affirmlogic

Rethinking Cyber Security in Financial Services

The Financial Services industry is comprised of a large number of institutions of various sizes and a wide array of interconnected systems that manage the processing of millions of transactions each day. These provide the foundation for the global economy. Yet the same factors that account for the industry's success make it particularly vulnerable to cyber-attack. In 2018 the financial services industry experienced 35% of all data breaches, putting it in the unfortunate position of being the most-breached sector worldwide. British financial services firms saw a fivefold rise in data breaches in 2018 compared with the year prior. And while 2019 data has yet to be released, the situation seems to be getting worse. These threats carry the risk not only of data breaches but of legal risks such as litigation and steep regulatory fines.

The **U.S. Securities and Exchange Commission** recently issued guidance for public companies to be more open to disclosing cybersecurity risks, even before a breach or attack occurs. The **New York Department of Financial Services** issued the following Cybersecurity Risk Alert:

> *There is currently a heightened risk of cyber-attacks from hackers affiliated with the **Iranian** government… all regulated entities should be prepared to respond quickly to any suspected cyber incidents. It is particularly important to make sure that any alerts or incidents are responded to promptly even outside of regular business hours – **Iranian** hackers are known to prefer attacking over the weekends and at night precisely because they know that weekday staff may not be available to respond immediately…*

How secure does a financial services firm need to be, to be safe? The obvious answer seems to be: "as secure as possible." But budget realities lead to compromise and organizations often have to make difficult decisions balancing security and cost. The key is to have a realistic sense of the risk, the necessary defenses in place, and an understanding of all of the implications of successful attacks.

Financial institutions rely on business-critical applications to serve customers, promote their services and connect to back-end databases. Many of these applications are hosted online, making them easily accessible to hackers via the Internet. The result: frustrated customers and trading partners who are unable to access critical services when they are most needed. For financial services firms, the repercussions can be even worse, including disrupted business flows, stolen data, damaged reputation and lost revenue.

Employees are among the top cybersecurity threats to financial institutions. They may fall victim to phishing scams or accidentally download malware. Unhappy employees may cooperate with hackers or insert “logic bombs” in internal systems to destroy them from inside if the employee is ever fired. often take years to detect. Research shows that malware (whether from external sources or insider threats) resides on corporate networks for an average of six years before being detected.

Amid increased exposure to these risks, financial institutions need to take measures to ensure greater data security to protect clients and minimize legal exposure. But perhaps just as important as technical challenges are institutional challenges, such as limited budgets and a lack of buy-in from leadership. Cybersecurity often takes a back seat to factors like customer satisfaction and regulatory compliance in the minds of executives, especially at smaller institutions.

Senior executives often convince themselves that their firm is not going to be a primary target of a “Zero Day” attack, and that they can implement stronger cybersecurity after they hear of attacks against other organizations. This leads to a dangerous case of “Security Complacency”, an attitude that nothing further is required to protect the firm, based on their own erroneous assessment of limited risk.

For security leaders to cope with the increasing complexity of their aging infrastructure, they must embed state-of-the-art security within their transformational plans. It’s imperative they look at how they protect their existing environment while simultaneously bolstering their security measures.

Banks aren’t immune to the ongoing cybersecurity skills crisis. As they struggle to build a world-class cyber security team, there is a chronic shortage of staff to manage basic tasks such as vulnerability patching, let alone to investigate recent attacks. Despite initiatives to use technology more effectively, there is still a surprising over-reliance on manual processes throughout the sector. This can be catastrophic.

Imagine the following scenario: A suspicious file is found on a network server. Analysis shows it is likely to be malware but knowing if it is malicious is only the first step. Was it a random attack or was someone targeting the organization specifically? If it was targeted, who is the attacker? What was their goal, a specific target or just general destruction? Has the malware been run yet, and if so, did it leave any damage behind, like data corruption or a “back door” for transmitting vital data to criminal third parties? Your ability to quickly answer these questions can be the difference between a nuisance and a nightmare.

The year 2020 is not going to be easy for executives responsible for cyber security in financial services firms. As cyber security talent remains scarce and threats multiply, they must invest in the skills, technology and advisors that can prepare and support them to face the most critical security issues facing their organization.

For more information on how leading financial services firms around the world are rethinking cyber security, please contact: