Bloomberg Law

Professional Perspective

Managing Insider Cyber Threats: How to Handle This Newly Appreciated Risk

Suzanne Rich Folsom and Robert T. Garretson, Manatt

Managing Insider Cyber Threats: How to Handle This Newly Appreciated Risk

Contributed by Suzanne Rich Folsom and Robert T. Garretson, Manatt

The practice—and, some would say, art—of risk mitigation is a critical skill and a top priority for general counsels and corporate legal departments today. While every company faces unique challenges based on its own business model and operating environment, there is one overarching danger on which all companies agree: the threat of insiders, especially with respect to cybercrime.

From a legal perspective, it is difficult to imagine a more troubling scenario than when an employee or approved contractor takes an active role in undermining the business, often over a long period of time and unbeknownst to others inside the organization. That fear of the unknown is indeed stark. This scenario is not dreamed up in idle speculation or pasted together in a late-night cable television dystopian movie. Sadly, it is all too real.

Insider threats are especially insidious, given that they originate from colleagues with legitimate access to an organization's cyber assets, using that gateway for unauthorized and malicious purposes. Add to this mix those who unwittingly create vulnerabilities with a mistaken click on a faux website or on an errant link in a phishing email infected with malware, and the depth of this challenge begins to seem endless. As a result, bad actors are able to penetrate the robust perimeter defenses that guard an organization's data and begin their exploitation.

"The role that insiders play in the vulnerability of corporations of all sizes is significant—and growing," said Greg Gitschier, corporate security expert and retired U.S. Secret Service Agent. IBM's 2019 X-Force Threat Intelligence Index (analysis derived by IBM X-Force research teams monitoring of data across 70 billion security events per day in more than 130 countries) makes clear that the cybersecurity threats are on the rise.

A 2015 IBM report found that insiders were responsible for 60% of all cyberattacks. IBM defines insiders as:

> …anyone who has physical or remote access to a company's assets. Those are tangible items—including hard copy documents, disks, electronic files and laptops—as well as non-physical assets, such as information in transit. Although the insider is often an employee of the company, he or she could also be a third party. That includes business partners, clients or maintenance contractors, for example. They're individuals you trust enough to allow them access to your systems.

In other words, they are already inside your circle of trust.

Of these insider attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors. The summary and forward-looking analysis were equally chilling:

- There were 64 percent more security incidents in 2015 than in 2014, and improvements in detection and policy refinement made that possible

In 2018, the finance and insurance industry – at 19 percent of total attacks and incidents – continues to be the most targeted industry, attracting attackers in every geography. Coming in second, at 13 percent of total attacks and incidents, is transportation services.

- "Your next attacker is likely to be someone you thought you could trust. Insider threats continue to pose the most significant threat to organizations everywhere"

The impulses that drive insiders to commit cybercrime are multifaceted and complex, ranging from immediate financial gain (think ransomware), to the theft of intellectual property for re-sale to competitors, to disgruntled employees, to physical damage or sabotage to networks and connected systems, to political protests, along with other motivations.

"Leading indicators of personal and financial stress often form a path for insider cybercrime," said Tom Miller, chief executive of ClearForce. "Stress will manifest in the distracted worker who makes inadvertent mistakes, or the employee under financial stress who becomes susceptible to steal or vulnerable to exploitation."

Financial stress in the workplace is pervasive in today's workforce. According to a 2017 Career Builder study, 78% of workers are living paycheck to paycheck, including 1 in 10 who earn over $100,000 per year.

With this potential threat landscape in mind, corporate legal departments are well- positioned to serve in a dual role: establish the rigorous and necessary preventative policies, procedures, and appropriate response protocols that will shrink this potential risk as much as possible, and act as a key member of the cross-functional cyber crisis response team tasked with the investigation of cyber incidents and the deployment of corrective actions.

The National Insider Threat Task Force highlighted this point in its 2017 Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards, noting that the office of the general counsel should be included in a company's insider threat working group to help address questions that may arise about authorities and legal impediments. Moreover, legal department involvement becomes even more critical since disciplinary and law enforcement actions will most likely be brought against bad actors once they are discovered.

Broadly, there are three commonsense elements in an effective corporate program to deter insider cybercrime threats.

Evaluate

In building a robust program to detect possible insider cyber threats, it is important to identify specific, tangible metrics against which evidence is measured—especially since, as matters such as this move forward, evidence is likely what this will become.

Generally, quantitative measurements especially pattern recognition (i.e., Does this employee usually access this database after midnight, or did that process only begin recently?) are combined with qualitative and behavioral analysis (Was this employee recently denied a promotion? Do they have financial commitments that they need to satisfy? Are there workplace grudges that could fester and turn negative?) at the outset of such an analysis.

Clearly, the boundaries of such an evaluation need to be undertaken with care, given that there may be perfectly legitimate reasons why an employee has changed his or her working hours, and is for example resuming work later at night (i.e., a change in childcare). Employees have rights too, and they need to be respected and protected. Since we know that insider risk is fundamentally a "people" problem, said ClearForce's Miller, shares that any solution to mitigate this risk must be built on a foundation of privacy and transparency. Companies should—and many already do—obtain appropriate levels of consent to support enhanced risk management to protect both the organization and its employees.

In-house counsel should also establish written procedures ahead of time with the assistance of external labor and employment experts to help ensure that the infrastructure of such a program generates the needed information and does so in a legally sound manner. Additionally, the larger the organization, the more important it is to understand jurisdiction-specific privacy laws and regulations and comply with them.

Build

In Nov. 2017, Forrester published best practices for building strong cybersecurity architecture to effectively confront the insider cyber threat, and an operational playbook to outline responses.

Of particular importance from an in-house legal perspective is the need to build—in advance of any urgent need—a tightly focused cyber crisis response team. With the understanding that internal investigations often lead to legal or disciplinary actions (a process where legal collaborates routinely with other departments such as corporate security and human resources on a variety of issues), staffing this team with personnel who recognize and understand the imperative that confidentiality and mature judgment are paramount.

Forrester recommends, and we concur, that this team should be based outside of the company's existing cybersecurity team. At its core, the insider cyber threat is not merely a technical problem (although there is certainly a need for technical expertise), but rather, one that more closely parallels existing protocols around employee investigations and corporate security.

Consequently, organizing this effort under the auspices of the corporate legal department will infuse this team with a powerful home that intuitively grasps the gravity of the potential threat and has the necessary authority and resources to have an impact. It will also provide a clear path to communicate the issues (as appropriate) to the executive management team, the board of directors, and to external stakeholders, if needed; and a commitment to develop the right rules and procedures to protect the company over the long-term.

For global organizations, this distinction is even more important. As general counsels and corporate legal departments understand, overseas operations may pose unique challenges when it comes to the protection of employee rights, especially with respect to privacy and medical information, and the consequences of non-compliance (whether intentional or not) can be severe.

Accustomed as they are to the need to gather the requisite knowledge to understand the company's challenges and risks and make difficult decisions, especially in the context of the need to work with outside regulators and law enforcement authorities, corporate legal departments are well-equipped to provide the speed, evaluation, judgment, and implementation that is often necessary to address the threat that an insider cybercriminal represents.

Donna Wilson, managing partner and co-leader of the privacy and data security practice with Manatt, Phelps & Phillips, which has successfully represented numerous companies faced with data security issues, concurs:

> As soon as a security breach becomes public or customers receive notice, multiple class actions are now commonly filed within hours and continue to be filed over the succeeding weeks and even months. In addition, a diverse group of regulators commence their own investigations. It is critical for your outside counsel with whom the company internal counsel works to activate quickly and deploy the necessary legal experts to support a multi-disciplined game plan to address all legal and reputational issues.

Continually Assess and Strengthen

As corporate legal departments have put in place regulatory and compliance programs to effectively investigate, measure, and manage risk from third-party partners and vendors, so too they are well-positioned to guard against cyber threats from inside the organization.

Even if the company believes that it has instituted a best-in-class program to detect insider cyber threats, it should continually assess the operating conditions and risks to determine whether personnel and resources are appropriately allocated and aligned with the potential threat environment. Any weaknesses, opportunities, or threats should be evaluated with the proper program enhancements put in place to maintain a robust and effective program.

Collaboratively teaming with other key corporate departments—from human resources and corporate security—a proactive program that is vigilant (in terms of monitoring potential threats and then acting on them with dispatch) and inquisitive (vacuuming up as much information as possible about the lessons learned from other companies and their encounters with cybercrime) will yield the most effective results.

While building a "hand-raising" culture can be difficult, there is real value in developing a strong internal culture where, to borrow a phrase from Homeland Security, "see something, say something" becomes a rallying point where team members can contribute to the organization's overall defense.

Going Forward

Seemingly trustworthy employees who are intent on breaking the law will continue to bedevil companies via cyber threats, financial fraud, insider trading, or a host of other equally illegal behaviors, but with the right programs in place, the threat they pose can be mitigated.