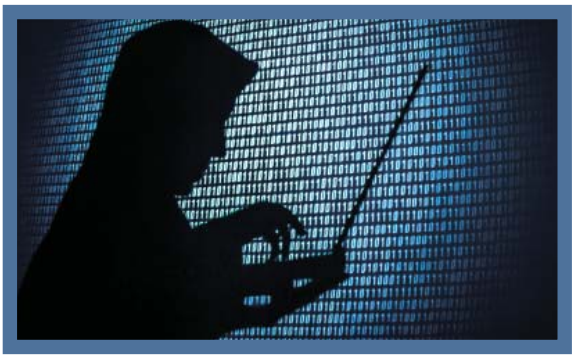
A breach from within

BY MICHAEL J. deBARROS



With constant media attention on hackers, the latest computer virus, and ransomware, it's easy for organizations to focus on external threats to their data. However, the biggest threat to a company's data often comes from within the organization.

Company insiders can steal or leak data with far greater ease than outsiders. Insiders typically have access to sensitive information on a regular basis, they know how information is stored and protected, and data leaks are often caused by the careless or misguided actions of insiders. Common sources of insider leaks include lost or stolen devices (laptops, iPads, cell phones, and USB drives), misaddressed emails, weak passwords, and transmission of data to systems with little or no security. Perhaps the most dangerous aspect of insider threats is that the harmful access and activities come from trusted sources and will often go unnoticed for lengthy periods of time.

Many organizations do not know how to secure their confidential information against these risks. The process begins by identifying the types of information stored and transmitted by the organization and categorizing that information by value and confidentiality. Companies should maintain accurate data-storage diagrams or "maps" and have a firm understanding of where sensitive data is stored. The most valuable data should be given the strongest defenses and the most frequent monitoring.

Once the information is identified, categorized and mapped, the organization should determine who has access to the information, how the information is accessed and what each person's access allows him or her to do with the information. If the insiders do not have a legitimate need for the information, their rights to the information should be eliminated.

Use and access restrictions should be bolstered by company policies controlling the access and movement of

information. The policies should be clearly communicated to employees, and the importance of securing information should be reinforced. In most corporate environments, few employees have any significant understanding of IT-security-related issues. As a result, viruses and malware are downloaded, accounts are hacked and corrupt devices are introduced to the corporate network. User awareness programs are key to educating insiders, and insider education is one of the most powerful tools in preventing data leaks.

Organizations should also develop an incident-response plan before a data leak occurs and update the plan at least once a year. The response plan should include the contact information of attorneys, IT forensic experts and vendors who can assist in collecting and preserving information, minimizing damages and notifying affected individuals and governmental agencies of the data leak. The plan should also identify who will have decision rights when an incident occurs and set forth action items to be completed immediately after the company learns of a potential data leak.

Companies handling sensitive information are advised to carry a wide variety of insurance covering costs associated with data leaks. Many traditional insurance policies do not cover electronic data loss or liabilities associated with data leaks, forcing companies to turn to specialized insurance products. Cyber polices can cover a panoply of risks, including losses to an insured's data or hardware, data-recovery expenses, the costs to hire forensic investigators, business-interruption losses, data-breach-notification and credit-monitoring services, and settlements, judgments and the costs of legal defense. However, cyber policies differ from one insurer to another and there is currently no standard cyber policy in the insurance market. To get the most out of cyber coverage, policyholders are best served by working closely with their staff members, brokers, attorneys and insurers to understand where their particular risks lie and what they are purchasing.

There is no silver bullet to protect against data leaks, and organizations need to be dynamic in their approach. One of the biggest mistakes a company can make is to view data security as an "IT problem" and not as a business problem. The consequences of a data leak can be serious and fines, injunctions, government audits and criminal liability can be imposed. The ability to quickly and inexpensively transfer data, files, records and other information around the globe has opened up a world of opportunity for many businesses, but it also presents a new world of risks. The risks are high; so be prepared, be proactive and develop a comprehensive strategy for addressing the risks.