Kevane Grant Thornton
An instinct for growth™

Advisory
Organization
Data protection

Addressing the threat within

September 16, 2019

The right way to combat insider cyber threats.

Ojel Rodríguez
Partner Head of Advisory
T (1) 787 754 1915
E ojel.rodriguez@pr.gt.com

Visit our website to view additional articles
www.grantthornton.pr

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

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.
- **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.

Getting it right

An effective insider security program will affect 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.

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.
- **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.
- **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.
- **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.
- **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.

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.

Source:
Grant Thornton library articles

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for assistance in relation to this or any other matter, we will be glad to assist you.

Kevane Grant Thornton
An instinct for growth™