SIFMA Insights:

Spotlight: Building Resilience with a Culture of Cyber Awareness

May 2019

sifma®

Spotlight: Building Resilience with a Culture of Cyber Awareness

There are few industries more prone to the threat of cyber attacks than financial services, as financial institutions move money and work with (and continue to protect) sensitive client data. Firms are constantly assessing the risks and areas of the firm that may be vulnerable. Organizations are making significant investments in personnel and technology to mitigate the risk from cyber attacks, and they are continuing to build cultures of cyber awareness across the organization to keep everyone vigilant in monitoring cyber risk.

Cybersecurity and data protection remain top of mind in the financial services industry. There are now more mobile devices than people on the planet: 8.9 billion versus 7.6 billion. The access to information is instant while on the move, with an increasing number of devices being connected to the Internet (Internet of Things/IOT: doorbells, medical devices, cars, refrigerators). There is also an unprecedented amount of personal information (data) posted and transferred online (LinkedIn, Facebook, Instagram). These access points create a more complicated cyber threat landscape.

Why Building Resilience Matters

The average cost of a data breach in 2018 was $3.86 million (all industries), of which $1.45 million was attributable to lost business[1] (this will vary by the nature and scale of the breach and data accessed). Another less measurable component is reputational risk in the aftermath of a cyber incident. As this type of risk includes the potential to lose the trust and confidence of clients, firms understand the importance of building cyber resiliency to preserve this trust.

Who owns reputational risk if there is a cyber incident? Preventing cyber incidents and managing their consequences is a responsibility that runs across the organization – from the front office who interact with clients, to the back office staff responsible for technology and risk management personnel, with final oversight by senior management and the Board. As such firms continue to utilize the three lines of defense model to mitigate the risk of a cyber attack: business, risk management and audit.

This culture of cyber resilience also includes an awareness of insider threats. The 2018 Verizon Data Breach Investigations Report indicates 28% of cyber attacks across all industries involved insiders. Financial services is lower at 19%. Notably, regulators acknowledge that financial services is among the most mature in developing cyber defenses. Yet, firms must continue to monitor for insider threats. Risk factors of concern cited by firms surveyed in the 2018 Insider Threat Report[2] included: user access privilege management (37%); an increasing number of devices with access to sensitive data (36%); and the increasing complexity of information technology (35%). Additionally, the vast majority (86%) of organizations (all industries) surveyed already have or are building an insider threat program: 36% have a formal program in place, 50% are focused on developing a program.

It's About People, Not Just Technology

Unlike 15 years ago, cybersecurity is not just about building defenses around a perimeter. The scope of cyber attacks has expanded to include malicious or destructive attacks, not just those aimed at stealing money and data.

[1] 2018 Data Breach Study; IBM/Ponemon Institute
[2] 2018 Insider Threat Report; CA Technologies, Crowd Research Partners and Cybersecurity Insiders

For example, a threat garnering heightened attention today is destructive malware which corrupts data (attacking the I in CIA, or the three parts of data security: confidentiality, integrity and accessibility). Therefore, today's information security is not just about the technology. It is also a human problem, ensuring humans using the technology do not unintentionally allow malware to enter the enterprise by, for example, clicking on a bad link. The financial services industry is also leading in human solutions by building a culture of cyber awareness at the: (a) firm level, with cyber resiliency programs, insider threat training and the use of innovative technology; (b) industry level, through information sharing and developing best practices (SIFMA's Insider Threat Best Practices Guide); and (c) sector level, partnering across firms, regulators, supervisors and law enforcement to share information and make the whole system more resilient.

Not all insider incidents are the result of malicious actors, some are the result of human error. This makes security crucial and necessary to be embedded into everything the organization does. In April 2018 IBM Security Intelligence noted 65% of Chief Information Security Officers (CISO) spend "sleepless nights" worrying about phishing scams, and 61% fear disruption to processes caused by malware. This indicates it is essential for firms to not just look at technology but also the human element of cyber defense. For example, phishing remains a popular method among cybercriminals of gaining initial access to databases and systems, and 49% of companies that have already suffered a significant phishing attack are targeted again within a year. Phishing is an attempt to obtain sensitive information by disguising an email as coming from a trustworthy source, for example another employee in one's firm.

Firms are countering this threat by developing programs of phishing training and using technology solutions to identify suspicious links or attachments. Security belongs to everyone, which is why many cyber experts tout the benefits of creating a culture of cyber awareness. The ISACA/CMMI Institute 2018 Cybersecurity Culture Report asked firms which steps they are taking to improve their cybersecurity culture: 80% said employee training; 79% replied communicating behavioral policies; and 75% noted the importance of management committee ownership.

A Culture of Cyber Awareness

Financial institutions have built a culture of cyber awareness from the top down, i.e. a leadership-driven culture. The messaging is simple – cyber resiliency awareness is an important part of the firm's success. Security is not just IT or compliance's problem, it is everyone in the organization's problem. And the key to mitigating cyber risk is having everyone in the organization concerned about cyber awareness. Financial services employees understand cyber resiliency is critical to meeting client expectations, delivering client services and safeguarding client data.

Maintaining this culture requires compliance training across the firm, having processes in place to report incidents or suspicious activity and constant monitoring of systems and activities. Additionally, IT and the cybersecurity teams partner with the front-line business units and openly communicate with them. There is evidence to show that there is a benefit to all parties if they work together – collaboration, not silos – to protect the firm from cyber attacks and the reputational risk from an incident. Training and ongoing communication changes the mentality of employees.

By reminding people that customer service could be disrupted with a cyber incident, which negatively impacts everyone across the organization, a culture of cyber awareness is continuously nurtured.

Author

SIFMA Insights
Katie Kolchin, CFA
kkolchin@sifma.org

SIFMA Insights can be found at: https://www.sifma.org/insights

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate on legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.