SECURING DATA: SIX KEYS TO AN EFFECTIVE CYBERSECURITY PROGRAM

By **LENA LICATA**
EISNERAMPER

Data is at the core of many companies' business operations. However, securing the tremendous amount of data collected on a day-to-day (even second-to-second) basis poses a monumental challenge to companies.

In order to develop an effective, comprehensive cybersecurity program, it is imperative to understand the six principles below to help identify, classify and secure data.

1. OWNERSHIP

After identifying the key data a company maintains, the next step is to determine who owns the data and who has the ultimate responsibility over the security of said data. While the data belongs to the business, its security is typically the purview of the chief information officer (CIO), chief technology officer (CTO) or some comparable professional. Establishing data ownership from the onset can help prevent confusion going forward.

The CIO, or someone else in the information technology (IT) department with the requisite skills and experience, should be charged with establishing governance along with the related cybersecurity roles and responsibilities. While this governance is created through IT — and is often its own sub-unit bridging the gap between the company and IT — both senior management and the CIO should have a hand in evaluating the success metrics going forward.

Part of the governance is developing clear procedures for granting data access. The IT personnel responsible for granting this access should obtain authorization from leadership to ensure "least privilege access" to the data. Least privilege means limiting data access to only what the user needs. Many data breaches occur when users have more access than necessary or when user roles change but access rights stay the same.

2. POLICIES AND PROCEDURES

Once data ownership is established, the CIO (or designated representative) should document clear policies and procedures that answer the following questions:

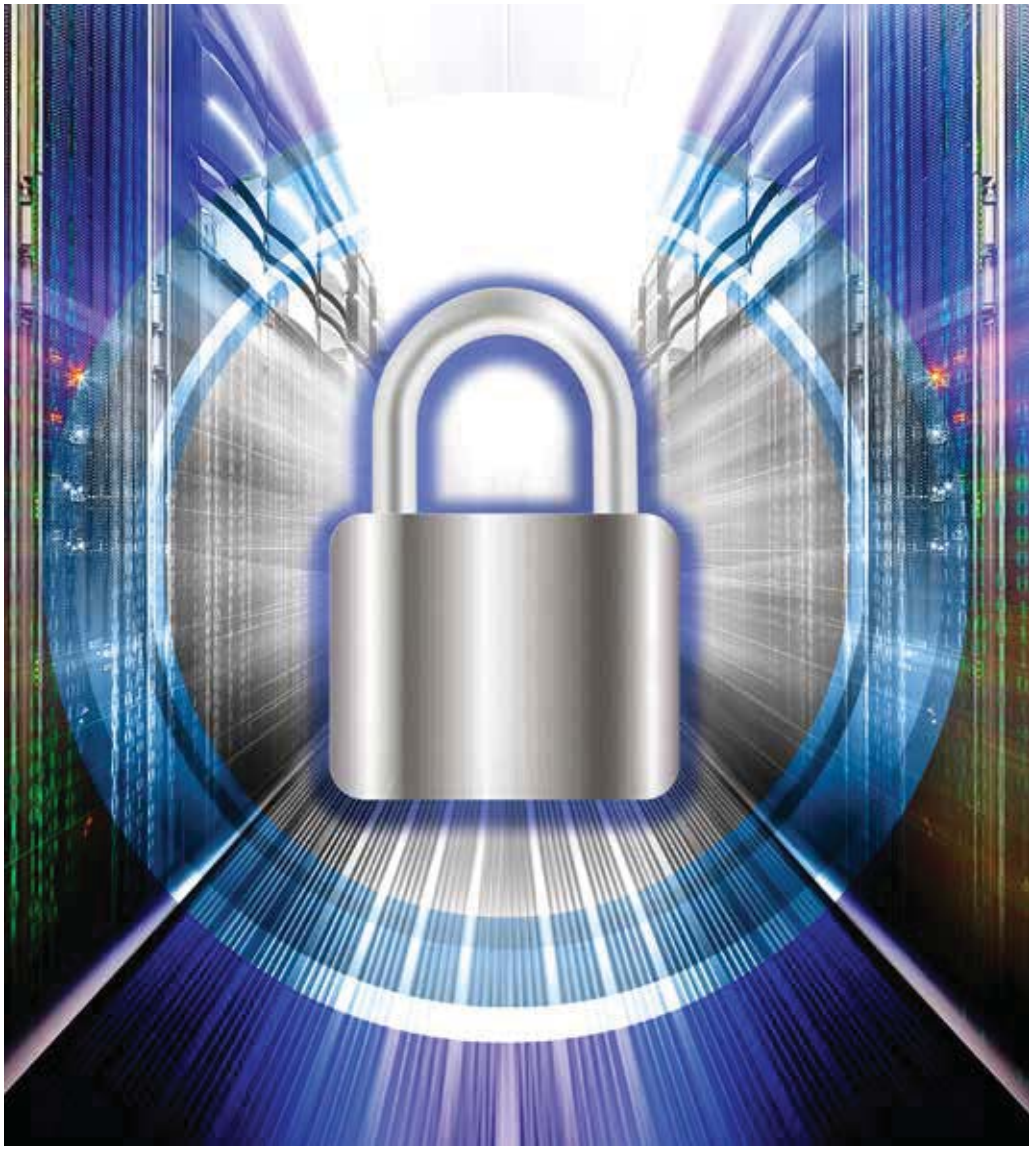
- ✔ What are key data elements for the company? Does it store personally identifiable information (PII), payment card information (PCI) or protected health information (PHI) data? Does it have intellectual property?
- ✔ How does the organization store data?
- ✔ What are the backup and recovery plans? How regularly should the company test the reliability of these plans?
- ✔ What are the obligations of employees to keep this data secure?
- ✔ What proactive mechanisms does the company use to secure this data?

Creating this documentation is an often-overlooked or underutilized step simply performed in a vacuum and then stored away. Why? It takes time to create, approve and implement the policies. It may simply be viewed as a regulatory exercise. However, it is time well spent to establish standards and consistency baselines. Think of the cost of *not* taking the time.

3. TRAINING

Another key to an effective cybersecurity policy is training and socialization. It should go without saying that companies should review policies often to make sure

they reflect current business practices. This periodic training creates a consistent top-down message to ensure policies become part of the corporate culture. Data owners should receive training on procedures, but all employees should receive annual training on how to secure data and acceptable use policies.



4. AUDIT PROCESS

Develop an effective audit process to monitor that policies and procedure are being followed. Periodic audits will help maintain that the least privilege access principles are in effect and only those with a business need have data access.

If you use identity management and group policy objects in the network environment, then policy should match granted rights to employees in the system to maintain proper access control. Audits are often performed by either the internal audit department or during the annual financial statement audit. However, if the company relies on a financial statement audit, it should be noted that the scope will only include those applications material to the financial statements and may not include all applications with business-critical data.

5. DATA RETENTION

Data retention is a critical component of a cybersecurity program. Too often, data retention policies apply to a company's physical data or paper files and not necessarily their electronic data. A company might be very good at destroying paper data based on a retention schedule but maintain 30 or more years of key data within their systems and on file shares. The inherent risk in this is tremendous. Network file shares are often jokingly referred to as the "Wild West" of data, but it is no laughing matter. Before the legal, IT and risk management teams take the all-important step of developing a comprehensive data retention policy, they must first classify data.

6. RISK ASSESSMENT

Businesses should perform an annual examination of the company's data vulnerabilities, threats, potential impact or losses, and effectiveness of security measures against the assessed risks. The assessment should encompass the key systems, processes and data flows within the organization. An effective risk assessment can be a key data security tool to identify weaknesses and facilitate planning to address those concerns. Management can then use the risk assessment to plan key IT and data initiatives for the coming year in its annual strategic plan and budgets.

CONCLUSION

Securing data against cybercrime is not a one-step process. It is a holistic program that affects everyone throughout the organization, whether they perform security, own data, use data or ultimately destroy data. Leadership must make it a priority to establish the program; properly define the program; provide training for those charged with implementing, overseeing and auditing the program; and mandate an annual review via a risk assessment in order to maintain adherence to the program and keep it current and effective. While no cybersecurity program is 100-percent effective, not having one (or just going through the motions) is a 100-percent invitation to disaster.

Lena Licata, CISA, CISSP, is a senior manager in EisnerAmper's Consulting Services Group. She can be reached at lena.licata@eisneramper.com or 732-243-7160.

READ MORE
CYBERSECURITY ARTICLES AND RESOURCES
njcpa.org/topics/cybersecurity