Forbes

WHERE AMBITION CONNECTS WITH OPPORTUNITY
Connect with HSBC's global network
START NOW
HSBC

Steve Culp Contributor

Leads Accenture's Finance and Risk Services globally.

Opinions expressed by Forbes Contributors are their own.

LEADERSHIP 5/10/2016 @ 3:02PM | 557 views

Cyber Risk: People Are Often The Weakest Link In The Security Chain

This post was co-written with Chris Thompson, a managing director in Accenture's Finance & Risk Services practice.

The threat of cyber crime has created a significant increase in interest on the topic of cyber security, with organizations spending billions of dollars to protect themselves against a fast evolving array of current and potential future threats. Many spend heavily on monitoring, surveillance and software; however, they often neglect the risk exposure created by their own people – and, in this digital age, by their customers.

Photo: Shutterstock

Like bank robbers of yore, cyber criminals target "where the money is," and that often means banks and financial institutions. With many decades' experience in protecting themselves against crime, banks and insurance companies typically have reasonably sound physical and technical cyber security defenses in place. The concept of currency has changed, however, and now, rather than trying to cart off bills and coins, cyber thieves seek to steal valuable information.

[8 Simple Rules For Beating Hackers And Cyber-Thieves]

Cyber criminals are willing to take extreme measures to obtain information from financial institutions. For example, criminals have infiltrated banks by placing employees within financial institutions – essentially their own deep-cover agents – who get in position to steal sensitive data and conduct fraudulent securities transactions. In many cases, even long-term, trusted employees may pose risks.

Vendors are another point of potential vulnerability. Financial institutions may have strong cyber defenses, but they also rely upon third parties – often entrusted with highly confidential data related to procurement and transactions, but who may not possess the same levels of security and sophistication of the financial institutions they are serving.

Cyber criminals gravitate to the weakest spots in institutions' defenses, and that often means going after customers. Bank accounts have typically become part of customers' technology "footprint" with account information contained on home PCs and on mobile devices. Criminals seek to compromise data security in a variety of ways, including installing malware – often using "phishing" emails – to compromise customers' data security, and emulating unsecured Wi-Fi facilities in cafes, restaurants and airports; thieves have even been known to set up fake accounts to direct traffic where they want it to go.

One of the big problems for financial institutions is that there are multiple people and departments responsible for managing the various risks related to cyber security. In an age in which cyber criminals can do enormous damage, there is a strong case to be made for aligning and/or integrating various functions such as fraud prevention, IT security and compliance into a more cohesive group, possibly with a chief cyber risk officer overseeing all digital security measures.

In our work with global financial services institutions, we have identified five key factors that should be addressed hand in hand with secure IT when dealing with the threat of cyber crime:

1. Training And Risk Culture: Financial institutions vary widely in terms of their culture. Some have grown through mergers and acquisitions into fragmented organizations with disparate cultures. Others are much more homogenous. Some, such as investment banks, drive their people hard but promise outsized rewards. Each organization has to identify its own unique learning styles and implement the appropriate initiatives – which may include advanced learning methods such as gamification – to impart the right kind of cyber behaviors.

2. Controls: Each terrifying cyber scenario needs to be decomposed into the steps or actions that the criminals need to execute if they are to succeed. From phishing, to installing malware, gaining access, controlling an account, executing fraudulent transactions, etc. – these steps are risks or issues that need a series of strong controls in place. There is no substitute for a holistic risk assessment and control management framework, with robust mentoring and testing.

3. Measurement With A Purpose: Organizations need new ways to identify and track employee behavior that may indicate cyber crime in progress, either because of an insider or because their account has been taken over through malware or a trojan. Analytics can help spot activities – such as employees working during non-working hours, employees with poor performance reviews who have access to customer data, or the downloading of unusually large files – which correlate strongly with misbehavior or outright crime.

4. Operating Model: Cyber security must work well across the organization. The right operating model bridges the IT, front office, fraud and risk silos. It can help define accountability, enforce good decision-making and measure effectiveness. Organizations have a number of operating models from which to choose, including establishment of a “cyber czar” position to set policy and influence activities, or the creation of an enterprise-wide cyber risk function to identify, measure and respond to threats.

5. Resilience: Despite the organization’s best efforts, things can and will go wrong. A comprehensive resiliency plan – which includes elements such as event response, communications, crisis management, detection, threat identification and operational monitoring – can help minimize losses and protect the organization’s reputation in the event of a breach.

The digital revolution has made it easier for financial institutions and their customers to work together, but digital commerce has created many new points of entry for potential cyber criminals. A comprehensive, organized approach to training, communicating with and monitoring people can help banks and other financial services firms limit their exposure to fraud perpetrated both from outside and inside the institution.

This article is available online at: