Key Considerations to Protect Against Insider Threats in Cybersecurity

Contributing Counsel

William Ridgway / Chicago

Most companies have strengthened their cybersecurity defenses against outside hackers, but many often neglect the equal threat posed by those within their network walls — employees who already have privileged access to proprietary systems and whose activity often goes undetected by security systems designed to identify outside attackers. According to a March 2017 study by IBM Security, in 2016 more than half of the cyberattacks against the financial services and health care industries were carried out by employees who maliciously stole or unwittingly distributed sensitive data. Companies in these and other industries find themselves increasingly vulnerable from the inside as the value and volume of their data grows.

The strategy for addressing the growing problem of insider threats must be multidisciplinary, drawing on a combination of employee policies and training, human resources techniques, and technical measures. Companies should consider the following four steps:

1. Set Clear Guidelines in Confidentiality Agreements. Organizations should consider requiring new employees to sign confidentiality or nondisclosure agreements that identify and specify the circumstances under which an employee may access valuable information, such as customer data or trade secrets. These agreements must be carefully crafted, for they often become the linchpin in a lawsuit against an insider who makes off with company secrets. Common provisions that may be critical in litigation include definitions of the technology and proprietary information as well as descriptions of their proper uses, procedures for documenting the authorized use of the information, and destroy or return provisions.

2. Set Data Access Restrictions and Monitor Employees for Suspicious Activity. Data access restrictions play a critical role in thwarting insider threats. Employees should be authorized to use only the resources needed to do their jobs, a notion that is often referred to as the principle of "least privilege." That principle may be enforced using network segregation or software to log access to confidential documents or databases.

Equally important for an organization is a security information and event management solution, which aggregates data from a variety of sources — including databases, applications, networks and servers — to continuously monitor employee network activity. To take full advantage of these tools, the data must be reviewed to establish a "baseline" for regular, sanctioned activity. Doing so will allow monitors to identify irregular use, such as connections to unusual IP addresses at unusual times, abnormally large data transfers or unauthorized uses of encryption. Monitors ought to pay special attention to remote access, terminated employees and highly privileged users.

3. Enforce Clear Written Policies and Procedures With Signed Acknowledgment. Employers should design and enforce all organizational policies and procedures in a clear and consistent manner. Many insider incidents result from misunderstood or poorly communicated policies. In several documented cases, insiders have taken to a new employer proprietary information that they had a hand in creating, unaware

This article is from Skadden's *2018 Insights*.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

Four Times Square
New York, NY 10036
212.735.3000

that their previous employer owned it. (See "The Rise of Trade Secret Litigation in the Digital Age.") Organizations ought to provide documentation of and reasoning for all policies, and ensure they are consistently enforced. These policies may be reinforced through training that incorporates awareness of both malicious and unintentional insider threats.

4. Prepare for Employee Departures With Separation Agreements and Asset Collection Policies. Exit interviews serve as an invaluable, and often overlooked, method of limiting the security threat of outbound employees, regardless of the circumstances surrounding their departures. The interview allows the employer to reinforce confidentiality provisions and procedures and collect all company assets. The company also may ask for a final signed assurance that no confidential information or trade secrets are being removed from company control. At the same time, the company's information technology team should ensure that departing employees have all privileges and access revoked.

* * *

The frequency and cost of attacks from insiders will likely grow in 2018, particularly because an increasing number of companies are encountering an operational need to give employees, partners, suppliers and contractors remote access to their networks. The safeguards discussed above should help put companies in the best position to prevent or mitigate this growing problem.