Data Lives

Information flows through business processes in an orderly fashion; security must flow right along with it.

by ERNIE HAYDEN

TODAY'S CHIEF INFORMATION security officer, schooled by the Common Body of Knowledge for Information Security, CISSP and CISM handbooks, and reliant on frameworks such as ISO 27001, tackles security as a collection of individual issues rather than holistically.

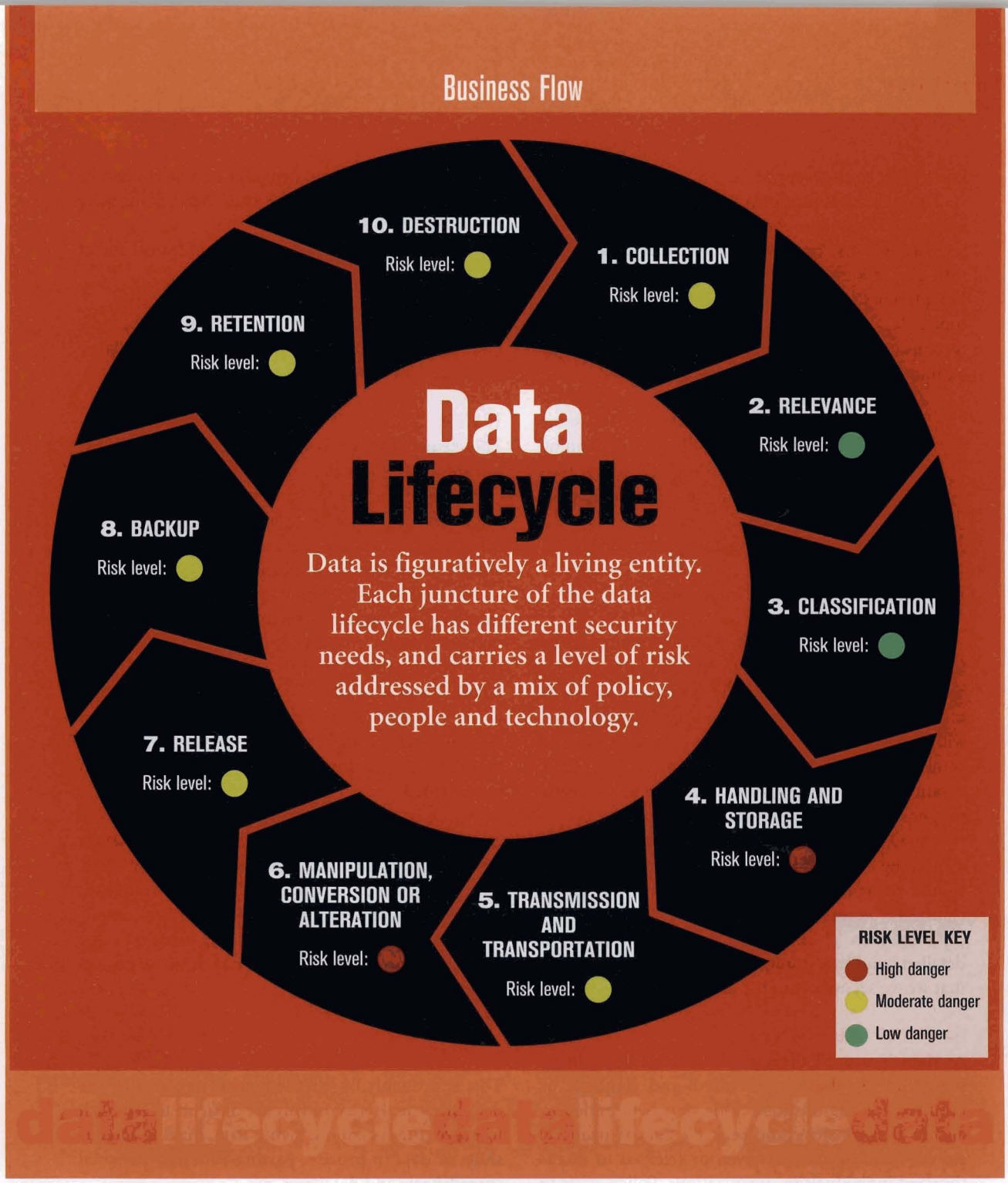
These time-tested resources don't necessarily help the CISO gain a grasp of the integrated flow of data and how to secure it. Enterprise executives don't think in silos; they look at business processes and flows. And this is how CISOs should examine data—as a lifecycle from birth to death, and as it resides within business processes. It is a business cycle to be reviewed, analyzed and contended with.

Similar to an economic value-add analysis methodology, the data lifecycle security model *(see right)* shows how data is collected, classified, stored, used, retained and ultimately destroyed. It shows process, transition and a business flow.

COLLECTION

Beginning the data lifecycle and data stream, we look at the birth of data: data collection. Actions taken early in the data lifecycle can ultimately pay off. For example, administrative rules can be established that prohibit the collection of unnecessary data, or data considered too significant a risk to collect.

Photograph by VEER



Consider prohibiting the collection of Social Security numbers, protected health information (as explained in HIPAA), complete credit card numbers and other sensitive data unless absolutely necessary for the performance of business. And, if you absolutely need this information, then be sure to encrypt, or at least look at truncation practices.

RELEVANCE

Another consideration in the data flow is whether the data is relevant to the business process. Administrative controls should discourage irrelevant data collection because it would be "nice to have" or useful for future projects.

Ultimately you need to think about the consequences to you as CISO and the business if this data were ever lost or breached. Will you be able to explain why this data was collected in the first place?

CLASSIFICATION

A key foundation to this process is data classification. In other words, if you have data in play, how do you

know what controls apply?

The data classification process and development of this area is well researched and discussed in many security forums. However, the consideration to put into play is simplicity and ease of implementation. Key players should include the data owner, data custodian, legal department and the CISO. It's important to consider a simpler process where there are only a limited number of classifications, including:

- Business sensitive or confidential
- Personal identifiable information (PII)—some state data breach laws may be helpful in defining this category and usually include name plus Social Security number, driver's license number or credit card/account number
- Protected health information (PHI) for HIPAA security
- Unrestricted or public information.

Data owners should classify documents based upon corporate guidance. The data custodian ensures only appropriate individuals have access to view and manipulate data based on role and classification. Legal will monitor this information for data retention and compliance activities such as e-discovery. The CISO, meanwhile, will use this classification to supervise proper storage, handling and release.

The CISO should also work with legal to prepare a marking standard, which states how a document should be marked and how classifications can be changed if necessary.

With each classification you should establish detailed handling, storage and disposal requirements that weave security into the data lifecycle.

HANDLING AND STORAGE

As data is moved through the lifecycle, it will be stored in databases, processed and handled as required for the business. This step is intended to ensure that sensitive and security data is properly stored, handled and not given or released to unauthorized individuals or organizations. Policy exists to ensure individuals do not digitally or physically handle or release sensitive data unless authorized. Some rules to consider here are:

- Encryption of appropriate data in transit and at rest
- Hashing data to be assured of data integrity
- Access controls to ensure only authorized individuals get to touch, view and manipulate data
- Activation and monitoring of audit logs.

TRANSMISSION AND TRANSPORTATION

This element of the lifecycle includes electronic transmission of data as well as physical.

For instance, considerations for data protection might include SSL or Transport Layer Security (TLS) tunneling, encryption of email and attachments, and email content filtering or blocking.

Physical transportation failures can be minimized by encrypting all media in transit (i.e., back-up tape encryption), tracking the media as it moves from point to point, and receipt management so the enterprise is assured the data is received when and where expected. Most state data breach notification laws also relieve the enterprise of the notification mandate if the lost or misplaced information is encrypted.

A key consideration here is to also ensure that contractual controls with the physical transportation company are in play, including indemnification of the enterprise should the courier lose the data in transit. Although indemnification is not necessarily a compliance issue, it certainly reflects an organization's due care and attitude toward its fiduciary duties to protect the company.

MANIPULATION, CONVERSION OR ALTERATION

This is probably by far the biggest risk area of the data lifecycle. Here controls are difficult to establish to prevent users from copying data, making screenshots of data in process, pasting data into personal spreadsheets and databases, etc.

CLOSING IN ON 50

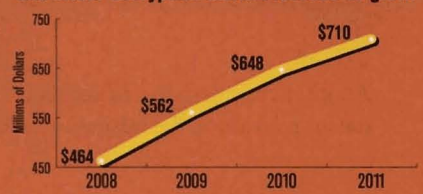
The National Conference of State Legislatures reports that 43 states plus the District of Columbia and Puerto Rico have approved legislation that requires notification in the event of a breach involving personally identifiable information.

LOOPHOLE CLOSED

Indiana's data breach notification law was updated July 1; it now frees companies from disclosure in the event of a breach if laptops are encrypted. Prior to July 1, password protection was enough to alleviate companies from having to notify.

CLIMBING

IDC forecasts endpoint full disk, and file and folder encryption market revenue to grow.



For instance "data personalization," aka "personal data collection projects," substantially increases the risk profile for the organization. As an example, an employee may be accumulating information from various company databases and screenshots for personal use, such as his or her own phone list or roster, or for future projects. Here the data lifecycle is seriously disrupted and sensitive data can wind up on users' workstations, USB drives, and even at their homes, regardless if the intent is positive and for the good of the corporation.

Controls to consider in this space are technical controls to prevent data flowing external to the enterprise unless it is encrypted, such as data leak prevention technology; email content review and management; and a draconian thought of prohibition of personally owned portable media.

Administrative controls could also include policies and procedures on how data should and should not be used or collected by individual employees. Rules forbidding use of company computers for employee off-hours activities may be necessary. Of course, focus on the first step—data collection—would help minimize this risk, too.

RELEASE

In 2003, the reputation of Jet Blue was seriously damaged because data held by the airline was improperly released to a TSA contractor. This event demonstrates that how and when sensitive data is released in the lifecycle must be closely controlled. Aspects of this lifecycle element should include:

- Definition as to who has authority to release data outside the organization
- Recognition that not all data can be released upon a simple request
- Data is not released unless appropriate for the business and only if legal and with appropriate controls.

Other subtle elements of data release also need to be examined. For instance, a company may use a vendor to analyze data as part of a contract. What controls are in play relative to data sharing, data control and data breach by the vendor? To reduce the enterprise's risk profile, strong contractual controls need to be established to indemnify it if the vendor loses the data or uses it for inappropriate purposes (e.g., using your data for vendor marketing campaigns).

BACKUP

This area tends to be a fairly mature domain for security. However, there continue to be breaches where unencrypted backup tapes are lost in transit. Look at the data lifecycle to ensure this process contributes to the security and availability of the data.

RETENTION

Data being held by the company is subject to discovery for legal process. Litigation holds are becoming more and more critical because of more focus on e-discovery due to the new Federal Rules of Civil Procedure issued in December 2006.

The data lifecycle needs to ensure that data is effectively and appropriately retained so that data can be readily located and held for these discovery requirements. However, you also want to ensure that data is destroyed at the appropriate time to ensure that surprises are minimized during the discovery process when data thought to be "dead" or gone surfaces.

DESTRUCTION

The end of the process—the "death" of data—is the data destruction process.

This is actually another area that can be fraught with problems for the CISO if not done completely and with the appropriate controls. If data is to be eliminated, then it must be fully destroyed and not left in any post-destruction residual. You don't want to hear about your surplus equipment being full of sensitive data now in the open market. Some key practices to consider:

- Destroy hard drives by physical destruction or shredding—there's too much risk with the incomplete "wipe." Costs run about 25 cents a pound and can be easily witnessed. Of course, you can also use disk-wiping tools, but the diligence required to assure disks are properly wiped and processed may actually cost more than the total cost and assurance of physical destruction.
- Destroy paper by shredding. The process should be periodically witnessed, and the enterprise needs contractual assurance that it is indemnified should the vendor fail to complete the process.
- Do not destroy information on litigation hold—data on hold for legal review or subpoena—or too early in the retention schedule.
- Make sure employees know how to handle waste that is classified as confidential, business sensitive, etc., so such documents do not wind up in a public landfill and are instead shredded or destroyed.

Now, your data may be dead, but that doesn't mean the lifecycle has ended. This new approach to looking at how data lives and dies begs for additional analysis.

One thought experiment is to map the "risk value" of each lifecycle stage. No empirical evidence necessarily supports this mapping, but it can be used to show the relative risks encountered when you look at data lifecycle security in the enterprise.

The biggest risk is the data manipulation, conversion or alteration stage. Since it is so easy for an individual to copy and collect data for other uses, data gets distributed throughout the enterprise and cannot be easily controlled. And the risk can be significant if the data is moved offsite, to a home computer, placed on an unencrypted USB drive, etc.

The flow of data is a new way to guide security professionals' focus, time and energy. They can look at new ways to not only protect the data, but also use this as a way to communicate risks and issues to executive management.

Also, this data lifecycle security approach can be a new way to build a security program, procedures and strategy. And it may be a new way to justify expense in critical areas of the organization, including security, legal and operations. ›

Ernie Hayden is former information security officer for a health care organization and former CISO for the Port of Seattle. Send comments on this article to feedback@infosecuritymag.com.

IN THE KNOW

RESOURCES

(ISC)² and ISO define the basics CISOs are expected to know in the Common Body of Knowledge (CBK) and 27001 standard respectively.

(ISC)² CBK

- Access Control Systems and Methodology
- Telecommunications and Network Security
- Security Management Practices (Security Management, Risk Management)
- Applications and Systems Development Security
- Cryptography
- Security Architecture and Models
- Operations Security
- Business Continuity/Disaster Recovery Planning
- Law, Investigations and Ethics
- Physical Security

ISO 27001 security areas

- Security Policy
- Organization
- Asset Management
- Human Resources
- Physical and Environmental
- Communications and Operations Management
- Access Control
- System Development and Maintenance
- Security Incident Management
- Business Continuity Management
- Compliance and Audit