network security administration tools have come a long way in the past few years, and what used to seem like prohibitively expensive or impossible to implement centralized access control solutions are now quite achievable and affordable.

Types of Access Controls

Access controls block or facilitate a user or system to communication and interaction with network resources such as computers, databases, email, Web servers, routers, or any other systems or devices. Access controls protect systems from unauthorized access and determine what levels of authorization are appropriate for a user or system. Access controls can be technical or operational. The following list highlights examples of different types of access controls:

- Access control policies and procedures
- Proxy servers and firewalls
- Physical access control cards
- OS capabilities
- Application system capabilities
- Database system ACLs
- IDS monitoring tools
- Access control security auditing
- Identity access or SSO tools
- Two-factor authentication tools (smartcards, tokens, and so on)

Laws and Regulations Require Access Controls

Besides being a prudent business activity, implementing access controls within the network is required by multiple laws and regulations, and additional legal requirements are established each month along with new contractual obligations for effective access controls.

HIPAA

The following excerpt is from the United States HIPAA security rule (http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf), which includes the following directive for access controls:

> "§ 164.312 Technical safeguards.
>
> A covered entity must, in accordance with § 164.306:
>
> (a)(1) Standard: Access control.
>
> Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
>
> (2) Implementation specifications:
>
> (i) Unique user identification
>
> (Required). Assign a unique name and/or number for identifying and tracking user identity.
>
> (ii) Emergency access procedure
>
> (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
>
> (iii) Automatic logoff (Addressable).
>
> Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
>
> (iv) Encryption and Decryption
>
> (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information."

This excerpt demonstrates the clear need for policies and procedures to create a framework for an information management program, to serve as types of access controls for an organization, and to meet compliance with HIPAA. Access controls need to be appropriate within each identified security zone.

The Gramm-Leach-Bliley Act

The following excerpt is from the United States Gramm-Leach-Bliley Act (GLBA) safeguards rule (http://www.ftc.gov/os/2002/05/67fr36585.pdf), which includes the following directive for access controls:

> "§ 314.3 Standards for safeguarding customer information.
>
> (a) Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.
>
> (b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:
>
> (1) Insure the security and confidentiality of customer information;
>
> (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
>
> (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."

This excerpt demonstrates how access controls are often legislated through implication. Although not explicitly stated, access controls are needed to achieve actions 1, 2, and 3.

European Directive on Privacy and Electronic Communications

The following excerpt is from Article 5 Item 3 of the European Directive on Privacy and Electronic Communications (http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf), which includes the following implications for access controls:

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

This excerpt demonstrates the need for access controls worldwide. In fact, countries other than the United States have much broader data protection laws that require organizations to be much more diligent in establishing information security controls. Notice this particular law emphasizes the need to give access to only those necessary to perform business activities, described as an "information society service."

Canadian Personal Information Protection and Electronic Documents Act

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) contains many requirements for access controls. The safeguards section includes the following directives, which include access control requirements:

> 4.7 Principale 7 — Safeguards 4.7 Septième principe — Mesures de sécurité
>
> Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
>
> 4.7.1
>
> The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.
>
> 4.7.2
>
> The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.
>
> 4.7.3
>
> The methods of protection should include
>
> (a) Physical measures, for example, locked filing cabinets and restricted access to offices;
>
> (b) Organizational measures, for example, security clearances and limiting access on a ''need-to-know'' basis; and
>
> (c) Technological measures, for example, the use of passwords and encryption.
>
> 4.7.4
>
> Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.
>
> 4.7.5
>
> Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

This excerpt demonstrates that laws requiring data protection do not focus solely on technology security requirements but also on organizational and physical security controls.

Japanese Personal Information Protection Law

The following excerpt from the unofficial English translation (Proskauer Rose LLP © 2005 unofficial English translation at http://www.proskauer.com/hc_images/JapanPersonalInformationProtectionAct.pdf) includes the following directive that has implication for access controls:

> Section 20 Security Control Measures
>
> A Business must take steps to prevent the unauthorized disclosure, loss or destruction of Personal Data and it must protect Personal Data security.

This excerpt demonstrates that some laws are written very broadly and result in wide interpretation by not only different organizations but also different positions within an organization, such as information security and legal. You must consider carefully what actions will be able to justifiably demonstrate your organization truly has tried to comply with the laws.

There Are No Longer Homogenous Environments

Implementing effective access controls is no longer the comparatively easy task it used to be when all information resided on one mainframe and there were only dumb-terminals sitting on the end users' desktops. Now the network environment in most, if not all, enterprise networks is a mix of systems owners scattered throughout the enterprise in various departments and locations, assortments of operating systems (OSs), and applications servers of every type imaginable. The complexity of networks is growing by leaps and bounds while the implementation and availability of security solutions correspondingly seems to grow by what sometimes seems to be creeps and crawls.

According to the 2005 Network World 500 Research Study of 500 participating organizations (http://www.networkworld.com/pdf/nw500study05.pdf):

—Wireless LANs (WLANs) will be deployed within at least 73 percent of organizations by 2007

—82 percent will deploy IP VPNs in 2006

—64 percent provided business partner access to their networks

Today, enterprise networks are composed of numerous devices, differing technologies, and wide ranges of applications that always seem to be pushed to internetworking with Internet components, business partner systems, and even directly with customers.

The complexities of internetworking multiple systems and the accompanying information create great risk that organizations will not be able to address the security of new business demands and functionality.

The network perimeter is porous. In complex enterprise networks and in today's business processing environment, there is no longer a clear line between the good guys, the bad guys, and the incompetent guys. Access controls can no longer be plunked down on one system and successfully control access to all the enterprise information resources. Zones are a necessity in today's computing environment. The ever-increasing complexities of interconnected networks and the utilization of the Internet for business transactions has not only exposed organizations to the vast global array of threats from online ne'er-do-wells but also created an amalgamation of networks, people, applications, and systems that can each impact any other point on the network through one weakness. The concept of the weakest link in the chain has never been more compelling than in today's network environment. To successfully incorporate security throughout a complex network, there must be a common thread; centralized points of security management that can oversee, guide, and manage all the diverse environments.

Headless Servers

A server that lacks a monitor, keyboard, or mouse is typically called a *headless server*. A headless server can also lack a video card. Headless servers are being used more and more within organizations. They offer several advantages:

- Organizations save space by not having monitors, keyboards, and mice for the servers.
- Organizations do not need to purchase a monitor, keyboard, mouse, or cables and switches to support servers, saving what could be considerable amounts of money, especially in a multiple-server hosting situation.
- Organizations improve the physical security; with no keyboard, monitor, and mouse, an unauthorized person can do little with or to the system.

However, headless servers also present some new security challenges:

- Without a mouse, keyboard, or monitor, administration will need to be different than the traditional approach. Remote administration tools will need to be used.
- Because a headless server does not have an associated user, it must be authenticated at the device level rather than at the user level.
- When the headless server is unavailable, administrators must be able to perform remote-management and system recovery tasks through the network or other standard remote-administration tools and mechanisms.

Just a few examples of remote administration tools include: terminal services, VNC, and Remote Administrator.

More organizations are using headless servers for the advantages listed earlier. These organizations need to ensure they have adequately addressed the identified challenges.

Before launching a headless server, organizations must prepare the server to ensure it can be fully and remotely administered.

Implementing headless servers throughout the enterprise should be done consistently, following documented procedures and guidelines. Centralized oversight and administration of the servers will ensure the servers within each of the security zones are protecting sensitive data consistently from one zone to the next.

Web-Based Servers

The number of Web-based servers organizations deploy also continues to grow by leaps and bounds as organizations depend more upon Internet presence and online sales to boost revenues.

> According to the December 20, 2005 edition of the New York Sun, "For the first half of 2005, the Interactive Advertising Bureau estimates such [online] advertising was $5.8 billion. Online advertising appears to account for more than 5 percent of total advertising and to be growing much more rapidly."

The increase in advertising and Internet sales demonstrates the growing dependence upon Web servers for Internet commerce. These Web servers are increasingly connected to enterprise networks in more locations and using more methods that increase the number of threats to the network information resources. Establishing consistent and centralized controls for all enterprise Web servers is essential for information security, regulatory compliance, and continued network availability.

> According to a November 2005 report from the United States Census Bureau:
>
> —Online sales accounted for $22 billion in retail activity in the third quarter of 2005
>
> —For 2005, online retail sales are projected to approach $90 billion (2.3% of total U.S. retail activity)
>
> —E-commerce is growing by about 25 percent annually

Incorporating Access Controls into the Development Life Cycle

To successfully incorporate access controls into the systems development life cycle (SDLC), the organization's required security parameters and requirements must be clearly documented and communicated to all systems and applications developers in terms applicable to the development processes. Such security requirements should be incorporated into the formal SDLC process in the same way that the business requirements and end-user requirements are defined.

The first phase in the SDLC is typically initiation. It is during this phase that an organization establishes the information security requirements. Such requirements must be based upon analysis of the application or system, and typically the requirements will be refined as the other SDLC requirements are refined. Normally the security requirements will be expressed at a high level, addressing the system or application objectives.

> An effective starting point for these high-level security requirements is the organization's information security policies, procedures, and standards.

High-level requirements are the basis for creating more detailed functional requirements and specifications.

Variety of Application Types

Today's enterprises have many more types of applications to manage than ever before, and usually the applications are completely different from one business unit to another. Managing access controls consistently throughout the enterprise in this type of situation is quite challenging and is often the impetus to many stressful workdays for the typical information security leader.

Organizations are realizing that effective management is being accomplished best through identity management. Very generally, identity management establishes and controls identity changes and access rules to resources using a variety of centralized actions:

- User enrollment and provisioning
- Password management and personal information updates through self-care capabilities
- Privacy preferences management
- User profile management
- Credential management
- Identity policing management, such as access rights change processes, user ID creation, and password strength

There are notable benefits to using identity management systems to centrally control access across a variety of application types:

- Enables easier and more effective management of access control to applications, Web services, and middleware
- Provides a single point of access control decision for new and legacy applications
- Allows for more granular control of access to multiple system resources
- Creates the ability for end users to make access control decisions to private personal information
- Enables a single point of user activity monitoring and auditing
- Allows for single, or reduced, sign-on and entitlements

Typical Application Developers

Typical application developers are quite knowledgeable about their particular applications but unfortunately often do not truly have the security experience or knowledge for that application to make prudent security decisions. However, because of their knowledge of the applications, they often believe that they know all there is to know about security for the applications for which they are responsible. When there are no clearly defined policies or requirements for including information security within the development process, there is great risk that developers will create a new system without adequately building in information security—or will include security in such a way that creates weaknesses and exposes organizations to threats and legal noncompliance.

> ☞ Organizations must create and implement a clear and explicit set of information security requirements for application developers to use to ensure security is appropriately built-in to applications.

Organizations must not only provide clear direction to detail the security requirements for applications but also monitor compliance to ensure the security is actually being implemented. Organizations need to establish ways to monitor applications security development requirements.

> ☞ Organizations should periodically review user access authority to ensure it is limited to the minimum required access level based on job requirements. Such reviews will discover and appropriately limit the access of application development staff to sensitive system resources.

Because of the need to separate responsibilities between application development and production, organizations need to monitor access to production resources.

> Without monitoring and proper access controls, there is great risk that application developers with access to production programs and data could add, alter, or delete payroll and personnel information (for example) without being detected.

Encryption

No organization can completely defend against all threats; the number of potential risks and threats is generally infinite, and many (if not most) are unknown or unanticipated until after they have happened. Those unknowns are typically what wreak the most havoc on organizations.

Of course, organizations must implement appropriate safeguards to protect against threats and demonstrate due diligence. One of the best ways to protect information, particularly information such as personally identifiable information that is covered by multiple laws and regulations, from unknowns is to make it virtually incomprehensible and unusable to unauthorized individuals by encrypting it. Assume one of those infinitely unknown threats will visit an organization; having sensitive data encrypted will significantly lessen the business impact when it happens.

The Need for Encryption

The increasingly porous network perimeter combined with the growing number of ways in which to share data with all locations throughout the world has generated an increasing need to protect information by using encryption. This protection should include encrypting not only the actual data but also, and perhaps more importantly, the authentication credentials (user IDs and passwords) for the applications that access the data.

> A large number of both commercial and freeware software tools allow information passing through a network to be intercepted and copied. These tools, commonly called sniffers, can be very beneficial for network administrators for troubleshooting. However, as you can imagine, in the hands of someone with malicious intent, any clear-text data—such as passwords and user IDs, credit card numbers, and other sensitive data—can be captured and, as an effect of these tools, no trail is created to indicate that the information was intercepted and copied. Imagine how many times user ID and password pairs may have been intercepted and then used to access databases with sensitive data without the knowledge of the legitimate account owner or the network administrator.

Contributing to these compelling technology factors is the exponentially growing numbers of regulatory requirements for organizations to implement safeguards to protect data more effectively than has been demonstrated in the past.

> 🕮 The December 25, 2005 issue of Iowa's Des Moines Register reported 3000 Iowa State University (ISU) employees may have had their personal data viewed by hackers who gained access to two computers earlier in December. One computer held about 2500 encrypted credit card numbers of athletic department donors. The second computer contained clear text Social Security numbers for more than 3000 ISU employees. The intruder could not have read the credit card numbers because they were encrypted; however, the Social Security numbers are at risk of being inappropriately used. ISU officials said they would not contact police to try to find the identity of the intruder because it would be very difficult to track a hacker who could have come from almost anywhere in the world.

It is interesting to read about incidents and note that sometimes there are pockets of sensitive information that is encrypted while other times other equally sensitive information is not encrypted, all within the same organization. For example, in the December 2005 ISU incident, credit card numbers were encrypted but the Social Security numbers were not. This variance is likely the result of the strict and specific requirements from the credit card companies to encrypt credit card numbers while in storage, but the lack of similar explicit regulatory requirements to encrypt Social Security numbers while in storage.

Although encryption will not protect data from every type of incident—such as when authorized insiders abuse or misuse their privileges—it does provide protection by ensuring only authorized users with valid decryption credentials can see the data, and keeps inappropriate viewing and use from occurring when data is lost, stolen, or otherwise compromised. Just consider the June 2005 Citigroup incident in which a backup tape containing information about 3.9 million individuals was lost by UPS while in transit (see http://www.msnbc.msn.com/id/8119720). If the information had been encrypted, the incident would have had much less business impact to Citigroup, and would have presented significantly less risk to the individuals whose information was on the tape. Unfortunately, many organizations still consider current encryption solutions to be too complex to realistically implement enterprise-wide or to have too much of a negative impact on application and network response times. It will be interesting to see how encryption practices change throughout 2006.

> 🕮 In August 2005, Forrester Research reported only 16 percent of North American companies implement data-at-rest encryption for their databases, and only 48 percent implement data-in-motion (network) encryption to support critical applications.

Legal Requirements for Encryption

In the ISU case, the fact that credit card numbers were encrypted on one system while the Social Security numbers were not encrypted on another system provides a classic example of implementing a narrow interpretation of doing only what is required by the "letter of the law" or the "letter of the contract" instead of implementing a wider interpretation of doing what is right according to the spirit of the law or performing due care activities to protect sensitive information.

Consider the PCI Data Security Standard (see a copy at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf), which requires cardholder data to be encrypted. If ISU wanted to process credit cards, they had to meet this standard. However, there are no laws that explicitly require Social Security numbers to be encrypted in storage. Even if this wasn't why ISU encrypted credit card numbers but did not encrypt Social Security numbers, it provides an example of a common practice—many organizations have only done, and make it a point to only do, the minimum required with regard to encryption (and any other security controls for that matter) as explicitly or specifically contractually or legally required.

Often in meetings with legal counsel and CISOs who are talking with their CEOs and CIOs, the legal counsel's strongest argument to not implement the security the CISO was requesting/recommending (even if it was a result of a risk analysis) was because it was not explicitly required by law or contract. Although this discussion isn't meant to be an argument against legal counsel, it demonstrates that their role within the organization is much different than an information security practitioner's role and often their bonus or pay is impacted by the amount of money they can save an organization by providing defendable opinions and reasonable interpretations that prevent excessive money from being spent.

> ☞ Identify the legal and contractual requirements for encryption to demonstrate the clear need for encryption solutions within the enterprise.

Need for Transparency

Currently, data is more commonly encrypted for remote access transmission instead of encrypted for storage. One common reason why is because data-in-motion encryption is usually seamless to the application and requires minimal effort to deploy and little action from the end user. Another reason is that companies have historically been more concerned about hackers getting the information as it passes through the Internet than with someone getting to the data in storage.

> ✎ A virtual private network (VPN) is an example of a transparent encryption solution. Most VPNs are engineered in such a way so that authorized individuals do not have to do anything to encrypt data that is being transmitted using the VPN solution; encryption occurs automatically without any involvement from the end user.

As the perimeter becomes more porous, it becomes more important to encrypt data-in-motion, especially user IDs and passwords, within the perimeter as well as outside of it. Data-in-motion encryption will need to be completely transparent since a growing number of systems within the perimeter are headless, many applications are legacy, and modifying enterprise legacy systems is simply not an option in most cases.

The demand to encrypt data at rest (while in computer storage) has not been as great and, as a result, vendors have not provided easy-to-implement transparent solutions. DBMS vendors that offer encryption application interfaces (APIs) often require changes to the application, especially when joining multiple tables and scanning data using encrypted columns, besides requiring creation of stored procedures, triggers, and views. However, as more incidents occur with unencrypted data at rest and as more regulations require organizations to consider encryption as part of their compliance activities, organizations are asking vendors to make transparent data-at-rest encryption solutions available. Until transparent data-at-rest encryption solutions are available, though, most organizations are depending upon access controls to protect the databases and the applications that access them.

A data-in-motion encryption solution must be able to work with all OSs found throughout a heterogeneous network. A native IPSec solution has restrictions for the type and revision of OS that can be supported. Only the latest Linux OS uses native IPSec, potentially leaving a huge portion of the network vulnerable to attack. Encrypting the data communications requires providing end users with a transparent interface to access applications. If end users must use a different, separate authentication action each time a non-supported application is run, it is more likely the end user will decide to find a workaround or to find a way to bypass the additional security interfaces. In addition to this increased end user risk, additional training will be required for end users to ensure they know how to correctly and consistently use the encryption solution.

> ☞ Encryption solutions must be as transparent as possible to be as effective as possible.

Encrypting Data in Motion

Securing data that goes outside the network perimeter presents challenges. VPNs have been the most common way of protecting information that must pass through a public network (such as the Internet) through the use of multiple security controls including encryption. Insider attacks are increasing at alarming rates, as discussed in Chapter 2. Network intruders realize that they can gain access to internal corporate networks because internal networks are more vulnerable and typically do not use encryption to protect data in transit that does not go outside of the network. However, as the number and severity of internal network attacks increases, organizations realize that using encryption is an essential tactic to prevent theft of intellectual property and personally identifiable information.

Encrypted data is hidden while it moves through the network from one point to another, such as a database to a client on an end-user computer or vice-versa. Encryption for data in motion should be done based upon risk to the information, for information transmission through the enterprise network, through the Internet, and through wireless networks.

The most common data in motion standards include Secure Sockets Layer (SSL), Transport Layer Security (TLS), and IPSec. Most database vendors use the SSL standard. This standard allows data to be sent between client and database vendor through an SSL tunnel that encrypts the data using some combination of RSA, RC4, DES, or the Diffie-Hellman algorithm.

It is important to encrypt sensitive data in motion to prevent the data from being intercepted by someone also using the network as the data is going back and forth between the client and the database.

Encryption helps to effectively prevent session hijacking, replay attacks, and access to user ID and password combinations.

To most quickly, easily, and cost efficiently meet the directives of enterprise leaders, systems administrators have typically chosen to use native IPSec, found in both Windows and the most recent version of Linux, to implement the enterprise encryption strategy. They do so because it is a proven standard, works transparently to users and applications at the network layer, and is well suited for enterprise use. Its weakness is in its deployment; it is difficult to administer and this difficulty increases exponentially as more servers are interconnected using it. Consequently, even though most organizations use it, it is used in small segments where the deployments can be managed manually.

IPSec is effective for the inside of the network but is difficult to administer. SSL works well outside the enterprise, but presents difficulty within enterprise networks.

Organizations are increasingly using add-on solutions that are specifically engineered to encrypt data-in-motion within networks. There are many new data-in-motion add-on solutions that are quite good and some of these focus on making the deployment of IPSec simple and highly scaleable, providing the best of both worlds— a transparent infrastructure to encrypt data-in-motion without the pain of the deployment issues. Organizations should consider these when developing their enterprise encryption strategy. A few vendors that provide data-in-motion encryption solutions include:

- Apani Networks
- CipherOptics
- Ingrian Networks, Inc.
- OpenConnect Systems, Incorporated

Encrypting Data at Rest

One of the most important decisions when implementing a data-at-rest encryption solution is selecting which data to encrypt. When encrypting databases, remember database lookups are designed to be very efficient. Unlike typical file systems, databases are expected to look through millions of rows, searching for specific items in seconds. These speed features present challenges for encrypting databases. It is not feasible for a database to decrypt each data element it must search.

It is critical to consider how applications will use the database while planning to deploy encryption. There are many possibilities for encrypting data at rest, including:

- Encrypt the actual database files at the OS level. Doing so provides protection from theft of the disk but can have a serious performance impact and does not provide for granular user access control.
- Encrypt on a column and row basis. This method is a more efficient and effective way to encrypt information in a database. This option requires tight integration with the database. However, if implemented properly, column- and row-level encryption solves problems that have stopped database administrators from implementing data-at-rest encryption solutions in the past.

Encrypt at the Network Layer

The ideal solution is to implement encryption at the network layer so that it is transparent to both users and applications and requires no modification to existing software applications, such as CRM, ERP, and inventory tracking systems. The success of VPNs to encrypt data in motion for remote access demonstrates that implementing encryption within the network layer allows for phased deployments within targeted security zones to add immediate benefit to enterprises. Implementing network-layer encryption solutions within identified security zones with careful planning and the right tools can even eliminate the challenging deployment and management of VLANs.

> ☞ Correctly implementing encryption within security zones can not only save time and costs but also mitigate the impact of a perimeter security breach.

Centrally Managing Solutions Is Crucial

Possibly the biggest challenge when implementing an encryption solution is solving key management challenges. Encryption implementations often hard-code the keys into procedures or scripts. This type of implementation will provide little security because reviewing the code will reveal the keys.

> It is critical for keys to be protected. Such protection must include encrypting the keys in storage and limiting access to only authorized owners.

A well-designed encryption system will operate separately—generating, storing, and protecting keys with very little user intervention. Mistakes or weakness in key management can quickly lead to system compromise. Key management is a critical area to focus upon when purchasing or building an encryption solution because mistakes and weaknesses within a key management system can quickly allow for system compromise.

Monitoring

An important tool for network security management is monitoring: monitoring compliance, monitoring access attempts, monitoring for malicious code, monitoring for any activity that can have negative impact on the business.

Personnel Monitoring

It is necessary to monitor business information processing to demonstrate due diligence, obtain evaluation information, and to comply with applicable laws and regulations. Doing so will often include some type of personnel monitoring. The types of employee information and methods for collecting it are quickly expanding. However, be aware that individuals are concerned with the monitoring that occurs—the growing number of court actions each year reflects this concern for workplace privacy.

Personnel Monitoring Examples

The following examples provide an idea of the breadth of concern and how court considerations are changing over time with regard to how monitoring activities within business are used to catch personnel doing bad things—supporting both the need for monitoring of some type in addition to addressing employee privacy protections:

United States v. Harrison, 1/13/04. A New York City Human Resources Administration (HRA) employee was arrested January 13 for an alleged multi-million-dollar tax and identity theft scheme. Veronica Harrison allegedly sold thousands of identities under the scheme, which involved filing thousands of false and fraudulent individual income tax returns in order to receive tax refunds from the Internal Revenue Service. Nineteen defendants were charged February 4, 2003, with engaging in this same scheme from 1997 through January 2003.

United States v. Fennessee, 1/8/04. A former employee of the Illinois Department of Human Services received a 2-year prison sentence for her role in an identity theft ring that stole personal information about state employees and used it to fraudulently obtain cash and personal property.

Haynes v. Kline, 12/23/03. A federal district court ruled that, even though a public employer's policy stated employees had no expectation of privacy in using their computers, it did not negate a staff attorney's expectation of privacy in electronic communications where he was informed during orientation that his computer contained private files inaccessible by others and there was no evidence that his employer had ever monitored or viewed other employees' private information.

Sieglock v. Burlington Northern Santa Fe Railway Company, 12/18/03. The court remanded the case, saying Burlington's faxing of 300 employees' confidential information might have subjected each to harm, and that Sieglock might be able to demonstrate relevant facts sufficient for a class action in Montana.

Privacy and monitoring at work is a complex subject. Organizations must determine the extent of monitoring controls and mechanisms needed for adequate security and demonstrated due diligence, and at the same time balance that with employee privacy needs. Technologies capable of invading privacy are being created every day and implemented by many organizations, typically not for the purpose of privacy invasion, but to improve the business efficiency, security, and controls in some way.

Employee monitoring is not new. In 1913, the Ford Motor Company established a Sociological Department, which included monitoring activities to determine whether employees participated in activities for which Mr. Ford did not approve, such as gambling, smoking, drinking, or other unseemly and unapproved behavior; even during their personal time.

Over the years federal and state laws have emerged to address employee privacy rights. However, employee privacy issues are still gray with regard to many types of private information and personally identifiable information, such as, but not limited to, the following:

- Background checks
- Physical and work area searches
- Surveillance (closed circuit television—CCTV, videotaping, audio taping, hidden microphones, and so on)
- Location tracking (Smart ID cards, RFID tags, and so on)
- Drug and alcohol testing
- Biometrics
- Employee non-business information (memberships, activities, hobbies, and so on)
- Personnel files
- Telephone and cell phone monitoring
- Keystroke monitoring
- Electronic message monitoring
- Internet monitoring (Web sites, blog activity, and so on)
- Wireless monitoring
- Health information
- Physical mail
- Job applications
- Personality tests and psychometric or aptitude testing
- Packet-sniffing software
- Keystroke loggers

Laws, Regulations, and Guidelines

In 1996, the International Labour Organization (ILO), a United Nations agency promoting human rights, adopted a code of practice for protecting workers' personal information. The ILO code is the standard used by privacy advocates for protecting workers' privacy rights. The protections advise:

- Employees to be given notice of information collection processes
- Personal information to be collected and used lawfully and fairly
- Employers to collect the minimum necessary information required for employment
- Personal information should only be collected from the employee, absent consent
- Information to only be used for reasons directly relevant to employment, and only for the purposes for which the information was originally collected
- Information to be secured
- Employees should have access to their personal information
- Employee information should not be transferred to third parties without consent or to comply with a legal requirement
- Employees cannot waive their privacy rights
- Employee medical data should be treated as private and confidential
- Certain information, such as sex life and political and religious beliefs, should not be collected
- Certain collection techniques, such as polygraph testing, should be prohibited

Several United States laws provide for employee privacy rights in various ways. Just a few of these include:

- Americans with Disabilities Act (ADA) prohibits employers from asking certain questions about employees.
- Privacy Act protects against disclosures by government entities and applies to government employee information under certain situations.
- Electronic Communications Privacy Act (ECPA) prohibits intentional interception of electronic communications. However, it generally gives employers the right to access employer-provided voicemail and email systems. The constitutions and statutes of some states, such as the California Constitution, may restrict this right, though. Additionally, employers do not have the same right to access email that is outside the company's system, such as on another Internet mail server.
- National Labor Relations Act provides the framework for fair labor practices and labor organizing, which addresses some privacy issues.

- Employee Polygraph Protection Act protects private-sector workers from exposure to polygraph "lie detector" testing. Government employees and certain government contractors are still subject to examination.
- HIPAA has requirements for ensuring protected health information privacy and impacts health information monitoring for employers who are covered entities under this law, as well as employers who are plan sponsors to protect their employees' privacy.
- The Fair Credit Reporting Act (FCRA) regulates methods of obtaining credit information about an applicant or employee. See the Federal Trade Commission's fact sheet on what employers need to know about using consumer reports at http://www.ftc.gov/bcp/conline/pubs/buspubs/credempl.pdf.

Most states have laws that address employee privacy rights in one way or another. At least 31 states in the United States allow employees, and sometimes former employees, to review, and sometimes copy, their personnel files under specified conditions. For example, Alaska law gives employees and former employees the right to inspect and copy personnel files. All states have laws that cover and could impact employee surveillance, including telephone monitoring, CCTV, audio taping, videotaping and wiretapping. At least one state, Connecticut, requires employers to notify their employees of monitoring practices. Additionally employees may sue employers for privacy invasions under privacy torts. For example, such torts may include intrusion upon seclusion, public disclosure of private facts, and false light.

International Issues

In many European jurisdictions, the employee's right to privacy is protected in the constitution, limiting the employer's ability to monitor in the workplace. Additionally, employers must often show regard for the rights of employees' representatives to be consulted regarding the implementation of any monitoring. There are several major issues you should consider for the privacy of your non-U.S. personnel. The following list provides a very brief discussion of some of the workplace privacy and monitoring laws; use this list as a springboard to launch your own research on applicable multi-national employee privacy requirements:

- In the United Kingdom, the Data Protection Act of 1998 regulates workplace monitoring. Detailed guidance for employers about how the legislation applies to monitoring at the workplace is set out in Part 3 of the Information Commissioner's Employment Practices Data Protection Code on Monitoring at Work.
- Although Germany does not have any specific legislation or codes of practice addressing workplace monitoring, employees (actually all individuals) have a right to privacy under the German constitution. The Federal Data Protection Act and Telecommunication Act also regulate workplace monitoring, and violations of monitoring prohibitions can lead to criminal prosecution.
- In Sweden, the Penal Code (Brottsbalken 1962:700) and the Data Protection Act (Personuppgiftslagen 1998:204) regulates monitoring and recording telephone calls and email. The Data Inspection Board published a report and guidelines relating to this area in 2003.

- In Italy, the main regulations for workplace monitoring include Sections 4, 8, and 15 of the Workers Charter and Sections 114 and 115 of the Personal Data Protection Code. Generally these, together with prevailing case law, protect employees from concealed workplace monitoring.
- In France, workplace monitoring is regulated by detailed legislation contained within the labour, civil, and criminal codes. The French Data Protection Authority has also published two reports containing guidelines on email and Internet usage.
- In Alberta, Canada, the Personal Information Protection Act, S.A. 2003, c. P-6.5 covers the information employers may and may not collect and disclose about workers.
- In Australia, Guidelines on Workplace E-mail, Web Browsing and Privacy, published March 30, 2000, is directed to organizations in both the public and private sectors.

Works Councils, Trade Unions, and Labor Unions

If an organization has work councils or trade or labor unions, those councils and unions need to be included in discussions regarding employee privacy and planned policies, procedures and actions. Whether the employer is required to seek the agreement of employee representatives or just needs to consult with them will depend upon the local requirements of each jurisdiction and the terms of the applicable agreements.

Be aware that restricting employee communications may violate fair labor laws when there is interference with union activities. For example, in Pratt & Whitney, Feb. 23, 1998, the National Labor Relations Board (NLRB) reported in an advice memorandum that a company's computer network was a "work area." Accordingly, monitoring email on the company network for non-business use could be unlawful. Employee monitoring that can be considered as selectively punishing labor-organizing activities could violate the National Labor Relations Act (NLRA).

Know what personnel monitoring you can and cannot do. The following list highlights areas of consideration regarding personnel monitoring:

- Identify employee privacy laws and regulations applicable to the organization and worksites.
- Determine the employee monitoring activities and technologies needed to support business security and due diligence, and activities that could be considered as violating privacy rights.
- Know what personal information can be requested on job applications. For example, in the United States it is illegal to ask about arrests or charges but you are allowed to ask about convictions. Some states, such as California, have restrictions on using information about convictions. It is also illegal under the United States Americans with Disabilities Act, which applies to organizations with 15 or more employees, to ask job applicants if they have ever been treated by a psychiatrist. Some state laws also prohibit discrimination on the basis of disability for organizations that have fewer employees (for example, California applies to 5 or more employees).
- Evaluate the risks for misuse when releasing employee personally identifiable information to third parties.

- Be aware of the types of employee information that is gathered throughout the company, such as on sign-in sheets, forms of identification, records retrieval and use, photo images, and posting personally identifiable information on bulletin boards, in newsletters, in lobby areas, and so on. Determine the necessity for this information and revise processes where appropriate.
- Keep up with changing technologies and laws related to employee privacy and implement additional safeguards as necessary.
- If applicable, let your employees clearly know your company reserves the right to review and monitor all types of communications.
- Implement comprehensive employee privacy policies that include notice and consent language. Identify the activities or areas that are subject to monitoring and tracking. Be sure to address all types of information and monitoring, including monitoring of instant messaging, email, wireless communications, cell phones, work areas, phone conversations, Internet use, and other technologies and information storage media as appropriate.
- Establish procedures and safeguards for protecting employee private information and personally identifiable information in all forms.

Other Types of Monitoring

Monitoring goes beyond just checking one or two types of network activities by using some sort of automated method. There is a very wide range of monitoring activities that organizations need to consider and use to have an effective information security program. At a minimum, types of monitoring to implement should include:

- Intrusion detection to identify when inappropriate access is occurring
- Intrusion prevention to keep unauthorized individuals from getting to information resources
- Systems and applications monitoring to ensure conformity with information security policies and standards
- Systems monitoring to detect unauthorized activities
- Systems monitoring to determine the effectiveness of security measures adopted
- Event logging
- Clock synchronization
- Log file entries standards
- Internet usage
- Business partner connections and related network activities
- Monitoring the effectiveness of security controls
- Monitoring user access to mission-critical and sensitive information

Organizations must determine—based upon their industry, business services and goals, contractual requirements, network configuration, and applicable laws and regulations—what types of monitoring will provide the most benefit and are required.

Awareness and Training

For network security tools to be effective, the tools administrators and end users must be properly trained in how to use them. Awareness and training, in and of themselves, are also highly valuable, but sadly underused, network security tools.

Awareness and training are important activities and key components of an effective information security program. In fact, many regulations require awareness and training as part of compliance. Currently, the most commonly discussed regulations are HIPAA, the Sarbanes–Oxley Act, and GLBA. However, personnel education has been a requirement under other guidelines and regulations for several years. For instance, the Federal Sentencing Guidelines enacted in 1991, used to determine fines and restitution for convictions, have seven requirements, one of which is for executive management to educate and effectively communicate to their employees the proper business practices with which they must comply. Many issues that impact the severity of the judgments, along with accompanying sentences are information security activities.

Much has been written about the need for security and privacy education through effective awareness and training activities. A regulatory education program should address the organization's interpretation of applicable security and privacy laws and regulations as well as support the activities the organization will take to mitigate risk and ensure security and privacy.

Executives must understand not only their own organization's training and awareness requirements but also the related requirements and legal considerations of their business partners, subsidiaries, and parent company. Information security leaders must also consider the training and awareness requirements of applicable international laws and regulations. It is vital for organizations to evaluate, and to reevaluate, the effectiveness of these education programs. Too many organizations spend considerable time and money to launch awareness and training programs only to let those programs then wane, wither, and die on the vine because they did nothing beyond the big implementation; they failed to put forth the effort and activities necessary to evaluate, update, and modify their programs as necessary to be truly effective.

Organizations must spend time not only on creating awareness and training programs but also on evaluating the effectiveness of the information security education efforts. Organizations will find that as they make improvements based upon evaluations, training methods will be more effective.

Legal Considerations

Always include legal counsel in decisions regarding information security and privacy—especially the education program activities. It is important to have knowledge of the legal ramifications and requirements for training and awareness activities. The legalities of information security and privacy risks and managing legal compliance with applicable laws and regulations are a growing concern for managers, lawyers, and human resources (HR) personnel. A plethora of international, federal, and state laws govern how personnel and individuals with access to personal and confidential information must be trained.

> Consequences of inadequate training span a wide spectrum, from regulatory penalties and fines all the way to lawsuits for failure to show due diligence by the training of employees and establishment of an environment that clearly has a standard of due care that is known to all personnel.

There are generally three ways in which an organization may legally establish the duty to train and make personnel aware:

- In certain industries, there may be a minimum standard of care that applies to organizational training and awareness programs. The standard of care is considered the level of activity and conduct expected of similarly trained professionals within similar organizations or industries; for example, in the healthcare and financial fields.
- A statute or a regulatory requirement may establish a standard of care that governs a specific type of information or specific type of industry. For example, the Children's Online Privacy Protection Act (COPPA) governs specifically how information must be handled and controlled, establishing a standard of care over that information. Such expected standards of care, often in combination with an organization's policies and published promises, can result in judicial decisions beyond applicable regulatory fines and penalties.
- An organization's own policies, procedures, and other practices can establish a standard of due care, especially when the organization clearly exceeds any applicable minimum regulatory or statutory requirements. Exceeding requirements can certainly help to draw more customers, establish a better public perception, and increase business competitiveness by showing the organization's concern about security and privacy, which is possibly greater than the competitors'. However, keep in mind that by doing so, the organization may establish a new, higher standard of due care with which the organization must comply. This higher standard could be considered within any potential and related legal action within which the organization is involved.

Summary

Many security practitioners are frustrated with trying to communicate the risks involved and threats to assets to decision makers, only to have the decision makers look at the bottom line cost and then decide it is worth a gamble that nothing will happen if it saves some money by not implementing controls. Some, perhaps many, business leaders are willing to gamble that the risks identified during risk assessments will not happen to their organization because the risk odds are unknown and cannot be communicated to them. However, good leaders do not want to be in noncompliance with laws or legal contracts and put the business at risk of significant negative business impact; or put themselves at risk of taking a potentially long vacation behind bars and/or selling their vacation homes to pay for fines and penalties.

Business leaders must be able to see the financial impact of a security incident or legal noncompliance upon the organization to understand the need for requested information security controls. One security breach can easily cost millions of dollars with impact lasting many years. When the cost of a security incident, and noncompliance with laws and contracts, is weighed against the cost of security solutions/tools, the security defense costs do not seem to be cost-prohibitive.

Exercises to project the cost of an incident and/or legal noncompliance as compared with the cost of controls can be a powerful motivator to executives. There are a number of impact calculators available. I created a comprehensive privacy breach impact calculator for my Privacy Management Toolkit; you can use a free scaled down version at http://www.informationshield.com/privacybreachcalc.html. Apani also provides a free, flexible security cost/benefit calculator at http://www.apani.com/tools/cost-benefit-calculator. Information security practitioners need to recommend what makes sense and is reasonable security-wise for their particular organization. Too many make the mistake of damaging their credibility with their business leaders by asking for large amounts of money to spend on security "solutions" just because it is a "best practice" or a "leading edge" security tool. Security must be implemented to the extent necessary to meet legal and contractual requirements, to demonstrate due diligence, and to mitigate risks to an acceptable level within the particular business environment.

All organizations must implement effective information security programs, which include the use of network security tools. Organizations need to realize that, even if they are not explicitly covered by laws and regulations and have made no data protection promises, they are still responsible for securing data and can be found liable if inappropriate access occurs for the information. Governments worldwide are becoming more proactive in addressing organizational information security problems, incidents, and practices.

On December 1, 2005, DSW Inc. settled United States Federal Trade Commission charges that their data security failures constituted an unfair practice under federal law, ultimately allowing hackers to access the credit card, debit card, and checking account information of more than 1.4 million consumers that were in their systems. This is the seventh FTC case charging a business with failing to exercise due care to protect sensitive consumer information and having inadequate and faulty data security practices.

The proposed settlement would require DSW to establish and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards in addition to obtaining, every 2 years for the next 20 years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order. The proposed settlement subjects DSW to standard recordkeeping and reporting provisions to allow the FTC to monitor compliance for 20 years.

The next chapter will discuss how to manage all these security tools, the security zones, the security layers, and compliance with data protection laws, regulations, and contractual requirements.

Chapter 7: Managing Internal Security

A comprehensive and effective information security program and supporting infrastructure is much more than just hardware and software components. Although most organizations wish there were such a thing, there is no magic information security silver bullet. Effective information security management requires the implementation and coordination of many components. Success requires vigilance by the information security group.

In addition to the motivations for individuals to compromise an enterprise information system discussed in Chapter 1, there are the mistakes and actions resulting from being uninformed that put an organization's information and network assets at risk. Managing enterprise-wide information security is a much larger and challenging task than just the subtask of managing the security of the network perimeter. Information security is a process, not a one-time achievement.

Management Devices and a Pure Perimeter Security Paradigm Is No Longer Effective

It is no longer sufficient or prudent to depend upon securing only the perimeter of the enterprise network with security management devices to protect all the enterprise information assets. The number of new entry points through most enterprise network perimeters can increase on a weekly, or even daily, basis.

The growing number of reported incidents not only demonstrates the impact of multiple breach notification laws but also indicate that organizations may still be focusing on just securing the network perimeter and not sufficiently securing all information assets wherever they are located. The following list highlights a few such incidents that have occurred. As you read through the list, consider how they could been prevented if effective internal controls and security management devices had been in place:

- From Risks Digest, posted by Thom Kuhn, January 27, regarding the auto-complete email feature: "Awhile ago I was listening to a public affairs program on NPR. One of the speakers was representing a trade association, and his comments really got to me. I Googled him and sent him a somewhat venomous email. A few hours later, I got an even more venomous reply. End of story? Not quite. My email address was now in his shortcut list. A few weeks later, I was copied on what was clearly meant to be an internal and confidential email from this gentleman to his colleagues."
- Reported July 11, 2005 in eGov monitor: "Central government departments have reported to have suffered at least 150 cases of computer theft in the past 6 months, according to official figures. The Home Office alone recorded 95 incidents of computer items being stolen between January and June 2005—equivalent to a theft taking place in the department every other day. By comparison, the Ministry of Defense reported 23 computer thefts to date in 2005, down from a total of 153 in the previous year. Ministers made the disclosures in response to a series of parliamentary questions tabled by Liberal Democrat MP Paul Burstow. In a written answer, Doug Touhig, a junior minister at the MoD, said the Ministry had also experienced 30 attempted computer hacking incidents so far in 2005, having only reported 36 for the whole of 2004. However, the Minister gave an assurance that 'none of the reported incidents of hacking had any operational impact'."

- Reported May 17, 2005 in VNUNet: "Lax firewall security is leaving companies open to the installation of malicious software on their internal networks, a newly published Harris poll has warned. Fewer than half of companies block executable files from the Internet, and the same percentage fail to prevent such software coming in via instant messaging. Some 40 percent do not even block executables in email, the major cause of virus infections. The phishing threat was highlighted in the research as a major problem. More than 80 percent of those questioned indicated that their company had received phishing emails, and 45 percent said that employees had clicked through to the bogus Web sites. Lack of awareness is key to this problem, according to the poll. Two-thirds of employees claimed not to know what phishing is, and half of all companies admitted to having no Internet security training."
- Reported December 15, 2005 in The Register: "One in five workers (21 percent) let family and friends use company laptops and PCs to access the Internet, dramatically increasing the chances of infection of the device and potentially the corporate network. This behavior also exposes work documents to prying eyes as well as increased malware infestation risks through use of a potentially unprotected home network connection. More than half (51 percent) connect their own devices or gadgets to their work PC and a quarter of these do so every day. Around 60 percent admit to storing personal content on their work PC. One in ten confessed to downloading content at work they shouldn't. Spanish workers were the worst offenders at this with just under one in five (18 percent) admitting to downloading inappropriate content, behavior that leaves firms at heightened risk to both security attacks and legal sanctions. Two-thirds (62 percent) of those quizzed admitted they have a very limited knowledge of IT security. More than half (51 percent) of those polled had no idea how to update the antivirus protection on their company PC. Most errant workers put their firm at risk through either complacency or ignorance, but a small minority is believed to be actively seeking to damage the company from within. Five percent of those questioned say they have accessed areas of their IT system they shouldn't have (including access to HR and accounting files), while a very small number admitted to stealing information from company servers."
- Reported August 17, 2005 by Reuters: "A judge in New York has sentenced a former employee of America Online (AOL) to 15 months in prison for stealing 92 million screen names from AOL and selling them to a spammer. Jason Smathers, who pleaded guilty earlier this year and cooperated with prosecutors, expressed remorse for his actions and asked the judge for leniency. Indeed, the judge could have given Smathers 24 months in prison for his crimes, which included conspiracy and interstate trafficking of stolen property. AOL has said it suffered monetary losses of $300,000 as a result of Smathers' actions. The judge in the case has given the company 10 days to prove those losses, after which he said he will impose a fine, hinting that he is leaning toward a fine of $84,000."

All these incidents could have been at least mitigated, but most likely prevented, if more attention had been placed upon internal security safeguards and controls. The risky behaviors described could virtually be eliminated with an effective enterprise-wide information security management program.

Unfortunately, too many organizations still believe that the same security management devices used for perimeter security can also be used to manage internal security. Perhaps they can for some activities. However, these perimeter network devices have some serious weaknesses when it comes to securing internal network resources. As discussed in Chapter 4, the network needs to be segregated into security zones; Chapter 5 discussed the need to layer security. These security methods are effective, but the effective management of all of them in unison takes planning and foresight to enable the security to be the most efficient and simple as possible. This process involves more than just the comparatively simple plug-and-play management devices that were used in typical perimeter security implementations. To effectively manage internal security organizations must:

- Understand that managing internal network security is more complex than managing perimeter network security
- Consider the porous perimeter
- Establish enterprise-wide responsibilities
- Comply with contractual and regulatory requirements
- Determine the value of information
- Secure outsourced access to information assets
- Track security program progress and incidents

Managing Inside Is More Complex than Managing the Perimeter

Implementing and managing information security within the network perimeter is much more complex than just managing the security of the perimeter alone. This idea makes sense when you consider what is involved with managing perimeter security. Generally, perimeter security includes four basic components:

- Firewalls
- Proxy servers
- Intrusion detection, and increasingly intrusion prevention, systems
- Malicious code prevention

This comparatively limited number of components is easy for most security administrators to grasp. When adding internal information security management to the picture, most organizations will get a list of components that look something like the following:

- Firewalls not only on the perimeter but also deployed within identified security zones
- Proxy servers not only on the perimeter but also deployed within identified security zones
- Unified intrusion detection, and increasingly intrusion prevention, systems between security zones
- Malicious code prevention between security zones
- Consolidated management consoles
- Unified alerting and reporting
- Unified monitoring
- Encryption systems
- Access control devices and systems
- Audit capabilities
- Policies and procedures
- Application controls
- Network controls
- Systems controls
- And even more information security controls ad infinitum ad nausea

There truly are a limitless number of activities to address for internal security management. The delimited list of activities will be unique for each organization and will depend upon the unique threats, risks, locations, operating systems (OSs) and applications, regulatory and contractual requirements, and industry of each. Table 7.1 compares just a few of the general key security management issues and how they differ from perimeter-only security to enterprise-wide internal security.

Perimeter-Only Security Management	Enterprise-Wide Inside Security Management
Typically one small team is responsible for performing systems security administration for all perimeter security devices.	Multiple teams, typically a different one within each security zone, have their own specific systems security administration rights.
A single set of information security tools and systems are implemented.	The set of information security tools and systems deployed within each security zone may vary greatly based upon the security needs for each zone.
A limited number of audit trails are maintained for the perimeter devices.	A large number of audit trails are maintained throughout all the security zones, systems, and applications.
Overall goal is to protect access to corporate environment	Overall goal is to protect corporate and confidential data.
A limited number of applications and systems need to be secured.	A wide range and large number of heterogeneous systems and applications must be secured.
A small group of people with perimeter management responsibilities must understand and appropriately apply information security practices.	Everyone on the enterprise network must understand and appropriately apply information security practices.

Table 7.1: Perimeter-only vs. enterprise-wide security management.

Effective and efficient internal information security management requires:

- Defining security relationships between data, users, applications, and systems
- Segregating the network into security zones to facilitate effective management
- Enforcing the established security relationships within and across the security zones
- Regularly performing applications, network, and systems audits to ensure security relationships are enforced
- Updating security relationships as business needs, systems changes, and compliance requirements dictate
- Securing data in motion between and within segments and protecting confidential information as well as usernames and passwords
- Creating audit trails and reporting capabilities to demonstrate due diligence and regulatory compliance

Plan your information security infrastructure carefully. Remember, the more solutions you have, the more you need to manage. If you get too many different security tools and solutions, it is likely many will not communicate with each other and you will have a difficult time managing them all. Also, the greater the complexity and variety of management systems, the greater the likelihood of inadvertently leaving a security hole that could expose confidential information or systems. Without proper management, your information security efforts will be ineffective, and ultimately, you will damage your information security program by having it viewed as being too complex, too expensive, and ineffective to boot. Transparency is also important here, as the more intrusive security systems are on users, the greater likelihood of them being circumvented.

Before making an information security management decision and purchase, research the interoperability issues. Many of the current security products are designed to work on a standalone basis and do not work well with other security solutions. For example, some personal firewall programs intended to protect roaming users with VPN connections do not work well with VPN clients.

Although multiple products working together provide a strong security infrastructure, not all solutions work well together.

The Porous Perimeter Must Be Considered

The perimeter is porous. Wireless connections, mobile computing, Web-based applications, back-office connectivity, and connections to business partner and outsourced vendor networks have eliminated the once clearly defined network perimeter. With all these complex relationships, it is difficult to tell who should have access to network components and who needs to be blocked. There are so many ways in which networks can now be accessed that information security management has become more challenging than ever before.

The Information Security Leader's List of "Things That Keep Me Up At Night"

- Wireless networks
- Remote and mobile users
- E-commerce and Web services
- Email attachments and hidden spyware
- Corporate spies
- Disgruntled employees
- Bribed security administrators
- Social engineering and gullible personnel
- Attackers setting up rogue Wi-Fi access points near hotspots tricking users into logging onto their networks
- Newly found security vulnerabilities and how to best apply security patches
- Malicious code
- Outsourced vendors with access to enterprise systems and/or information
- Careless disposal of sensitive information
- Consultants and contract workers attaching their computers to the enterprise network
- Unencrypted data on multiple backup tapes and media

Firewalls, once considered the network security savior, are now mere islands of security in an ocean of threats; they will stop a small percentage of enterprise information pirates, but many more threats exist to the internal network than firewalls alone can stop. Various studies demonstrate how porous the perimeters of almost all enterprise networks have become:

- The CERT/Secret Service 2005 Insider Threat Study reported the predominant means of executing an insider attack was through remote access.
- A 2005 Nemertes Research study reported that 90 percent, on average, of employees work away from the business facilities. Another 2005 Nemertes Research study reports there has been an 800 percent increase in virtual (remote) employees based in different geographies from their managers and peers, from 2000 to 2005.

The fact that organizations today are predominately in part virtual, with IT, sales, support, and executives potentially scattered all around the world has blurred the network perimeter to such a degree that it truly is very difficult to determine where the "workplace" really is. Organizations must understand that in today's world, it is not a question of "if" unauthorized individuals will penetrate their perimeter; it is a case of "when". Inside the perimeter must be treated with the same level of security as has traditionally been provided to the "outside"—including access control and encryption.

Enterprise-Wide Information Security Responsibilities Must Exist

For many years, organizational leaders have regarded the IT unit as being the only area needed to manage and address all information security issues without any need for input or cooperation from other areas of the enterprise. Many business leaders mistakenly believed the only threats to data were electronic threats. As more accountability is created for business leaders to ensure information security, and as they then become more aware of the related issues, they are starting to understand that information security must be integrated throughout the entire enterprise. To be most effective in integrating information security responsibilities throughout the organization, two very important factors must exist:

- Information security must be clearly supported and promoted by the highest executive leaders within the company.
- The information security function needs to be as high in the corporate structure as possible in order to set and enforce information security directives and policies. As history has proven, unless the information security department is powerful enough to establish and enforce information security administrative, operational, and technological initiatives, the rest of the organization will not follow information security requirements but instead choose ease of use and functionality; they see information security as inhibiting.

Security Goes Beyond Technology Products

Simply implementing firewalls, VPNs, IDS servers, and auditing products will not create a secure environment. Unfortunately, many organizations believe this product implementation is all they need to do and, as a result, many have experienced some significant information security incidents. Technology tools certainly are part of the solution. However, risk assessment, information security strategy, operational procedures, security education, and appropriate personnel behaviors are also necessary components.

Education Is Imperative for Success

If you expect information security to be addressed enterprise-wide, you must implement an effective information security awareness and training program to educate all personnel about their responsibilities and policies and procedures. Awareness must be an ongoing activity. Training must be regularly provided and mandatory. Executive leaders must actively support these efforts.

The enterprise information systems and information assets are not secure until all personnel know and understand the importance of securing information and network resources as it relates to their job activities. People truly are the weakest link in enterprise information security programs.

According to the Deloitte 2005 Global Security Survey:

Only 65 percent of organizations have trained their personnel how to identity and report suspicious information or network-related activity.

Only 6 percent of organizations provide information security education as part of the new hire orientation.

Even though 86 percent of organizations are concerned with employee misconduct involving information systems, the amount of funds allotted to the awareness and training budget was less in 2005 than it was in 2004.

You cannot expect your personnel to know how to do the right thing if you do not effectively teach them what the right thing is to do!

Centralization and Decentralization

As discussed in Chapter 5, a centralized security management area with ultimate enterprise-wide security oversight has distinct benefits to organizations, including increased security efficiency, economy of scale for security implementation, and the ability to enforce security requirements centrally through monitoring, evaluation, security activity, and program updates.

There are also appropriate activities that through divide-and-conquer methods can be made more efficient and effective. Decentralized security management will help to ensure appropriate and cost-effective security is addressed within each of the organizational business and operations areas. It can also be used to more effectively ensure appropriate authorization is given to personnel based upon their job functions and to more effectively incorporate security into all the business processes.

The key is to identify those activities that are best performed centrally and which are best performed within each of the business units. The right combination of the two will lead to cost reduction, better risk management, regulatory compliance, and more effective security operations.

Cost reduction through the right combination of centralization and decentralization can be achieved in such areas as:

- Password resets
- Demonstration of compliance with enterprise policy and security/privacy regulation
- Awareness and training
- Adequate service level provision
- Access administration
- Acquisition and maintenance of security solutions
- Account disablement for dismissals and job changes

The right combination of centralization and decentralization can also result in better risk management practices, helping enterprises better address the following questions:

- Who can access the enterprise's sensitive information databases and intellectual property?
- What is the enterprise's vulnerability to new or existing threats?
- What is the state of the enterprise's compliance with its own security policy, guidelines, and procedures, and how can compliance be enforced?
- How quickly can the enterprise react to new threats (assessment, solution design, solution testing, and solution/patch implementation)?
- How can the enterprise mitigate the security weaknesses inherent in users having to remember multiple user IDs and passwords?
- How can the enterprise be confident that its systems are configured securely, as the IT professionals doing so are not necessarily security professionals?
- Are user actions contributing to, or detracting from, security?

Contractual and Regulatory Requirements

It is vital to ensure that information assurance activities support, and information security leaders understand, the existing regulatory and legal requirements for safeguarding information throughout the enterprise. The penalties, fines, and jail time for noncompliance can have a devastating impact on not only the business but also the business leaders personally.

Contractual Requirements

Unfortunately, many information security leaders have not been informed of, or have not thought about, the types of safeguards they must put in place to comply with existing third-party business partners. Visa provides a good example of the importance of contractual requirements for information security.

When Visa announced the Visa Cardholder Information Security Program (CISP) in April 2000, and mandated compliance by June 2001, the organizations that processed credit card purchases suddenly realized the importance of such contracts. Visa gave merchants and service providers until September 30, 2004 to submit their compliance documentation.

> The Visa CISP requires organizations to implement security to comply with 12 basic security requirements, including implementation of appropriate physical and logical controls and performance of regular audits. The program also requires organizations to immediately report security incidents as well as be able to investigate and take appropriate action to limit exposure of cardholder information. Organizations in compliance are automatically indemnified against any fines.

All entities that stored, processed, or transmitted Visa cardholder data were required to comply with CISP and were responsible for ensuring the compliance of their merchants or agents. If organizations did not comply, Visa contractually reserved the right to fine them up to $500,000 per incident. Very large organizations were scrambling to comply with the Visa requirements because they had been notified, after sending a perfunctory checklist to Visa to demonstrate their compliance, that they needed to provide solid documented evidence of their compliance or they would have their ability to process Visa card payments discontinued.

> On December 15, 2004, credit card associations created a set of industry security requirements referred to as Payment Card Industry (PCI) compliance. Generally, the agreement among the credit card industry was that, if a merchant is Visa CISP compliant, MasterCard, American Express, and Discover would honor the CISP compliance and consider the company PCI compliant.

In the past few years, I have performed many security reviews for organizations' business partners, and almost all the contracts the organizations had with the third parties contained some very clear information security requirements within the Master Service Agreements (MSAs). However, upon speaking with the third-party representatives responsible for information security, I found that only a small handful were even aware that the MSA contained such information security requirements. In today's business environment, contracts with third parties should include requirements to protect information. A breach of contractual requirements could result in a costly court action.

> Organizations must include information security requirements within the contracts they have with their business partners and know their contractual information security obligations.

Regulatory Requirements

Governmental regulations cover almost all aspects of corporate operations, scrutinizing and controlling everything from how the physical security of computer labs are managed to how new employees are trained on security responsibilities. Security management is at the heart of almost all data protection regulations. Without a strong security infrastructure that protects systems, applications, data, and processes from unauthorized use or access, compliance with any regulation is very difficult. The requirement for strong security management cuts across all major regulations.

Staying on top of legal and regulatory compliance is a comparatively new, but hugely important, task for managing internal security. Table 7.2 provides a high-level overview of the information security requirements of prominent laws and regulations.

Regulation	Example of Information Security Management Principles Covered
Sarbanes-Oxley Act (SOX)	Continuity of secured network operations Data confidentiality Data retention Detailed auditing capability Enterprise and application-level policy enforcement Secured information access
Gramm-Leach-Bliley Act (GLBA)	Application-, systems-, network-, and data-level security Data confidentiality Data secured in transit Detailed auditing capability Security and integrity of stored data
Health Insurance Portability and Accountability Act (HIPAA)	Application-, systems-, network-, and data-level security Authentication and access controls Data confidentiality Data retention Data secured in transit Detailed auditing capability Security and integrity of stored data
California State Bill 1386 (CA SB 1386)	Alerting capability with reporting Confidentiality of personal data Detailed auditing capability Detailed policy controls Monitoring capability Notification procedures Personal data secured in transit Security of personal data in storage

Table 7.2: Overview of the information security requirements of prominent laws and regulations.

As you can see, there are some very apparent commonalities between these regulatory requirements. This chapter will discuss this idea in detail a little later.

And Many More Regulations Worldwide

The number of data protection regulations is increasing rapidly. It seems a week does not go by without reading about a new proposed bill or law. Just a few of the other existing laws and regulations impacting information security management, beyond those discussed earlier, include:

- Canada: Personal Information Protection and Electronic Data Act (PIPEDA) of 2000
- European Union Data Protection Directive of 1998
- Japan: Personal Information Protection Law of 2005
- Australia: Privacy Act of 1988
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) of 2001
- Children Internet Protection Act of 2001 (CIPA)
- Fair Credit Reporting Act of 1999 (FCRA)
- Children Online Privacy Protection Act of 1998 (COPPA)
- Privacy Act of 1974

> ☞ Effective information security management practices must include a way to stay up to date with all the laws and regulations that apply to the enterprise.

Common Regulatory Data Protection Requirements

In a panic to answer corporate executives' questions regarding their accountability requirements for specific information protection practices, and meet the "letter of the law" for each individual regulation, many information security and privacy professionals have been trying to address regulatory requirements in a piecemeal fashion, looking at one law, and the corresponding minute applicable detailed requirements, at a time. This practice is not only stressful to those responsible for compliance but also generally inefficient.

As Table 7.2 demonstrates, when you examine the multitude of data protection laws and regulations, common themes of information security requirements reappear. By viewing these commonalities between the regulations and managing information security to them, then addressing any outstanding specific requirements within any one particular law, information security management will be much more effective.

Figure 7.1 illustrates common information security management areas covered by most of the major regulations. Although each regulation typically includes specific differences within these areas, a common requirement of all regulations is for organizations to have implemented a strong set of information security controls and practices to protect critical enterprise information assets. A strong information security management platform is necessary to achieve this requirement.

Secure Data Storage	Change Control Management	Disaster Recovery & Business Continuity	Documented Policies & Procedures	Security & Privacy Accountability
Records Management and Retention	Configuration Management	Physical Security	Risk Assessment	Training & Awareness
Access Control Management	Monitoring & Auditing	Identity Management	Secure Data Transmission	Incident Response

Figure 7.1: Common information security regulatory requirements.

Determining the Value of Information

Very important, but sorely lacking in most organizations, is an inventory of information assets that have been classified according to their sensitivity and criticality. Especially with today's regulatory requirements to notify individuals of security breaches, it is a necessity to know the information you have and where it is located, if you expect to know when the information has been compromised.

After you have your inventory of information compiled, you can ensure appropriate security is applied based upon the value of the information. It is not feasible, or prudent, to try to secure all information at the same level. By knowing the value of the information, you can then more successfully manage the security within your security zones and layers by applying the most robust security within the zones in which your high-value information assets are located. In addition, you can use appropriate mechanisms within the security layers, which will prevent you from investing as many resources in those zones that have information assets with lesser values.

Information Valuation

So what is the value of information? There are few, if any, organizations that do not place a high dependency upon information for their business success. This dependency alone has great value.

There are many types of enterprise information, including customer data, patient files, accounting records, Human Resource files, marketing plans, product designs, emails, and basically an infinite number of others.

The amount of information within an enterprise is growing exponentially. Consider email. According to IDC, a typical 1000-user organization generates more than 3 terabytes (TB) of email data annually. CIOs, CTOs, legal, IT departments, and enterprise managers in every industry must address the growing challenge of complying with multiple regulations that cover the types of information found within email messages.

> 🕮 IDC reports the current (2006) number of daily emails worldwide is 35 billion.

The value of information is greatly impacted by the state, federal, and regulatory requirements governing the management and safeguarding of information. Noncompliance with those information-handling directives can, and has, cost organizations millions of dollars. The value of each kind of information changes as it goes through its life cycle. The usefulness of information typically lessens. However, the financial impact of a breach to sensitive information can be as damaging no matter where in the life cycle information is.

Organizations need to determine the types of information that could have the most financial impact and build security around those high-value items appropriately. What will make this task challenging are the many unstructured forms in which sensitive information may be saved, such as in email, Word, Excel, PowerPoint, and other type of end-user controlled formats. This challenge highlights the need to implement a clear, strongly supported set of information security policies that contains a very good information classification policy.

Considerations for Outsourced Access to Information Assets

Many organizations are outsourcing very specialized data processing and management activities in an effort to save money or because they just don't have the resources, experience, or capabilities to do it themselves. Organizations also often outsource to get specific expertise that they may not possess and cannot afford to hire full time. Organizations that outsource application programming probably expect that the individuals doing this work will know about application security and will incorporate it into the product they create. These same organizations probably also expect the individual to know how to protect information in a shared customer environment; making sure that the code created for the organization is not accidentally sent to another customer, and so on.

When an organization entrusts third parties with the organization's confidential data, they basically place all direct control of security measures for the data completely into the hands of someone else. That trust cannot be blind. Numerous recent security incidents have resulted from loose security practices within outsourced third-party organizations:

- Reported January 12 2006: UPS lost People's Bank computer backup tapes containing clear-text information about approximately 90,000 customers.
- Reported December 16, 2005: DHL lost an ABN Amro computer backup tape containing clear-text information about approximately 2 million customers.
- Reported March 17, 2005: A computer at Boston College with access to an alumni database was infected with a virus that might have exposed personal information about more than 100,000 individuals. According to officials at the college, the computer was operated by a third-party IT service, which officials declined to name.
- Reported May 2, 2005: Iron Mountain Inc., lost Time Warner Inc.'s computer backup tapes with clear-text Social Security numbers and names of 600,000 current and former employees and dependents. This was the fourth time so far in 2005 that Iron Mountain lost tapes during delivery to a storage facility.
- Reported October 7, 2004: A Pakistani transcriptionist (a subcontractor) hired to transcribe records for the University of California San Francisco (UCSF) Medical Center, informed UCSF via email that she would post its patients' private medical records on the Internet if she was not paid for the work she was hired to do by the company she was subcontracted by—Texas MT. Texas MT was subcontracted by a Florida subcontractor, Sonya Newburn, who was hired by a Sausalito, California company, Transcription Stat, which was contracted to provide transcription services to UCSF.

When organizations outsource critical data processing and management activities, they must implement measures to stay in charge of their own business data security and minimize business risks. Many organizations indicate the security issues related to outsourcing are a big concern. Alarmingly, it seems few organizations actually address this issue.

In a May 15, 2005 CIO Magazine article titled "Don't Maroon Security," Atul Vashistha, CEO of NeoIT, an offshore outsourcing consultancy, said, "I'd say fewer than 20 percent of my clients audit the security of their providers. They just accept the suppliers' defined security plan and don't check to see if they are living up to it." Steven DeLaCastro, a consultant with offshore outsourcing company Tatum Partners, indicated he believes it is more like 10 percent. "Sarbanes-Oxley requires the right to audit outsourcers, yet companies aren't putting [audits] into the contract," he said.

How do you know the third party is complying with your regulatory responsibilities? How can you demonstrate to regulators that you are in compliance when someone else possesses your data? You need to hold third parties to strict security standards. In many instances, such standards will be more stringent than your own organization's security requirements.

The measures you take to make sure your business partners are taking appropriate actions to protect the data with which you've entrusted them depends upon the situation and existing legal restrictions. The following list highlights general actions you should consider taking:

- Require a potential third party to provide a copy of a recent security audit of their operations that was performed by an independent reputable party. Even if the audit is broad, it will demonstrate they have gone through an audit by a reputable company.
- Require third parties to complete a security self-assessment questionnaire, provided by your company, about their information security and privacy program. When creating this questionnaire, it is an effective practice to structure the questionnaire around the ISO/IEC 17799 topics as they apply to third parties protecting another company's information.
- Include security and privacy requirements within the contracts you have with third parties. Include enough detail that you cover all issues but don't be so specific that you allow them a way to avoid doing a security activity just because you did not specifically state it within the contract. Include within the contracts citations of the specific laws for which your company must comply that the third party must also then comply with.
- Require third-party personnel to have training for appropriate security practices prior to handling or accessing your company's information. Don't limit the training to electronic data; if they handle storage media such as paper documents, make sure it is covered in the training. Require regularly scheduled training and awareness to occur following the initial training.
- Review the third party's information security policies. Ensure the policies cover all the topics related to the activities they are performing for your company. Ensure the wording is strong enough to actually impact the personnel activities. Look for executive endorsement of the policies and for clearly stated sanctions for policy infractions.
- Require an abbreviated form of the self-assessment form, a type of information security and privacy attestation, again provided by your company, that they must complete each month, have their executives sign, and submit to your company as a requirement of continuing to do business. The signatures and contract language will help to demonstrate due diligence on the part of your company and will also hold the third party to a legal standard of due care.
- For third parties handling particularly sensitive and/or regulated information, require a clean-room environment to keep information from walking out the outsourced company's door. In a clean-room environment, all the machines and output devices except for terminals are disabled. Copies of data cannot be made, hard drives cannot be used, PDAs cannot get information downloaded from any of the computers, and data is otherwise not available for downloading, printing, copying, or accessing beyond the contracted purposes. The servers reside in your country of residence. There is no way for the information to leave the outsourced company. Typically, in such arrangements, the outsourced company's employees are physically searched when entering and leaving. These are very strict precautions, so they will not work for every company, but they definitely should be used if your level of risk warrants such measures.

- Limit the amount and types of information the outsourced personnel can see based upon the business needs. For example, if the outsourced company verifies a customer is a good credit risk, don't send all parts of the application; just send the information required to approve the application.
- Require criminal and, where appropriate, financial checks to be performed on the third-party personnel prior to their hire. No matter how many safety precautions are taken, it's difficult to stop an opportunist who will steal data for money, revenge, or some other reason. Ensure that the people handling your data have not been convicted of criminal activity that would make them a high risk for handling your data. This may be tricky in some countries because records of criminal activity may not be centralized or such information may be labeled differently. As mentioned earlier, and worth emphasizing again, make sure the outsourcing workers are trained properly about procedures and legal consequences.
- Make sure none of your disgruntled ex-employees are now employees of the organization to which you are outsourcing your data handling. Such situations have led to devastating situations for companies.
- Send personnel from your company to visit the outsourcing sites regularly to view the facilities, meet employees, and monitor employee turnover and subcontracting activities.
- Find out how the third party screens and monitors employees. It is ideal to require that they perform criminal, credit, and reference checks as part of their background check process. However, this is not possible in some countries that do not have a centralized criminal database system. It is also not possible in some countries where doing such checks are against their privacy laws.
- Obtain documentation for how the third party will handle a system breach. Formal breach identification and notification procedures should exist.
- Determine where disputes will be resolved. Have you contractually required that any legal actions will be resolved in your jurisdiction? Make sure you discuss this carefully with your legal counsel.
- Ensure the third party has liability insurance and identify what the insurance covers. If there is a problem that occurs with your information while in the third party's control, liability could rest with your organization—and will likely rest with your organization if the third party is located outside your country.
- Identify the laws and regulations that apply if a system breach occurs at the third party.
- Determine whether your organization's liability insurance covers outsourcing activities.
- Contractually require the third party to obtain your organization's authorization before they subcontract any work that involves your organization's information or access to your systems.

Common Weaknesses

The following list notes recurring vulnerabilities for third parties; be sure to pay particular attention to these:

- The information provided within the vendor's security self-assessment responses often does not match the security requirements within the third party's security policies. For example, the respondent for the self-assessment may indicate the passwords used are a minimum of six characters, but the policy may indicate passwords must all be a minimum of eight alphanumeric characters. Such conflicting information should raise a red flag for you; it may indicate the third party does not enforce compliance or communicate the security policy requirements to its personnel.
- The third party may be subcontracting the processing of your data to yet another company that does not have good security practices and/or may be located in a different country from yours or the third party. Be sure to cover this within your contract with the outsourced company.
- The third party may not have any security policies or controls in place for mobile computing devices (laptops, PDAs, Blackberries, smart phones, and so on) or for their employees who work from home. However, they may have personnel who use these types of computers to process your data. Be sure appropriate security is in place for such situations.
- Business continuity and disaster recovery plans are often either missing or were written several years ago and never tested. Make sure the third party has up-to-date plans in place and tests them regularly.
- The third party may have been involved with a security or privacy breach. There are multiple services you can use to check on this in addition to dozens to hundreds of useful Web sites to search for news about the third-party company and any security breaches for which it was involved. If you find the vendor had a breach, be sure to ask the company about it and find out what actions they have taken to prevent such a breach from occurring again.

A few of the sources to check whether an organization has been involved in a security or privacy breach include:

- http://www.google.com
- http://www.bna.com for the Privacy and Security Law Report
- http://www.ftc.gov
- News sites such as http://www.CNN.com
- http://www.supremecourtus.gov (Supreme Court Cases)
- http://www.virtualchase.com/resources/criminal_records.html (Criminal Records Check)

- Encryption is often not used to protect information in storage, in transit, or on mobile computing media and devices, such as laptops, PDAs, backup tapes, USB drives, and so on. Be sure encryption is used by the vendor to mitigate the risk involved in such situations and when the company is storing information from other companies in the same servers as they are saving yours.

Tracking Progress and Incidents

Unfortunately, information security leaders cannot track their success and progress with information protection initiatives. Not only is it wise and necessary to track information security progress and incidents in order to have an effective information security program, it is a requirement of many laws and regulations. The following regulation examples illustrate this requirement:

> The HIPAA Security Rule requires covered entities in § 164.308 Administrative Safeguards:
>
> *(a)(1)(ii)(D) Information system activity review*
>
> *(Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*
>
> The GLBA Safeguards Rule requires covered entities in § 314.4 Elements:
>
> *(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.*

Effective information security leaders will establish formal monitoring and program evaluation procedures and implement appropriate tools to help them keep up with the day-to-day status of their enterprise information security posture.

Items to Monitor and Log

There is a wide range of activities throughout your enterprise you will need to monitor, and multiple types of activities you will need to log. These will not all be electronic based. You should have identified many of them while establishing your security zones (discussed in Chapter 4) and implementing your layers of security (discussed in Chapter 5).

Carefully consider the cost, resources, and liabilities associated with each considered logging and monitoring activity.

The following list highlights items most organizations will need to log to meet compliance with a wide range of regulatory requirements and keep up with an ever-changing network environment in which new threats are introduced every day:

- Email messages and activity
- Paper mail
- Work areas
- Log-in attempts
- Voice communications
- Access to personally identifiable information
- Software and system vulnerabilities and patch updates
- Malicious code (viruses, Trojans, spyware, worms, and so on)

- Personnel awareness and training activities
- Network and remote access points and connection activity
- Mobile device inventories
- Business partner contracts
- Enterprise-wide compliance with the organization's policies
- Authorization capabilities
- User access capabilities
- Backup tapes and media
- Disaster recovery plans and sites
- Systems administrator activities
- Intrusion detection and intrusion prevention systems
- Data and media disposal records
- Regulatory compliance

As you can see, this list covers all the layers of security you need to have implemented throughout your organization.

The logging and monitoring activities you implement within your organization need to be determined based upon an analysis of the risks to your enterprise's unique network and systems environment.

Auditing and Tracking Mechanisms

Establish auditing and tracking mechanisms for personally identifiable information and other sensitive and mission-critical information. Doing so will likely require one or more of the following:

- Audit software and systems
- Database logs
- Servers dedicated to housing the audit and monitoring logs and information
- Secured physical locations to house the audit and tracking information
- Sign-in sheets
- Closed circuit television and other surveillance equipment

Summary

If all you do is protect the perimeter, you will lose the information security battle. Effective information security management requires security throughout the entire enterprise. To effectively manage internal security organizations must:

- Establish information security management with the understanding and expectation that it will be more complex than simply managing perimeter network security
- Realize the network perimeter is increasingly porous and address all the many ways in which threats can enter the insider of the perimeter as well as mitigate the risk within the perimeter when it is penetrated
- Establish a comprehensive enterprise-wide information security framework that includes not only centralized responsibilities but also decentralized information security functions
- Identify, understand, and take action to comply with contractual and regulatory data protection requirements
- Identify and inventory the information stored, handled, and processed by your organization, then establish appropriate security for the information based upon the determined value
- Take action to ensure the security of information assets that are handled, stored, or accessed by outsourced business partners
- Ensure that—as much as possible—your security elements are automatic and transparent to users.
- Track and monitor information security program progress, security incidents, and incident resolutions

The next, final, chapter will discuss how to put together the ideas and practices discussed so far into an effective enterprise-wide information security management plan.

Chapter 8: The Recipe for Security Within the Perimeter

The past seven chapters have discussed the myriad reasons why organizations must address security within the perimeter as diligently, or even more so, than they approach security of the perimeter. This chapter will boil all this information and advice down into an information security recipe for effectively addressing security within the perimeter. With this in mind, this chapter reviews the key concepts within each chapter, then identifies the key actions organizations need to take—the information security recipe—to ensure the entire enterprise is secured within the perimeter.

New Threats Continue to Emerge for the Same Security Issues

Executives must be concerned about and address information security in today's business environment. Information security incidents not only cost companies significant time and money to resolve, they also significantly impact company brands, customer loyalty, and reputations and can have hard-hitting legal penalties, fines, and long-lasting judgments—with many consent orders requiring annual reviews and audits for 20 years.

The threats and challenges for today's business information processing environment are many:

- Network perimeters are now like sieves—The well-defined perimeter has disappeared. Mobile employees, wireless access, Web-based applications, remote workers, contractors, and business partners who have access to your network have put an end to the perimeter fortress. Attacks can come from anywhere at any time.
- Issues are nothing new, but the threats continue to grow—Businesses face numerous issues with regard to handling and protecting information. The number and type of threats created by computers and innovative technologies continues to grow.
- Urgency to address old problems with new solutions—Businesses must address the problems of technology evolving faster than the associated security solutions. Businesses must keep employees vigilant with their security practices for mobile computing devices. What used to work is no longer effective.
- Scalability—The internal network environment presents unique challenges compared with perimeter security. Internal security involves significantly greater scale of the environment, scope of the environment, numbers of users, speeds, and volume of traffic.
- Multi-national considerations—Businesses must comply with world-wide regulations to ensure the privacy of their customer information as well as the security of the intellectual property that resides on internal networks. These global requirements drive an increased need for internal security. There is also an increased awareness about malicious network attacks on internal networks that can be launched from anywhere in the world.
- Addressing compliance issues and requirements—Numerous laws and regulations mandate businesses maintain adequate information safeguards and controls to ensure that only authorized individuals are able to access personal information, and to ensure the continued availability and integrity of the information.

Gumball Security No Longer Works

The long-used gumball approach to securing networks by making the perimeter like a hard outer impenetrable shell and leaving the inside of the network soft with less vigorous security in place is no longer effective or acceptable.

Addressing Security Within the Perimeter

The overall value of data inside the perimeter has skyrocketed, which has lead to a new class of cyber criminals who are organized, well funded, and very focused on attacking organizational data. At the same time, the perimeter is becoming more porous, and attackers have new techniques for bypassing perimeter security barriers.

The attackers are not only coming from the outside—the increased value of data elements also represent a significant temptation for internal people, and these internal threats in many ways are more dangerous than external threats because the internal threats are difficult to detect and prevent.

Network perimeter security can be defeated in many ways—for example, by tricking inside users and systems to execute code containing worms, which then spread to other systems behind the firewall, and by tricking users who have JavaScript and ActiveX enabled in their Web browsers to execute malicious code hidden in external Web sites.

Identifying Internal Security Requirements

Businesses must identify security requirements in the context of how those requirements impact business with regard to existing risks, threats, vulnerabilities, and legal and contractual requirements. Alternative paths into organizations, along with application-layer attacks, are increasing the threats that highlight the need to complement perimeter security with a comprehensive and pervasive range of internal security activities and tools.

At a high level, there are three main ways to identify security requirements inside the perimeter:

- Assess risks to the organization, taking into account the organization's overall business strategy and objectives. A risk assessment will identify threats to assets and network components and evaluate the vulnerability and likelihood of occurrence.
- Identify legal, statutory, regulatory, and contractual requirements with which your organization, trading partners, contractors, and service providers must comply.
- Take into consideration the particular set of principles, objectives, and business requirements for information processing that your organization has developed, formally or otherwise, to support its operations.

A Wide Range of Factors Are Working Against Securing Just the Perimeter

Tribal thinking must change. Businesses cannot blindly trust that everyone with access to their internal network knows the right things to do or will not do bad things on purpose. The numbers of people with access to the typical business network goes well beyond employees. And employees are often motivated to take advantage of operational and systems weaknesses to inappropriately obtain information or wreak havoc on network and systems resources availability.

Trust Where Trust Makes Sense

Not only are security measures necessary to help protect against the malicious activities of those employees who cannot be trusted, such security measures are also necessary to help protect against well-meaning employees' mistakes and lack of knowledge that could lead to business-closing incidents.

Preventing Crime by Insiders Is Difficult

It is difficult for companies to guard against crimes in which internal staff is involved. This reality makes it even more important to implement internal security measures.

New Technologies Make Securing Networks Increasingly Difficult

New technologies make it very easy to link networks and information. Authorized network users who do not realize the threats they present use new technologies widely inside the network, often without the knowledge of management. Inexpensive technologies are easily accessed by large numbers of people, employees, and outsiders alike. More employees work away from the office and on their home computers. Putting security responsibilities and decisions into the hands, and control of, employees makes businesses more vulnerable to unauthorized network intrusion and abuse. Recent studies demonstrate the devastation insiders can have on network and information resources.

The Perimeter is Porous

Perimeter-based security fails because there is no longer a clearly defined perimeter. An explosion in outsourcing, mobile computing, wireless networking, business partner connections, and Web-based applications has created a spider web configuration of connections to virtually anyone, from anywhere, with any device. Significantly large numbers of individuals who are not employees have access to business networks and information. A "trusted" internal network environment is now likely connected directly to the Internet through a home or partner link or through an unapproved wireless connection.

Mobile and wireless computing increases threats to business because:

- Business use of these technologies is increasing. The top-tier executives are among those most likely to make extensive business use of mobile computing devices; they are also the personnel with the most critical and confidential business information.
- Mobile devices store increasingly large amounts of data. Handheld computing devices are now capable of storing gigabytes of information. If a mobile computing device or memory stick falls into the wrong hands, it is likely to expose huge amounts of business information, potentially including customer information, business email, corporate plans and strategies, and so on.

Legal and Regulatory Compliance

Regulations and laws governing the implementation of information security safeguards are becoming more common. Virtually all businesses are impacted by legislation with which they must comply. Penalties and fines for non-compliance with these requirements can have a huge impact upon an organization.

Inappropriate Technology for the Purposes Being Addressed

Organizations have often tried to use inappropriate technologies to address internal network security challenges, often spending inordinately too much time and money trying to create in-house solutions or succumbing to false promises of vendors selling them software and hardware that really doesn't address their business environment and needs. Security solutions must be appropriate to the risks, threats, and vulnerabilities being addressed to be effective.

Increasing Data Value Increases Threats

Data is extremely valuable to business. This value is another compelling reason to protect data in all places.

Organizations Must Implement Multi-Dimensional Enterprise-Wide Security

Multi-dimensional security protects information assets and associated resources within all areas of an enterprise and in compliance with all regulatory, policy, and contractual requirements. It places protection at not only the perimeter but also wherever information is stored, processed, or transmitted.

Multi-dimensional security involves more than just technology solutions; it also utilizes operational, administrative, and human forms of protection to help reduce the risks to information wherever information can be found.

Multiple Protection Strategies Are Needed

There is no such thing as a single solution that, in and of itself, will secure all enterprise information assets and systems in compliance with all contractual and legal requirements. Multiple protection strategies must be used to most effectively reduce and manage the risks that exist within today's highly decentralized and widely connected systems.

Risks Today Are Different Than Those of Yesterday

Businesses used to address risks within the insurance coverage portfolio for the organization. Information security risk was not something that business leaders considered when risk management was discussed. Smart business leaders now know information is a cornerstone of successful business, and needs to be effectively protected to reduce the risks to the confidentiality, integrity, and availability of the information.

Risk Assessment and Analysis Methodologies

There are a wide range of risk analysis and assessment methodologies and technologies. Organizations must choose what is best for them based upon their business environment and the goals for their assessment.

You Cannot Predict the Future… But You Must Still Identify Your Risks

Organizations cannot realistically calculate with any amount of accuracy the threats that will impact their organization or the dollars needed to invest in information security. However, performing risk assessment/analysis is still necessary for businesses to be able to understand information risks and to determine which controls and tools to use to prevent the risks. The most realistic way to do so is through the use of qualitative risk analysis based upon regulatory requirements and the potential impact from non-compliance fines and penalties. The assessment/analysis should then communicate what the financial impact experiences for each risk have been in other companies.

Risk Analysis and Assessment Must Be Part of a Multi-Dimensional Security Strategy

Business leaders must recognize two facts:

- Each information system and process has its own risk environment
- Each information system and process has its own unique inputs, outputs, level of activity, and associated costs

Because of these differences, each information system and process has unique security requirements that are determined by the associated risk environments.

Security Policies, Procedures, and Standards

Information security policies, procedures, and standards are all important and organizations must formally document and implement them to have an effective information security program as well as to comply with multiple data protection laws and regulations. Each type of document serves a different purpose.

What Does an Information Security Policy Do?

An information security policy establishes the framework within which the business rules and regulations for handling information and reducing risk are described. Effective policies are created to help bring the organization into compliance with applicable laws and regulations as well as to address how to secure the business information processing environments within the organization.

What Does an Information Security Procedure Do?

Information security procedures describe how to implement the policies. Procedures document the step-by-step detailed actions necessary to successfully complete a task that supports the policies. Procedures provide personnel with the information necessary to complete a task and provide assurance to management that the tasks are being completed in a consistent approved manner. Procedures improve efficiencies in employee workflow and assist in the prevention of misuse and fraud.

What Does an Information Security Standard Do?

An information security standard is a detailed specification for hardware, software, and human actions to support the information security policies. Standards can detail the requirements for a wide range of issues, from the software and hardware that must be used to the remote access protocols that must be implemented to describing who is responsible for making information security approvals. Standards provide a documented way of ensuring that programs and systems will work together. By establishing standards, the enterprise limits the possibility of rogue application, systems, platforms, hardware, or software; in addition, there is less time spent in supporting non-standard activities or products. In short, standards define cost-savings processes that support the efficient running of the enterprise.

Regulatory Requirements for Information Security Documents

Many laws and regulations require organizations to formally document data protection requirements in policies and procedures. Additionally, these documents demonstrate that a standard of due care has been established within the enterprise.

Education

Organizations must supply personnel with the information they need to appropriately safeguard data while performing their job responsibilities. If personnel do not know or understand how to maintain the confidentiality of information, or how to secure it appropriately, organizations risk having information mishandled, inappropriately used, and obtained by unauthorized persons, as well as being in noncompliance of a growing number of laws and regulations that require certain types of information security and privacy awareness and training activities. Issues under the United States Federal Sentencing Guidelines that impact the severity of the judgments include consideration of the types of training and awareness organizations provide to their personnel.

Audit and Validation

Security audits and compliance validation reviews provide an in-depth examination of an organization's security infrastructure, policies, people, and procedures. When performed effectively and successfully, they will identify areas of weakness within the infrastructure. The auditor or reviewer can then provide recommendations for appropriate actions to address the weaknesses and reduce the accompanying risks.

Simplifying Complexity

The enterprise information security strategy must simplify the complexity resulting from highly diverse, dispersed, and multi-dimensional environments. Organizations must simplify the complexity of information security management by taking the large number of technology, human, and compliance issues and making them understandable to the business, while at the same time implementing solutions to integrate them throughout all business processes so that information security is built into all products and services from the beginning of a business idea right through until the resulting service or product is no longer offered.

Information security complexities can be simplified using a common framework of information security disciplines and by obtaining the support and cooperation of leaders throughout the organization rather than focusing on each individual issue one at a time. The first step in simplifying information security is by appointing an enterprise-wide information security position to oversee and coordinate information security activities and decisions for the entire enterprise. This position will not only be the first step in simplifying complexity but also lead to consistency in addressing information security issues throughout the enterprise.

Use Security Zones

Business leaders must not only be aware of, but also strive to be in compliance with, the multitude of regulations that are applicable to their companies. This complexity can be made more manageable and more clearly provide demonstration of due diligence by tackling the requirements in zoned chunks across the enterprise.

Establish Network Security Zones

The network should provide a solid first layer of defense against outside attacks, complementing operating system (OS)- and application-level security. Separating the network into security zones allows security managers to consolidate resources in a cost-effective manner and control user access to each application and related information. The network then creates a secure environment not only at the perimeter but also in security zones throughout the enterprise.

Enterprise Security Zone Management

Dependence on the network, along with functional enhancements to the business systems, increases the importance of security and dependable accessibility to information. Implementing network security zones helps organizations achieve their goals of scalability, availability, security, manageability, performance, supportability, and geographic distribution, while realizing savings at many levels throughout the enterprise. Enterprise security zones must be centrally managed to be most effective and prevent gaps. Enterprise network security zoning provides many benefits to the enterprise:

- Streamlines business processes
- Mitigates risk within the network perimeter
- Saves organizations time, money, and human resources
- Reduces operational risk

By implementing security zones, an organization will shift reliance from perimeter security to an asset-centric business-supported model that protects the right assets from the right threats with the right measures. Security zones will allow assets of greater organizational criticality and value to be held to higher security standards and protected by additional layers of defense. If possible, they should be compartmentalized, or zoned, into their own networks and segments. By doing so, the perimeter will be considered an asset like everything else.

Use Physical Security Zones Along With Network Zones

Physical and environmental controls are also an important component to protecting enterprise information and systems. Effective physical and environmental controls are necessary to prevent a complete network failure. Consider the following steps when planning security zones.

Identify Critical Enterprise Information and Network Assets

Create a list of critical enterprise information and network assets, then document the ones essential to the reliable and necessary operation of the enterprise. Follow a documented, risk-based process for your identification methodology. Establish risk-based criteria that correspond with the unique environment, requirements, services, and products of an organization.

Create an Asset Inventory

Create an inventory and corresponding classification of critical enterprise information and network assets if this has not already been done to facilitate business continuity processes and comply with numerous regulatory requirements for identifying and protecting certain types of information.

Identify Security Zones by Grouping Assets

Segment the enterprise data processing centers into areas that are logically separated from one another based upon their associated critical assets and revenue areas to contain an attack and keep the impact as minimal as possible to the overall business. Zones can support individual applications or application tiers, groups of servers, database servers, Web servers, e-commerce areas, and storage resources.

Create a Road Map to Implement Security Zones

After identifying the security zones, create a plan, or road map, to ensure the efficient and effective implementation of the security zones into the enterprise, based upon criticality, over a reasonable period of time. Integrate the security zones into the existing enterprise network. Define the access and security requirements for every service so that the network can be divided into security zones with clearly identified security and access levels.

Work with each security zone separately. It is likely each zone will have a different security model necessary to address the identified risks. Security controls should be implemented so that security breaches and incidents can be confined to a particular zone or part of the network as much as possible.

Implement Zone-Specific Protections

Each identified security zone needs to have controls and protections implemented based upon the risks specific to that zone. It is likely all zones will have some similar protections, such as virus control systems. However, each zone will likely need unique controls that no other zones may have, such as a zone with a remote access server (RAS), or a zone that houses a credit card processing system. There will probably be zones that need to have internal firewalls to protect them, and other zones that will not need such firewalls.

Integrate Security Zones Within a Layered Security Strategy

Do not stop at zoning alone, though. Zoning is just one of the key components of an organizational security strategy. To successfully defend against the multiple and varied types of threats and address the numerous and diverse vulnerabilities, organizations need to create and implement a layered security strategy.

Perimeters, infrastructure devices, OSs, applications, and data must be assessed and appropriately fortified to mitigate the risks that threaten your organization. Use multiple complementary approaches for security enforcement and defense at various points in the network, which will remove single points of security failure.

Implement Layered Security Throughout the Enterprise

Using just one tool or performing just one activity will not accomplish an effective information security program. An effective information security program consists of many layers.

Using many different layers of many different types of security, based upon business goals, services, and risk evaluation, will most effectively protect the enterprise from the attacks and threats that exist from all directions and in all ways, both malicious and accidental, to information resources. This layered defense is often compared to the layers of an onion, creating many different types of security layers that must be penetrated before the target at the core of the onion (the critical information infrastructure) can be reached.

Security layering establishes a more reliable security posture; if a failure or breach occurs in one layer, it will not compromise the other concentric layers.

Security Program Management Layer

The information security program is an information security layer that permeates multiple levels of the enterprise and benefits the organization in many ways. Every level enhances the entire information security program by making use of various types of expertise, authority, and resources. Generally, as a result of this layered security program management:

- Executives will better understand the organization as a whole and have better knowledge to most appropriately and effectively use their authority to protect the enterprise information assets.
- Managers within each of the business and operational units will be more familiar and cognizant of the specific security requirements, including technical and procedural requirements, and the associated challenges of the systems and information users.

Centralized Security Management

Establishing a centralized security management area with ultimate enterprise-wide security oversight will result in distinct benefits to organizations.

- It will increase the efficiency of security throughout the organization, allowing security to be implemented with an economy of scale that is more resource efficient than having security assigned independently to different groups.
- It will allow the organization to enforce security requirements centrally as well as to centralize monitoring, evaluations, and updates to the enterprise security program.

Distributed Information Security Management

The enterprise information security management program will address the entire range of information security issues for the enterprise. Distributed information security management programs will help to ensure appropriate and cost-effective security is addressed within each of the organizational business and operations areas.

Application Security Layer

Information security controls built-in to business process applications are an important enterprise information security layer. Examples of how to build information security into applications include programming checks and controls for segregation of duties and for data:

- Completeness
- Accuracy
- Validity
- Authorization
- Encryption

Node-Level Security

Another important information security layer is node-level security. Leading practices to accomplish node-level security implementation use a combination of identification, authentication, and logical access controls. Identity management focuses on integrating these activities into the business environment.

Identification and Authentication

Identification and authentication are necessary to help prevent unauthorized user and process nodes from being able to access networks, systems, applications, and information. Access control mechanisms are used to differentiate between these users and processes to allow only those authorized to perform the activity they are requesting.

Identification

Identification is the information the end-node user or process provides to uniquely distinguish their activities and capabilities. The most common form of identification is the user ID. However, there is also a need to identify devices, especially inside the perimeter where there can be a large number of headless servers. Certificates are also frequently used to provide identification for users and devices.

Authentication

Authentication is used in conjunction with identification to validate the entity using the identifier is truly the associated user or process it claims to be. There are three ways in which identification can be authenticated:

- Using something the user knows, such as a password or PIN
- Using something the user possesses, such as a token or smart card
- Using something with biometric characteristics, such as voice patterns or fingerprints

Network devices also need to have identity validated. Certificates are the primary method used to authenticate the identity of network devices.

Logical Access Control

Logical access controls are system-controlled ways for a node (such as an end user or process) to be explicitly enabled or restricted to do something with a computer resource, such as view, update, or delete data.

Logical access controls not only allow the user or process to have access to a specific network or system resource but also provide the specific type of access to the resource.

Organizations should implement logical access controls based upon the information security policies that cover the corresponding systems, networks, and applications. Logical access controls should be based upon business processes and goals, with information security, operational requirements, and ease of use incorporated into the control decisions.

Network Security Layer

Security within the network layer must be incorporated into, and addressed, within many different components and using many different techniques.

Transmission Control Protocol/Internet Protocol (TCP/IP) is an important part of the network security layer, but security within the network information security layer goes beyond TCP/IP. The open nature of TCP/IP complicates security implementation and makes it more challenging.

Networks can span many organizational and business partner boundaries. Organizations must understand and take into account the risks associated within the data flow as well as ensure that legal and contractual issues exist in harmony with the business services and practices. Additional security must be applied within the network to protect sensitive information that passes through public and business partner networks and zones that are not trusted.

Network Security Controls

Networks must be effectively managed and controlled using multiple tools and techniques to protect the network and associated components from a multitude of threats as well as to provide security for the systems and applications that depend upon the network for business processing. There is a wide range of security controls within the network layer that business leaders must consider and appropriately utilize, such as:

- Separation of duties—Separate operational network responsibilities from the other computer authorization responsibilities. No single person should be able to access, modify, or use network assets without the separate authorization or detection from another distinct position or area. Network change actions must be separated from the authorization of the actions. When designing network controls, this separation of duties must be considered.
- Remote network access—Clearly document and communicate the responsibilities and procedures for managing remote systems and how they connect to the network.
- Data transmission protection—Establish controls to protect and safeguard the confidentiality, availability, and integrity of data that is sent over public, shared, and wireless systems. The endpoint systems and applications must be protected from the threats these open networks present.

Encryption is one example of an effective tool that can be use to protect data transmissions.

- Logging and monitoring—Determine the appropriate logging and monitoring necessary to record relevant security and network activities to enable successful security incident investigations in addition to providing other necessary evidence for business processing. Logging and monitoring is also mandated and restricted by laws, regulations, and contractual requirements and aids troubleshooting. Audit trails created from logging and monitoring are becoming more and more important, not only for regulatory compliance but also for being able to correlate multiple network activities throughout all security layers, and for computer forensics activities following network security incidents.
- Management coordination—Network security activities must be carefully coordinated with network operational management activities to ensure security is applied consistently throughout the network and information-processing infrastructure. Without effective communication and coordination, there could easily be conflicting activities taking place or the failure to accomplish necessary tasks because one area thinks another area is performing specific security activities. For example, without coordination, a system may never get backed up because two groups assume that the other is performing the backup.

Securing Network Services

Identify, and include within networks services agreements as appropriate, network security features, service levels, and management requirements for all network services. This task should be done with not only outsourced services but also the services provided in-house.

Physical Security

The physical information security layer is a very important component of information security, though it is often overlooked by information security practitioners. This aspect of information security is commonly left solely to the facilities security personnel.

> Physical security controls are necessary for preventing unauthorized physical access, damage, and interference to information assets and resources.

Organizations must consider the physical security risks, threats, and vulnerabilities and address them within the information security program. The information security area must work in partnership with physical security departments, end users, business partners, and other identified areas to ensure adequate physical security is implemented to protect mission-critical and sensitive information processing facilities.

Information processing facilities and systems should be located within secure areas and protected by defined security perimeters:

- Appropriate security barriers and entry controls should be applied.
- Data and processing centers need to be physically protected from unauthorized access, damage, and interference.
- Mobile information systems must be appropriately physically secured using a variety of methods.

> All information security physical protection methods need to correspond with the identified risks, threats, and vulnerabilities as well as the corresponding potential business impact.

Use the following physical security controls checklist to help determine the types of controls to be considered and implemented as appropriate to the organization's industry, size, geographic locations, and regulatory and contractual requirements:

- Site selection and physical security
- Public access, delivery, and loading areas
- Physical entry and access controls
- Security for offices, rooms, and facilities
- Environmental security
- Computer processing equipment security

> Organizations cannot depend upon facilities security alone to adequately protect computer-processing equipment; too many vital computer devices are mobile. Appropriate controls must be implemented for mobile computing devices and storage media to help prevent loss, damage, theft, or the compromise of assets and interruption to the organization's activities.

Supporting Utilities

Organizations depend upon power to keep information processing and computing facilities going. Protect processing equipment from power failures and other disruptions caused by failures of supporting utilities

Equipment Maintenance

Information processing equipment must be properly maintained to ensure the continued confidentiality, availability, and integrity of the information and systems processed on it.

Securely Decommission Equipment

Check all types of processing equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal, re-use, sale, or donation outside the organization.

Taking Computing Equipment Off the Premises

Do not allow equipment, information, or software to be taken off-site without prior authorization. Maintain documentation of the employees, contractors, and third-party users with authority to permit off-site removal of assets.

Human Resources

The most vulnerable of the information security layers are the human resources that organizations depend upon to follow information security policies and procedures. Individuals must know and understand how to appropriately handle and safeguard the information and associated computing resources that they use while performing their job responsibilities.

Organizations must invest time and resources to help ensure personnel do the right things by:

- Hiring qualified and appropriate individuals
- Providing effective training and awareness
- Motivating individuals through clear career paths and making security part of job responsibilities that are used for performance appraisals
- Establishing a defined compliance review process
- Mitigating risk of overdependence on key resources by using more than one person for a role in addition to cross training and ensuring proper separation of duties

Monitoring and Evaluation

The monitoring and evaluation layer of information security is one that is often not adequately addressed. Organizations must establish methods for monitoring and evaluation to maintain operational assurance and information security.

There are various methods for monitoring and evaluation, including:

- Performing scheduled audits
- Implementing ongoing monitoring of key applications, systems, and network components
- Performing evaluation activities

Disaster Preparedness

Events of the past decade demonstrate the importance and criticality of security components such as business continuity plans and disaster recovery activities. Organizations must have business continuity and disaster recovery plans in place not only to support the business goals for continued operations as much as possible under adverse circumstances but also to meet regulatory requirements.

Incident Response

An information security incident can result from a number of events that can range from a computer virus, other malicious code, a system intruder, and denial of network services to a lost laptop computer or lost backup tapes.

> The definition of an information security incident is what an organization determines it means to its own particular environment.

Incident response is sometimes included as a part of contingency planning because of the need to quickly and efficiently respond to business disruptions and get back to normal processing as soon as possible. However, there are specialized activities within incident response that are compelling reasons to make this a separate information security layer within organizations.

Implement Business Appropriate Tools Within the Zones

Organizations must manage information security in multiple ways throughout the enterprise and as appropriate within each of the identified security zones. Network security management must effectively manage access to information assets and establish rules that network users must follow, limit access to network information resources to only those that have a business need for the access, and create notifications whenever incidents and inappropriate actions occur.

Powerful security safeguard tools must be implemented within established security zones to make the zones effective. When determining the security tools to implement, keep in mind that most reported information security incidents stem from three business weaknesses:

- Poorly implemented security measures revolving around improper access controls
- Lack of encryption
- Trusted insiders purposefully or accidentally accessing, using, or damaging information resources

Access Control

Problems will quickly emerge if proper access controls are not implemented throughout the enterprise and appropriate to each of the zones within which the controls are applied.

Authorized users within the zones will download and install mobile code from the Internet onto the organization's computers, carry in problems on their mobile computing devices, or introduce problems from their remote locations.

Workstations and endpoints within the network perimeter must now be viewed as hostile territory and potential threats. Desktop access controls must be managed centrally, including such controls as desktop firewalls, malicious software prevention tools, security policies for the zones within which they reside, and user authentication and authorization. Information and network asset protection success relies on the measures implemented close to the IT resource, within multi-tiered applications, and on active security management.

There Are No Longer Homogenous Environments

Implementing effective access controls is no longer the comparatively easy task it used to be when all information resided on one mainframe with only dumb-terminals sitting on the end users' desktops. The network environment in most, if not all, enterprise networks is now a mix of systems owners scattered throughout the enterprise in various departments and locations, assortments of OSs, and applications servers of every type imaginable. The complexity of networks is growing exponentially while the implementation and availability of security solutions seems to grow fractionally.

The types of resources to manage and secure now are many. A couple of challenging ones include:

- Headless servers—Implementing headless servers throughout the enterprise should be done consistently, following documented procedures and guidelines. Centralized oversight and administration of the servers will ensure the servers within each of the security zones are protecting sensitive data consistently from one zone to the next.
- Web-based servers—The number of Web-based servers organizations deploy also continues to grow exponentially as organizations depend more upon Internet presence and online sales to boost revenues.

Incorporating Access Controls into the Development Life Cycle

To successfully incorporate access controls into the systems development life cycle (SDLC), the organization's required security parameters must be clearly documented and communicated to all systems and applications developers in terms applicable to the development processes. Security requirements should be incorporated into the formal SDLC process in the same way that the business requirements and end-user requirements are defined.

Variety of Application Types

Today's enterprises have many more types of applications to manage than ever before, and usually the applications are completely different from one business unit to another. Managing access controls consistently throughout the enterprise in this type of situation is quite challenging and is often the impetus to many stressful workdays for the typical information security leader.

The Need for Encryption

The increasingly porous network perimeter combined with the growing number of ways in which data can be shared with all locations throughout the world has generated a growing need to protect information by using encryption. This protection should include encrypting not only the actual data but also, and perhaps more important, the authentication credentials (user IDs and passwords) for the applications that access the data.

Legal Requirements for Encryption

The use of encryption is often listed as an option organizations must consider within the wide number of data protection laws and regulations throughout the world. Encryption is a consideration within the many United States state-level breach notification laws. For example, notification activities do not need to occur if the data breached was encrypted.

Need for Encryption Transparency

Data is currently more commonly encrypted for remote access transmission than for storage. One common reason is that data-in-motion encryption is usually seamless to the application and requires minimal effort to deploy and little action from the end user. Another reason is that companies have historically been more concerned about hackers getting the information as it passes through the Internet than with someone getting to the data in storage. However, as many recent data breaches demonstrate, protecting data at rest is just as, if not more, important.

Encryption must be as transparent to the end user as possible in order for it to be successfully, consistently, and effectively used throughout the enterprise.

Encrypting Data in Motion

Securing data that goes outside the network perimeter presents challenges. VPNs have been the most common way of protecting information that must pass through a public network (such as the Internet) through the use of multiple security controls including encryption.

Insider attacks are increasing at alarming rates. Network intruders realize that they can gain access to internal corporate information resources because internal networks are more vulnerable and typically do not use encryption to protect data in transit that does not go outside of the network. As the number and severity of internal network attacks increases, organizations must recognize that using encryption for data in motion within the network is an essential and practical tactic to prevent theft of intellectual property and personally identifiable information.

Encrypting Data at Rest

Encrypting data at rest is another essential and practical tactic for protecting information within the network perimeter. A successful information security strategy will identify not only the types of encryption methods to use for data at rest but also the types of data that need to be encrypted.

> ☞ When encrypting databases, remember database lookups are designed to be very efficient. Unlike typical file systems, databases are expected to look through millions of rows, searching for specific items in seconds. These speed features present challenges for encrypting databases. It is not feasible for a database to decrypt each data element it must search. It is critical to consider how applications will use the database while planning to deploy encryption.

Encrypt at the Network Layer

Implement encryption at the network layer so that it is transparent to both users and applications and requires no modification to existing software applications, such as CRM, ERP, and inventory tracking systems.

> ✎ The success of VPNs to encrypt data in motion for remote access demonstrates that implementing encryption within the network layer allows for phased deployments within targeted security zones to add immediate benefit to enterprises.

Implementing network-layer encryption solutions within identified security zones with careful planning and the right tools can even eliminate the challenging deployment and management of VLANs.

Centrally Managing Encryption Solutions Is Crucial

A well-designed encryption system will operate separately; generating, storing, and protecting keys with very little user intervention. Mistakes or weakness in key management can quickly lead to system compromise. Key management is a critical area to focus upon when purchasing or building an encryption solution because mistakes and weaknesses within a key management system can quickly allow for system compromise.

Monitoring

An important tool for network security management is monitoring:

- Monitoring compliance
- Monitoring access attempts
- Monitoring for malicious code
- Monitoring for security incidents and breaches
- Monitoring for any activity that can have negative impact on the business

Personnel Monitoring

Most states in the United States have laws that address employee privacy rights in one way or another. In many European jurisdictions, the employee's right to privacy is protected in the constitution, limiting the employer's ability to monitor in the workplace. Additionally, employers must often show regard for the rights of employees' representatives to be consulted regarding the implementation of any monitoring.

If an organization has work councils or trade or labor unions, those councils and unions need to be included in discussions regarding employee privacy and planned policies, procedures, and actions. Whether the employer is required to seek the agreement of employee representatives or just needs to consult with them will depend upon the local requirements of each jurisdiction and the terms of the applicable agreements.

Other Types of Monitoring

Monitoring goes beyond just checking one or two types of network activities by using some sort of automated method. There is a very wide range of monitoring activities that organizations need to consider for an effective information security program. At minimum, types of monitoring to implement should include:

- Intrusion detection to identify when inappropriate access is occurring
- Intrusion prevention to keep unauthorized individuals from getting to information resources
- Systems and applications monitoring to ensure conformity with information security policies and standards
- Systems monitoring to detect unauthorized activities
- Systems monitoring to determine the effectiveness of security measures adopted
- Event logging
- Clock synchronization
- Log file entries standards
- Internet usage
- Business partner connections and related network activities
- The effectiveness of security controls
- User access to mission-critical and sensitive information

Awareness and Training

For network security tools to be effective, administrators and end users must be properly trained in how to use them. Awareness and training are important activities and key components of an effective information security program. Many regulations require awareness and training as part of compliance.

Legal Considerations

Always include legal counsel in decisions regarding information security and privacy, especially education program activities. It is important to know the legal ramifications and requirements for training and awareness activities.

The legalities of information security and privacy risks and managing legal compliance with applicable laws and regulations are a growing concern for managers, lawyers, and Human Resources personnel. An overabundance of international, federal, and state laws govern how personnel and individuals with access to personal and confidential information must be trained.

Managing Information Security Throughout the Enterprise

It is no longer sufficient or prudent to depend upon securing only the perimeter of the enterprise network with security management devices in order to protect all the enterprise information assets. The number of new entry points through most enterprise network perimeters can increase on a weekly, or even daily, basis.

The growing number of reported incidents not only demonstrates the impact of multiple breach-notification laws but indicates that organizations may still be focusing on just securing the network perimeter and not sufficiently securing all information assets wherever they are located.

Managing Inside Is More Complex Than Managing the Perimeter

Implementing and managing information security within the network perimeter is much more complex than just managing the security of the perimeter alone. When adding internal information security management to the picture, most organizations will get a list of components that look something like the following:

- Firewalls—Not only on the perimeter but also deployed within identified security zones
- Proxy servers—Not only on the perimeter but also deployed within identified security zones
- Unified intrusion detection, and increasingly intrusion prevention, systems between security zones
- Malicious code prevention between security zones
- Consolidated management consoles
- Unified alerting and reporting
- Unified monitoring
- Encryption systems
- Access control devices and systems

- Audit capabilities
- Policies and procedures
- Application controls
- Network controls
- Systems controls

The Porous Perimeter Must Be Considered

As more accountability is created for business leaders to ensure information security, and as they then become more aware of the related issues, they should understand that information security must be integrated throughout the entire enterprise. To be most effective in integrating information security responsibilities throughout the organization, two very important things must exist:

- Information security must be clearly supported and promoted by the highest executive leaders within the company.
- The information security function needs to be as high in the corporate structure as possible in order to set and enforce information security directives and policies. As history has proven, unless the information security department is powerful enough to establish and enforce information security administrative, operational, and technological initiatives, the rest of the organization will not follow information security requirements, but instead choose the ease of use and functionality they see information security as inhibiting.

Address Contractual and Regulatory Requirements

It is vital to ensure that information assurance activities support, and information security leaders understand, the existing regulatory and legal requirements for safeguarding information throughout the enterprise. The penalties, fines, and jail time for noncompliance can have devastating impact on not only the business but also to the business leaders personally.

Determine the Value of Information

Something lacking in most organizations is an inventory of information assets that have been classified according to their sensitivity and criticality. With today's regulatory requirements to notify individuals of security breaches, it is a necessity to know the information you have, and where it is located, if you expect to know when the information has been compromised.

After the information inventory is compiled, you can ensure appropriate security is applied based upon the value of the information. It is not feasible, or prudent, to try to secure all information at the same level. By knowing the value of the information, you can then more successfully manage the security within your security zones and layers by applying the most robust security within the zones where your high-value information assets are located, and using appropriate mechanisms within the security layers, and not investing as many resources in those zones that have information assets with lesser values.

Information Valuation

Organizations need to determine the types of information that could have the most financial impact and build security around those high-value items appropriately. What will make this challenging are the many unstructured forms in which sensitive information may be saved, such as in email, Word, Excel, PowerPoint, and other end-user controlled formats. This emphasizes the need to implement a clear, strongly supported set of information security policies that contain a very good information classification policy.

Considerations for Outsourced Access to Information Assets

When an organization entrusts third parties with its confidential data, the organization basically place all direct control of security measures for the data completely into the hands of someone else. That trust cannot be blind. When organizations outsource critical data processing and management activities, they must implement measures to stay in charge of their own business data security and minimize business risks.

Tracking Progress and Incidents

Not only is it wise and necessary to track information security progress and incidents in order to have an effective information security program, it is also a requirement of many laws and regulations.

📖 Chapter 7 discussed these requirements in detail.

Items to Monitor and Log

There is a wide range of activities throughout the enterprise that must be monitored and there are multiple types of activities that need to be logged. These are not all electronic based. You should have identified many of them while establishing your security zones and implementing your layers of security.

Auditing and Tracking Mechanisms

Establish auditing and tracking mechanisms for systems activities, key security-related events, personally identifiable information, and other sensitive and mission-critical information.

The Recipe for Achieving Information Security Inside the Perimeter

Business leaders must consider all the issues involved with managing an enterprise-wide information security program as discussed throughout this guide, and create a type of information security recipe to successfully create a secure enterprise-wide information processing environment. Each organization's recipe for success will be unique to their business goals and environment, but the following generic recipe, based upon proven security concepts, can be used as a foundation.

Ingredients

- A top-level executive leader, such as the CEO, with strong, obvious support for information security efforts
- A position or team with formally documented and well-communicated overall enterprise information security responsibility
- Business unit leaders from all areas throughout the organization to cooperate and work with the information security position to successfully integrate effective security throughout the enterprise
- Knowledge of the business environment, goals, products, services, and legal and contractual requirements
- Well-written information security policies and procedures
- Technology tools to support and enhance the information security strategy goals
- Evaluation techniques to ensure appropriate changes are made to ensure the most successful information security strategy

Instructions

- Simplify information security complexity.
  - Appoint a position to be responsible for enterprise-wide network security
  - Support the position from the highest leadership positions
- Identify legal and regulatory requirements for data protection and safeguards.
- Identify risks—using the appropriate risk analysis processes for your environment—to the organization and information systems and assets throughout the entire enterprise.
- Develop a multi-dimensional security plan to protect information assets and associated resources within all areas of an enterprise and in compliance with all regulatory, policy, and contractual requirements.
- Establish enterprise network security zones.
  - Thoughtfully plan the zones with input from the business areas and by considering risks
  - Complement effectiveness with physical zones
  - Centrally manage security zone activities through the help of decentralized responsibilities

- Implement security layers.
  - Security program management
  - Application-layer security
  - Node-level security
  - Network-level security
  - Identification and authentication
  - Network services
  - Physical security
  - Human Resources
  - Monitoring and evaluation
  - Disaster preparedness
  - Incident response
- Implement security tools.
  - Access controls
  - Encryption
  - Monitoring
  - Education
- Create organization-appropriate and well-written policies, procedures, and standards.
- Educate all individuals using the enterprise information assets and resources about the policies, procedures, and other information necessary to successfully safeguard information.
- Establish audit and monitoring functions to constantly stay aware of the information security environment.

Implementer Tips

- The porous perimeter, new and emerging technologies, and legal and regulatory requirements necessitate that security be addressed and risks be identified throughout the entire network, not just at the perimeter.
- Many information security threats and risks exist in today's business environment, both outside and inside the organization.
- Laws, regulations, and customers demand information to be adequately safeguarded no matter where it resides.
- Information security safeguards are necessary to protect against not only malicious intent by insiders but also against mistakes.
- Trusted insiders with authorized access to sensitive information will sometimes still choose to take part in malicious activities. Controls need to be in place to help prevent or catch such activities.
- New and emerging diverse technologies create threats to the enterprise network. Information security leaders must keep up to date with them.
- Using inappropriate technologies and tools for security will leave data vulnerable.
- As data increases in value, the number of threats to the data also increases.
- Incorporate access controls into the development life cycle.
- Use encryption to effectively protect data at rest and data in motion.
- Create and maintain an information inventory.
- Evaluate the information security program regularly and report to business leaders