FS-ISAC

Cyber Trends & Threats in Asia Pacific

Guidance for 2022

Overview

As financial services rapidly digitize across the Asia Pacific region and around the world, cybersecurity is now a key business priority. The high-profile supply chain attacks and explosion of ransomware over the last year are not happening in a vacuum. Several fast-moving trends are transforming financial services: a widespread move to the cloud, new fintech players gaining ground on traditional financial institutions, and growing use of cryptocurrencies by institutional and retail investors. This convergence of trends and threats necessitates a reimagining of cybersecurity principles and priorities for an era of constant change and ever-more complex cyber risks.

Asia Pacific faces key regional trends and threats, some of which overlap with the rest of the world. Based on intelligence sharing, member reporting, and ongoing conversations among our member financial institutions in the region as well as open source intelligence (OSINT) and partner data and analysis, FS-ISAC has gleaned the top trends and threats APAC financial institutions are facing and recommends principles firms should adopt now and looking forward into 2022.

Strategic Trends

Accelerating Digitization

Edge security threats are increasing in APAC as financial institutions digitize and move from on-premise managed systems and networks to hybrid models that expand the threat boundaries away from centralized data and network operating models. With the demise of the traditional perimeter due to widespread adoption of digital services as well as remote working brought on by the pandemic, the attack surface will continue to expand, with ever more data being vulnerable to security threats.

Regulation

While the regulatory environment across APAC tends to be less mature than in other regions, it is developing quickly. The Monetary Authority of Singapore and the US Department of the Treasury recently announced an MoU formalizing and strengthening cyber intelligence sharing related to the financial sector, including regulations and guidance, cybersecurity incidents, and threat intelligence. This may lead to further guidance on requirements for sharing by firms on observed threats as well as vulnerability and threat mitigation disclosure across the region.

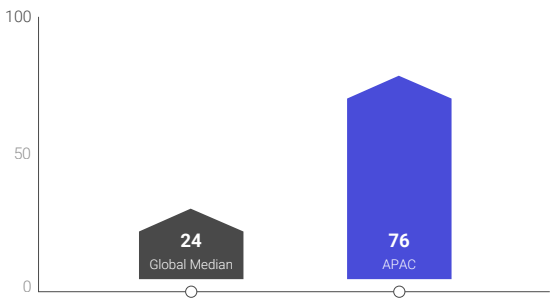
Cybersecurity Talent Shortage

As financial institutions digitize at lightning pace, demand for cybersecurity professionals in APAC continues to outpace supply. With security infrastructure quickly moving to cloud, data science, and machine learning paradigms, cybersecurity teams are competing with many other industries for the same advanced technical skills. The talent shortage is exacerbated by COVID-19, which is restricting the movement of skilled professionals to and around the region, as well as the move by certain countries to preference citizens over foreign nationals to protect local employment.

Organizational Challenges to Threat Response

Many organizations are not built to act and react as quickly as nimble threat actors, but attackers often take advantage of long known patchable issues. One reason they are successful is that many companies are not diligent enough about patching and updating external-facing devices. This seems to be particularly true in APAC. According to FireEye, in 2020 APAC had an average "dwell" time of 76 days when it came to responding to known threats and vulnerabilities. This is three times longer than the global median of 24 days.

Average Dwell Time for Patching Vulnerabilities



Source: FireEye

Key Threats

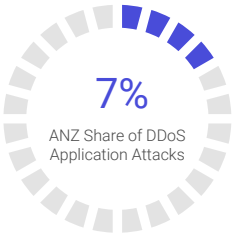
Supply Chain Risk

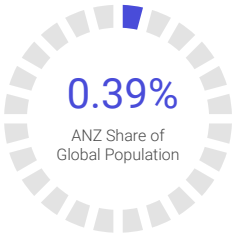
The digitization of financial services was already well underway in APAC but has accelerated with the pandemic. In the race to get new digital services to market fast, most financial firms use third party suppliers to provide software, services, infrastructure, and products to optimize their time to market and operational efficiency.

There is a clear trend of attacks on third party suppliers, especially software vendors, to the financial sector as well as other industries. While financial services firms tend to have robust cybersecurity controls and defenses, third and fourth parties performing critical services for multiple valuable clients will continue to be lucrative targets for threat actors with a variety of motivations. With many firms using the same suppliers, there is an additional challenge of concentration risk, where an attack on one major vendor has the potential to impact a significant number of participants in the financial system, either regionally or globally.

Resurgence of DDOS and new DDOS tactics

Distributed Denial of Service (DDoS) attacks have been on the rise across APAC, especially Australia and New Zealand (ANZ), with the largest ever volumetric attacks occurring in 2021. A troubling development is the increase in application layer attacks, which are more efficient for the attacker and therefore create more damage with less bandwidth. According to Imperva, Australia ranks third and New Zealand sixth in the world's most targeted countries for application layer DDoS. Collectively, ANZ accounted for 7% of application DDoS attacks globally, though it only has .39% of the world's population. More than half a dozen ANZ institutions have been under active DDoS attack by a sophisticated attacker in Q3, with four New Zealand banks having their operations impacted.



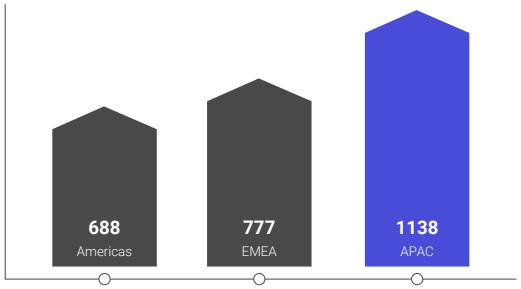


Compared to 2020, DDoS attacks this year have been shorter in duration, which may signal a new tactical threat development. Specifically, shorter durations may indicate that DDoS is a distraction tactic used as part of a wider, multi-vector attack to create noise in an institution's network and infrastructure. This noise makes it harder to detect other incidents that might be taking place; for example, using volumetric attacks as cover for lateral movement or data exfiltration.

Ransomware

In the last year, we have seen large-scale, high-profile ransomware attacks in Asia Pacific, including on large insurers and tech companies. These come on the heels of multiple ransomware attacks around the world, including on IT firm Kaseya as well as Colonial Pipeline and meat supplier JBS in the US. According to Check Point's 2021 mid-year report, the world faced a 93% rise in ransomware attacks this year. Asia Pacific faced the highest number of organizations being attacked weekly (1338), compared to EMEA (777) and the Americas (688). Japan, Singapore, and Indonesia have experienced the sharpest increases in attack activity in APAC so far in 2021.

Average Weekly Ransomware Attacks



Source: Check Point

Ransomware is a growing threat due to the wide availability of ransomware kits (known as Ransomware-as-a-Service) that non-tech savvy criminals can easily obtain, new business models such as auctioning off the stolen data on the dark web, and the rise of cryptocurrencies as cross-border payment methods that are difficult to track. The value of ransoms demanded is also increasing.

Many organizations have mitigated the risk by purchasing cyber insurance which includes coverage for ransom payments,

and therefore may opt to pay ransoms to minimize operational and reputational damage. However, this may not be a viable long-term strategy. Cyber insurers are increasing their premiums, tightening coverage terms, introducing ransomware payout limits, and adding clauses that remove liability for attacks by nation-states. Some insurers are ceasing cyber insurance completely, which could have a knock-on effect on victims' willingness to pay ransoms and, in turn, the revenue of ransomware groups. This has not gone unnoticed by cyber criminals. In fact, one large insurer's APAC subsidiary was a victim of ransomware just days after announcing its cyber insurance policies would no longer cover ransomware payments in another jurisdiction.

Governments around the world and in the region are becoming more vocal about discouraging the payment of ransoms and the possibility of compelling ransomware payment disclosure. Further, many ransomware groups are subject to sanctions by various governments around the world, which could be a challenge for firms operating across multiple geographies.

Resurgence of Trojans

Digitization of financial services has also brought a new wave of trojans, a type of malware that helps criminals gain access to data and systems and install backdoors across banking infrastructure. Remote access trojans allow criminals to access systems from remote locations and are used for many purposes, including espionage. Banking trojans are designed specifically for the purposes of obtaining access credentials or one-time passwords to online bank accounts or to manipulate users and hijack control of live online banking sessions. Both can target individual users as well as firms. Both are on the rise in APAC, with the Philippines being hit especially hard. We expect this trend to continue given the exponential growth of digital payments across the region.

Start 2022 With Stronger Cyber Defenses

Today, financial firms are actively investing in strengthening both third party due diligence and operational resiliency, which is the ability to keep running even in the face of a cybersecurity incident. The following security principles should be part of a robust and systematic protocol for managing cyber risks in this rapidly evolving environment.

01

Protect data

While safeguarding data is critical to protect against all types of cyber threats, it is especially important in defending against ransomware. Savvy ransomware attackers are known to lock up and/or exfiltrate data backups before making ransom demands. Firms should invest in a data vault that is not connected to main systems or backups. By safekeeping critical data offline, firms can not only ensure that disruption and losses are kept to a minimum, but also retain valuable leverage during ransom negotiations.

02

Make sure vulnerabilities are patched quickly

One of the best ways to improve vulnerability management is to build a strong asset management program to understand exactly what devices your institution is using, where they are located, and what versions of software they are using. A robust tracking system allows firms to quickly identify what devices need to be updated and when.

03

Reinforce existing defenses

This includes fortifying endpoints, focusing on email security, upskilling staff to minimize human error and securing networks. Firms must also ensure senior management and boards position cybersecurity as a top priority to secure sufficient investment.

04

Share threat intelligence

No matter how many threat intelligence feeds a firm subscribes to, no one firm can anticipate all cyber threats all the time. Suppliers to the financial sector often serve firms around the world, and ransomware attackers often target victims on multiple continents. Therefore, it is critical to share intelligence on a trusted global platform, as well as in smaller communities that focus on industry verticals and/or regions of operation. Intelligence sharing can not only help firms build pre-emptive defenses against specific attacks but can also help victims understand the modus operandi of attackers, such as whether they are likely to decrypt data upon payment or post the data publicly.

Further, intelligence sharing organizations help ensure that correct and timely information is disseminated quickly to the entire sector, minimizing the potential impact of large-scale attacks on suppliers. In the wake of recent attacks and the media hype surrounding them, SolarWinds, Accellion, and Microsoft all used FS-ISAC as a platform to get the right information about vulnerabilities and mitigation tactics out to the whole sector at once, helping the industry act quickly.

05

Build the muscle memory to respond to attacks

In addition to regular exercises involving all teams that play a role in responding to an incident, firms can use red teaming - simulating attacks to measure how well they are prepared to respond - and threat hunting. The premise behind threat hunting is to assume compromise has already occurred and have a team comb system for what the compromise is. To do this effectively, cyber defense teams should understand the current threat actors targeting the sector and their attack strategies. FS-ISAC produces intelligence reports for security testers that detail attack scenarios that they can use internally to detect the same malicious behaviors.

06

Strengthen third party risk management

Maximize cybersecurity on the firm's side of all interactions with third parties, minimizing the chances that third party vulnerabilities impact systems and data. Systematically review documentation, processes, security protocols, and personnel related to or used by suppliers. Consider employing external risk monitoring services to assist in evaluating the internet-facing risk posture of vendors.

07

Recruit and build diverse teams

In this constantly changing environment, a talent pool with diverse skills is a business imperative. Without a wide variety of different experiences, skillsets and ways of thinking, it will be virtually impossible to stay ahead of nimble and innovative cyber criminals, giving them an unnecessary strategic advantage. With the global and regional shortage of cybersecurity talent, investment in the next generation of cybersecurity professionals, with an emphasis both on diversity and advanced technical skills, is fundamental to safeguarding the industry and society at large.

To learn more about FS-ISAC's work in Asia Pacific, connect with our regional Managing Director Christophe Barel on LinkedIn.

Follow FS-ISAC on LinkedIn and Twitter