REPRINT FINANCIER WORLDWIDE

NOVEMBER 2017

FINANCIER WORLDWIDE corporatefinanceintelligence

BANKING & FINANCE

Financial services on the front lines for cyber security

PAMELA PASSMAN

CENTER FOR RESPONSIBLE ENTERPRISE AND TRADE

In 2016, the global financial messaging system, SWIFT, was at the heart of a high profile $81m heist at Bangladesh Bank. A series of attacks using the SWIFT banking network exploited the vulnerabilities of member banks, allowing attackers to gain control of legitimate SWIFT credentials. They then used those credentials to send 'trusted' SWIFT fund requests to other banks.

This case marked a new era of sophistication by hackers and highlighted the vulnerabilities associated with third parties and those across value chains.

The financial services sector is particularly reliant on third parties to reduce costs, gain competitive advantage and improve the customer experience. PwC's 20th annual Global CEO Survey highlighted the rapid evolution of the sector through new technologies, such as artificial intelligence, the mining of Big Data and the importance of tapping into this innovation to gain access to new customers. Many companies are turning to third parties to do so – 31 percent of the CEOs surveyed from banking and capital markets

CREATe.org
Center for Responsible Enterprise And Trade

Pamela Passman is the president and chief executive of the Center for Responsible Enterprise and Trade. She can be contacted on +1 (202) 842 4701 or by email: ppassman@createcompliance.com.

are planning to collaborate with entrepreneurs or start-ups over the next 12 months.

This, combined with the plethora of additional third-party partners, and what the sector deals with every day – capital and personal information – puts financial organisations on the front lines of cyber security. Indeed, the financial sector is considered a vital component of the US' critical infrastructure by the federal government.

What is at stake?

The Ponemon Institute found that companies experience a 5 percent decline in their stock price after a cyber breach has been disclosed and 31 percent of consumers surveyed said they discontinued their relationship with a company that had a data breach. The sources of such breaches often are not the financial institutions themselves. Breaches can often be traced to something as simple as a contractor that performs human resources work for a large bank, for example. All it takes is for one person to make a mistake.

Though larger firms and multinationals face pressure to have effective cyber security measures in place, smaller third parties are not usually as secure. They might lack the resources and know-how, or they might simply take the view that they will deal with a breach after it happens. This is clearly on the minds of executives. Navex Global's 2016 Ethics & Compliance Third Party Management Benchmark Report found that cyber security, along supply chains, was among the top concerns, behind conflicts of interest and bribery and corruption.

These cyber security concerns are translating into procurement decisions. A 2015 survey by Gartner found that by 2018, 50 percent of organisations in supply chain relationships would use the effectiveness of their third parties' security policies – and associated controls – in determining whether to continue the relationships (up from 5 percent at the time of the survey).

What financial services organisations need to do

The guidance on cyber security that organisations should have in place stems from a bevy of sources, including the New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies, the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the International Organization for Standardization (ISO) 27001 standard.

There are practical measures that companies can implement across their third-party risk management approach. At a high level, cyber security involves people, process and technology.

Working with the human resources groups, it is important to make sure employees understand their role in helping the organisation to be secure; preferably this will be done in employees' initial 'onboarding' training. Given the evolving nature of cyber attacks, however, ongoing training is vital, as well as policies and procedures to ensure that employees only use authorised software and do not introduce improper devices onto the network. They must also consider the ramifications for non-compliance. Are they being consistently communicated?

It is important that training goes all the way to the highest level of the organisation. Curiously, just 25 percent of organisations train their board members on cyber security, according to Navex Global's 2017 Ethics & Compliance Training Benchmark Report.

CREATE.org
Center for Responsible Enterprise And Trade

Monitoring is the weak link in most organisations. Monitoring can take a variety of forms, from an ongoing review of networks, to identifying unusual activity, to processes to catalogue who has access to sensitive data, systems and networks. Is there a procedure to determine whether all software is up to date? Is there an integrated response plan – with an emphasis on backup and recovery – across IT, human resources, operations and other departments? Who needs to be involved and when do you bring in outside experts?

Protecting against a cyber attack requires a broad range of technology measures as well. From access controls, to physical and virtual network protections and patching software with security updates, among other procedures.

It is not a matter of if a breach will happen. Today, it is really a matter of when. For financial services organisations – often the guardians of information that can threaten a person's finances or upend whole economies – it is critical to build cyber resiliency that is flexible enough to enable innovation with third-party partners, and provides a robust fortress built for addressing today's evolving security challenges. ■