FINANCIAL SERVICES & MARKETS

Sector Overview

Australia is well-positioned as a hub for the Asia-Pacific region and boasts a sophisticated financial services industry (FSI). A compulsory retirement savings program, a highly qualified multilingual workforce, and cutting-edge corporate infrastructure contribute to the financial services industry's success. Australia's financial services strength is largely supported by the expansion of its investment funds industry, with one of the world's largest pools of contestable funds worth an estimated A$1.3 trillion (US$850 billion).

Cyber threats to the FSI in Australia

In Australia, many cyber-attacks each year are targeted at financial, retail, and business services. Targeted attacks on FSIs increased by ~200% in 2022. Threat Actors with motivations to conduct cybercrime campaigns target credit cards, account information, personally identifiable information (PII) and network access to financial institutions to conduct ransomware attacks.

Australians' PII is particularly sought after by cybercriminals who want to make money by selling it, holding it for ransom, or using it in financial schemes and fraud. From a global perspective, financial services organisations are among the most mature in cyber security controls. However, this has been a necessary investment given the lucrative targets they present.

Cybersecurity Challenges

Continuous digital transformation and innovation

As with many industries, financial services organisations are undergoing rapid digital transformation and migrating services to Cloud providers while servicing a hybrid workforce and customer base. Cloud technologies are attractive as they present scalable options to increase data processing, fraud detection and big data analytics capabilities. Hybrid computing through the adoption of Cloud and Software-as-a-Service (SaaS) technologies introduces additional complexity, which, as the adage goes, is the enemy of security. Additional technologies and integrations broaden an organisation's attack surface, which is the exposed systems requiring protection by security controls.

Complex supply chains

FIs have led the way in optimising service delivery by leveraging third-party service providers, which as with complex computing environments, increase the potential attack surface. Third (and fourth/fifth) parties can provide varying business-critical support, and a subset is even likely to be processing organisations' most sensitive data. Dedicated third-party risk management functions provide initial and ongoing assurance; however, regardless of contractual protections, the security of third-party networks is outside the control of FIs and presents an ongoing risk. Fourth parties present an additional layer of potential exposure, whereby FIs have a direct relationship. However, their data could potentially be exposed, as witnessed during the 2020 Accellion FTA attack.

Software Supply chain risks

Threat actors are increasingly focusing on software vendors to infect consumers along the supply chain with malicious malware through updates or downloads that appear to be legitimate. These assaults disrupt software distribution networks, giving threat actors access to the networks of the compromised supplier's clients. One of the most notable attacks in recent years was the SolarWinds supply chain attack. However, the Log4J vulnerability caused equivalent angst as FIs struggled to ascertain their exposure.

Cyber threats in the financial sector

Ransomware

Attacks by ransomware groups may impact an FI's ongoing operations and result in the irreversible loss of sensitive and important data. Ransomware organisations have also increased the scope of their assaults in recent years to focus on the theft of private data. This may lead to regulatory fines for the company and the disclosure of sensitive financial information about bank clients on the dark web. Understanding the potential regulatory impacts that FIs face as the result of a material data breach, ransomware groups are doubling down on sensitive data exfiltration, sometimes not even bothering to encrypt internal systems.

Phishing

Most FIs receive a large number of 'spray and pray' phishing emails, however, campaigns targeted at employees performing specific roles, such as executives, finance or procurement, are also common. Campaign intent varies, however, the payloads generally contain malicious links to malware or copycat login pages for commonly used enterprise services, which aim to harvest employee credentials. FIs customers are also regularly targeted by attackers, with the objective of stealing PII, account/login details and installing Malware to gain access to Internet Banking portals.

Web application attacks

Local File Inclusion, SQL Injection, and Cross-Site Scripting are the three most prevalent online attack types that target financial services. On July 2, 2021, Morgan Stanley, disclosed a data breach caused by zero-day attacks on Accellion's legacy File Transfer Appliance (FTA). A SQL injection vulnerability (CVE-2021-27101) was the main attack vector, allowing an unauthorised attacker to execute remote commands on affected Accellion FTA servers. Attackers gathered customer data for Morgan Stanley by breaking into the Accellion FTA server of a third-party vendor, Guidehouse.

Vulnerability exploitation

Threat Actors can exploit flaws in a computer's software, hardware, or service components to obtain unauthorised access and launch a cyberattack. FIs have complex environments, including many legacy systems that do not use modern authentication protocols and are susceptible to exploitation. Vulnerability Management is an ongoing assurance exercise to identify and patch exposures before attackers identify them. Effective vulnerability

management requires a comprehensive inventory of software used within the FI and threat intelligence to inform the prioritisation of internal teams.

Distributed-Denial-of-Service attacks
Distributed Denial of Service (DDOS) attacks are used by attackers to flood a target resource by overloading it with traffic, as opposed to typical malware that seeks to infect networks or steal information. The threat actors employ commercial toolkits and websites that provide DDoS attacks for hire to create attack traffic from infected computer systems.
Ransom-DDOS was an emergent trend in 2021/22, whereby Threat Actors threatened a massive, distributed denial of service (DDoS) attack unless a ransom was paid. In September 2021, multiple FIs in Australia and New Zealand suffered distributed denial of service attacks, including the New Zealand stock exchange being closed for trading on multiple consecutive days.

Responding to threats against the finance sector in Australia

Most Financial sector entities won't be able to share 'machine to machine' intelligence, so an industry partner is needed as the enabler/facilitator for cyber threat intelligence (CTI) and collective defence via other means. By taking on the role of the trusted advisor/facilitator for the intelligence exchange, an industry organisation would ensure the overall quality of information flowing through its systems and out to the CI members.

'Forewarned is Forearmed', and by joining a trusted cyber community of Critical Infrastructure owners and operators responsible for protecting their finance assets, you can join the movement to share contextual intelligence and proactively approach cyber defence. Cyber threat activity shared into the CI-ISAC ecosystem by one member has the potential to help others across the sector and the broader CI community stop similar attacks before they impact operations.

CI-ISAC, as a not-for-profit, member driven organisation, with a mission to serve its members and in turn their customers by building a trusted community and leveraging the best technology in its intelligence platform, and drawing on resources and resilience through its industry peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

More information on CI-ISACs sovereign intelligence-sharing capability can be found on the official website: https://www.ci-isac.org.au, or by emailing info@ci-isac.org.au.

Published: 17th April 2023