Canadian Institute of Actuaries
Institut canadien des actuaires

Cyber: financial and insurance threat landscape

JESSE JORDAN

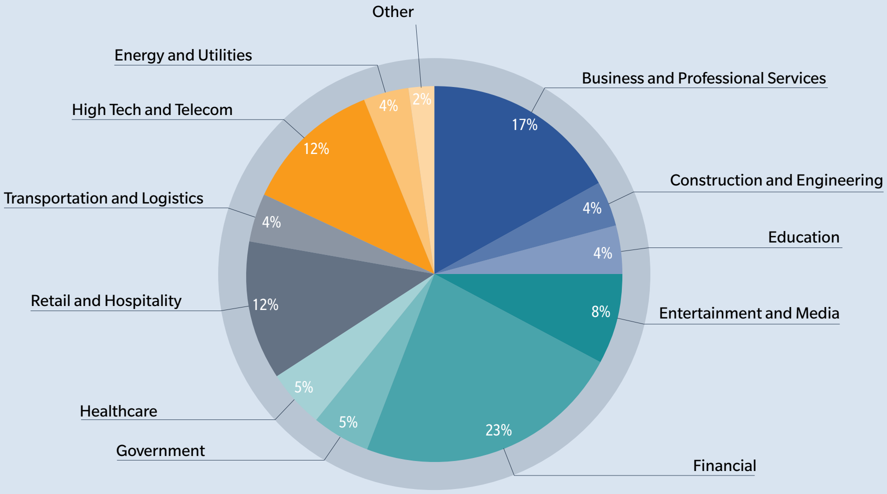
Principal Consultant, FireEye Mandiant

This article is part of *Enterprise Risk Management 2019: The New Wave of Risks*, a collection of articles on enterprise risk management (ERM) from the Canadian Institute of Actuaries (CIA). The articles are written by subject matter experts, both actuaries and non-actuaries, giving us their own professional opinions and experiences, and highlighting new and emerging hot topics taking centre stage in today's world of risk management. **Read all the articles at cia-ica.ca/erm**.

Cyber security attacks continue to evolve. Organizations of all sizes being are being targeted by a variety of threat actors using a wide range of tactics and techniques. Extortion incidents are on the rise and attacks against cloud services have increased due to organizations moving more workloads to the cloud as part of their broader IT strategies.

Although cyber security attacks against all industries are noted, financial institutions continue to make up the majority. Of the incidents that the Mandiant consulting division at FireEye (a cyber-security firm) responded to in 2018, 23 per cent were from the financial services industry.

Figure 1: FireEye Mandiant M-Trends Report 2019 – industries investigated



Source: FireEye Mandiant 2019. Reproduced with permission.

Financial and insurance threat landscape

State-sponsored threat actors continue to pose a high risk to the financial and insurance industries, both of which have access to a range of sensitive information on their clients. Specific to insurance, brokers examine potential risks associated with their clients as part of the underwriting process. The information gathered, which includes comprehensive profiles of vulnerabilities in high-value assets, can be used by threat actors to derive where potential weaknesses exist. State-sponsored threat actors can also inform a nation's commercial interests by obtaining economic intelligence from business negotiations with foreign entities.

In 2018, North Korea, Russia, China, and Iran were responsible for the greatest number of cyber espionage attacks worldwide. We have seen enhanced sophistication of attacks from North Korean actors targeting financial institutions through the exploitation of previously unreported vulnerabilities (zero-day vulnerabilities), targeted phishing attacks against CEOs and chief financial officers, and financially motivated supply chain attacks. Supply chain attacks can occur when threat actors successfully infiltrate an organization through a third-party supplier or service provider through shared code or infrastructure via trusted distribution methods. These attacks are particularly effective, as a single compromise along the supply chain can compromise a vast number of victims. Mandiant has noted recent examples where threat actors were able to embed malicious code into collaborative software resources, in some cases via malicious insiders, or where devices with malware pre-installed were shipped to clients. If the supply chain breach is deep enough, state-sponsored threat actors essentially go unnoticed.

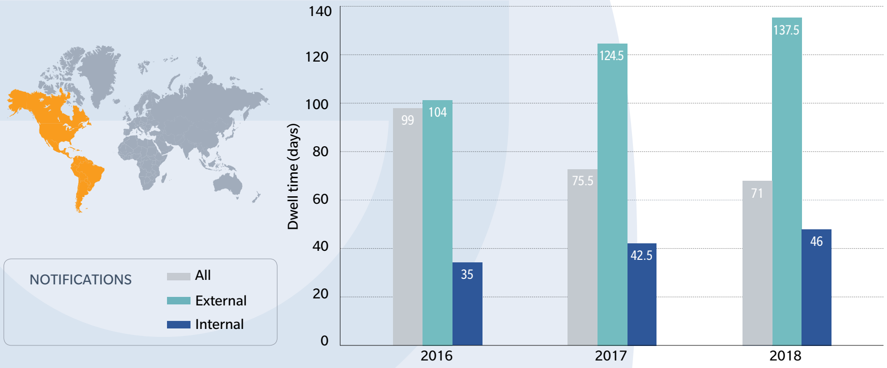
Supply chain attacks are seen by threat actors as an effective way of bypassing years of investment into perimeter-based defences made by organizations with mature cyber defence capabilities. Over the past few years, Mandiant has identified a substantial increase in these types of attacks.

The rise of financially motivated supply chain attacks by state-sponsored threat actors can partially be attributed to increased sanctions against some of the referenced nation states, where the need to obtain funds using any means is considered necessary. For example, in operations across the globe, North Korean threat actors have attempted to steal over US$1.1 billion from financial companies by abusing bank-to-bank transfers over the previous two years.

Cyber criminals also continue to target companies in the financial and insurance space by leveraging social engineering and phishing attacks to deliver ransomware with the aim of extorting organizations for financial gain. Cyber criminals use similar methods to steal sensitive information from both insurers and their respective clients, holding this information with the threat of public disclosure should the organization not meet certain financial demands. Cyber criminals will also leverage client/underwriting relationships to gather sensitive information and subsequently sell this on underground markets for identity theft, extortion, and fraud.

Mandiant predicts that cyber crime, especially cyber fraud, will continue to increase in 2019. Attacks against financial websites where virtual "skimmers" are used to steal personal information, payment card numbers, and credit card CVV codes will continue to rise. In 2018, financial threat actors used advanced techniques to reverse-engineer account registration processes against online portals to gain access to accounts, transfer funds, order cheques, and modify transaction destinations.

Figure 2: FireEye Mandiant M-Trends Report 2019 – Americas median dwell time



Source: FireEye Mandiant 2019. Reproduced with permission.

Hacktivists, although posing a relatively low risk to the finance and insurance sector, continue to cause disruption in the form of ideologically motivated attacks where the goal is often to cause reputational damage to an organization that results in loss of business, either by exposing sensitive client information, stealing proprietary information, or attempting to cause business downtime by performing denial-of-service attacks against customer-facing websites or other critical systems.

Early detection and response are key

Organizations in the Americas are getting better at detecting threats to their environments early. The median dwell time, which is the amount of time threat actors have remained on victim networks from first evidence of compromise through to detection of the breach, decreased from 99 days in 2016 to 71 days two years later (see Figure 2). Much of the decrease can be attributed to organizations working to continually improve their ability to detect threats early – either through creating internal-threat-hunting capabilities or developing enhanced network, endpoint, and cloud detection and response capabilities.

In addition, ensuring security involvement within ERM practices with a clearly defined risk strategy as it relates to cyber threats is important. Organizations should adopt a structured and measured view of security risks and provide clear strategies for mitigation and remediation.

Detailed processes around quantification, ranking, ownership, tracking, and mitigation should be developed to ensure a consistent and comprehensive approach is followed. Centralized risk management solutions can be implemented to assist with standardized tracking of cyber security risks and associated processes.

When tracking risk, factor in suppliers that could expose the organization if breached, and associated controls such as managing a reduced supplier base and imposing strict vendor controls and attestation requirements, while also ensuring that unauthorized changes to software are detected through established processes.

Organizations must also ensure a consistent and systematic framework and methodology for detecting cyber security incidents, along with a defined process for analysis, prioritization, containment, and response.

Table-top exercises to test response effectiveness combined with regular "red-team" assessments to test the organization's detection and response capabilities can be used to further streamline and enhance capabilities. Internal and external penetration testing are also an effective way to detect vulnerabilities and configuration issues that threat actors use to exploit environments to gain further access.

Training staff on how to spot and report a phishing email, especially those that ask the user to take a particular action, is also an important factor in preventing threat actors from gaining initial access into the environment. Regular phishing simulations are a proven way to test awareness messaging and overall program effectiveness.

Security breaches are inevitable, but with strong security governance practices, along with a defined approach to incident handling combined with preventive measures, organizations can lessen their overall impact.

Sources

[Mandiant] FireEye Mandiant Services. 2019. *M-Trends 2019: FireEye Mandiant Services |Special Report]*. Milpitas: FireEye. https://content.fireeye.com/m-trends