Addressing the threat within

The right way to combat insider cyber threats
News coverage of cyber breaches tends to focus on external threats like cybercriminals, paid hackers or state-sponsored actors. But threats from insiders—employees, contractors and others with sanctioned access to your systems and data—are every bit as real and every bit as dangerous. Insiders face much lower barriers when committing cybercrime. Where external actors must devise ways to break into a target organization’s system, insiders enjoy ready, sanctioned access. Unfortunately, organizations pay insider threats little heed and exacerbate the issue by failing to report insider incidents. Yet the FBI notes that damages from individual insider incidents that it investigates range up to $3 million. Losses include:

- the value of stolen data
- the significant costs of IT services and countermeasures
- legal fees
- lost customers and revenue
- credit monitoring services for customers and employees affected by insider incidents.

The 2013 Snowden case caught the attention of senior executives and risk committees well beyond the public sector. Snowden, a security contractor to the US National Security Agency, was not a high-level executive with elevated privileges to access sensitive data. He was an IT contractor with access to data he did not need to perform his job, allowing him to appropriate and release large volumes of classified material. Snowden both the public and private sectors to reevaluate both the frequency and potential damage of insider cybercrimes.

The FBI notes that damages from individual insider incidents that it investigates range up to $3 million.
A number of other private-sector insider breaches have received media attention:

- A foreign national employed by a major technology company, one of few people with access to the source code for proprietary software, copied that software and attempted to sell it to benefit himself and his home country. He was arrested by the FBI in a sting operation.

- A former reservations agent for a regional airline sabotaged her employer’s ticketing and seating management system, during the two months before her exit, by setting up a fake employee account and disrupting the company’s IT infrastructure. She was discovered, apprehended, and pleaded guilty to accessing a system to which she did not have lawful access rights.

- A car manufacturer discovered that an employee using false user names sought to change code to sabotage the organization’s operating system and to export valuable IP to third parties. The stated motive of the employee for these actions was revenge over not receiving a promotion.

- Over three years, an employee at a global wealth management organization illegally downloaded to his home computer the personal and financial information of more than half a million customers. The employee apparently planned to use the data at a new employer.

All of these cases point to the need to reduce risk by reviewing how access to systems and data is controlled for employees, contractors, and partners. How effectively that is done makes a major difference in your security.

**Identifying and addressing threats**

Insider threats fall into three broad categories:

- **IT sabotage:** An insider uses access to IT systems to harm the organization; an associated organization, such as a supplier or customer; or an individual, such as a senior executive. This could be accomplished, for example, by undermining operational or reporting processes.

- **Theft of IP:** An insider uses IT to steal the organization’s IP, such as account information, trade secrets or financial or strategic plans. This category includes industrial espionage involving outsiders who recruit insiders.

- **Fraud:** An insider uses IT for the unauthorized modification, addition or deletion of an organization’s data (not programs or systems) for personal financial gain, or to steal information associated with crimes such as identity theft or credit card fraud.

An insider uses access to IT systems to harm the organization; an associated organization, such as a supplier or customer; or an individual, such as a senior executive.
The motives behind insider threats may be emotional or financial. Emotional motivations include resentment toward organizational policies, anger at not receiving a promotion or raise, political or social activism or a desire to embarrass the organization or its leaders. Financial motivations include direct payments from external parties for acts of sabotage or for access to intellectual property, seal-dealing arrangements, kick-back schemes or other frauds.

Getting it right

An effective insider security program will effect more than security. It also impacts the relationship between your people and your organization and potentially the efficiency with which they can do their jobs. Therefore, addressing insider security requires a broader team and a more nuanced approach than dealing with external threats. As with external security programs, this effort should involve their chief information security officer’s (CISO’s) function, the chief risk officer (CRO) and the chief legal officer (CLO) or general counsel. But an internal security program should also involve the chief human resources officer (CHRO) to ensure that the impact on and communications with your personnel are appropriately addressed.

An effective insider security program will effect more than security. It also impacts the relationship between your people and your organization and potentially the efficiency with which they can do their jobs.

This multi-disciplinary team should begin by determining which positions need access to which systems and data. This involves interviews and surveys of functions throughout the business to drive a disciplined analysis of business needs and interrelationships. The team must then establish procedures for appropriately granting and controlling access to and use of the data and systems in question, including methods for ongoing monitoring to ensure future compliance. Next, communicate the program to all employees and contractors in ways that both support the organization’s compliance and legal concerns and that engender acceptance and cooperation.
An effective program for controlling insider cyber risk addresses each of the five following issues:

- **Program governance.** The first step toward an effective insider threat management function is to develop and deploy the right frameworks, policies and procedures, access, and activity monitoring and response protocols. The CISO may champion the program, but it should be aligned with HR, legal and, possibly, compliance and risk management. This team should develop and manage the program on an ongoing basis to detect, monitor, address and recover from insider incidents and breaches. It should also design, implement and ensure the proper performance of tiered vetting and background checks for sensitive roles, such as those for executives and system administrators.

- **Vetting processes.** The degree of vetting should be scaled to the sensitivity and value of the data and systems to which individuals in specific functions and positions have access. One size does not fit all, yet this is the approach many organizations employ. When employees move to new positions involving more sensitive or more valuable IT assets, be sure they are re-vetted according to the sensitivity of the new role.

- **Controlling access.** For any given role, access to systems and data should be grounded in an analysis of what is actually required to perform that function. For reasons mainly related to convenience and a fear of insulting otherwise trusted insiders, many organizations fail to appropriately limit access. Your insider risk team should also escalate or deescalate user privileges as required when people’s roles or the organization’s IT assets change. To prevent movement of sensitive data to unsecure locations, the program should monitor the movement of data and use security analytics to understand insiders’ behavioral patterns.

Movement of sensitive data to unsecure locations, the program should monitor the movement of data and use security analytics to understand insiders’ behavioral patterns.
• **Communication.** Communication concerning an insider risk program requires sensitivity and diplomacy. You do not wish to give the impression that insiders are not trusted, but instead seek to clearly communicate the need for an internal risk control program and explain its role in mitigating threats. Organizations also must be mindful of the legal or privacy implications of such a program – including, but not limited to, any requirement to inform employees concerning routine security monitoring activities. By increasing security awareness, the program can communicate insider threat themes, develop and deploy modules targeted to certain functions and issues and educate insiders about secure handling of sensitive data. It also assists by training managers to spot indicators of employees who may be at heightened risk, such as those with personal or financial problems or those displaying disgruntlement.

• **Enhanced monitoring.** An effective insider risk program can build out appropriate investigation and response models based on behavioral patterns, data movements, incidents and breaches. These should address the need to monitor people in different roles who use different data, and activities within a given environment. This also entails tracking insider threats and cases to refine the organization’s understanding of the threats it faces and their potential causes, and to improve vetting, access management and communication efforts.

In general, insider threat management programs tend to be under-developed. Some organizations “like to trust” their employees. Others underestimate the seriousness of the threat or the potential damage. Still others have programs that are not integrated with other functions or that lack essential features, such as proper vetting or access controls. And some programs are too heavy-handed, which can hamper efficiency, cross ethical or legal lines, or alienate talented employees and contractors.

By increasing security awareness, the program can communicate insider threat themes, develop and deploy modules targeted to certain functions and issues and educate insiders about secure handling of sensitive data.
Trust, but verify

In today’s digitalized environment, employees, contractors and partners understand the need for an organization to protect its digital assets. Oddly, in our experience it is often senior management that fails to understand that need, or to act on that understanding.

The risks are real and serious due to the growing value of an organization’s data, IP and processes. Management can readily address these risks, with the right expertise, experience and assistance. But management commonly overlooks these risks, often with serious consequences.

To assess the effectiveness, efficiency and ethical tone of your insider threat management program, get in touch with a Grant Thornton professional today.
Contacts

John Pearce
Principal
Cyberrisk
T  +1 703 637 4071
E  john.pearce@us.gt.com

Johnny Lee
Principal
Forensic Advisory Services
T  +1 404 704 0144
E  j.lee@us.gt.com