By Christophe Barel

Financial institutions must act in concert to defend against threat actors.

READY FOR WHATEVER COMES: MOVING TOWARDS CYBER RESILIENCE

In a rapidly evolving and increasingly fraught cyberthreat landscape, financial institutions are doubling down on cybersecurity, especially amidst rapid digital adoption that has greatly expanded attack surfaces. But with the ubiquity of cyberthreats and growing likelihood of attacks, protecting data is not enough. Financial firms must be able to keep operating even in the face of cyberattacks. They must be cyber resilient.

Cyberthreats are increasingly intertwined with geopolitical conflicts. In the current invasion of Ukraine by Russia, cyberattacks are part of a multipronged approach to modern warfare.

Furthermore, the pandemic has accelerated digitisation, where firms increasingly rely on third-party suppliers of software and infrastructure, vulnerabilities proliferate, and cybercriminal tactics continuously adapt and evolve. In this complex cyberthreat landscape, it is urgent for financial firms to prioritise cyber resilience and preparedness.

Cyber resilience is not only about sustaining operations even while under attack; it is about trust.

In financial services, maintaining customer trust is paramount; we would have no business without it. We are seeing a trend in Asia-Pacific of appointing trust officers to executive leadership roles to oversee privacy, security, and risk management. Cyber resilience is a key focus of their remit.

Furthermore, the pandemic has **ACCELERATED DIGITISATION, WHERE FIRMS INCREASINGLY RELY ON THIRD-PARTY SUPPLIERS OF SOFTWARE AND INFRASTRUCTURE,** vulnerabilities proliferate, and cybercriminal tactics continuously adapt and evolve. In this complex cyberthreat landscape, it is urgent for financial firms to prioritise cyber resilience and preparedness.

BUILDING THE MUSCLE MEMORY TO RESPOND

Just as sports teams study their opponents' strategies and practice defending against them, financial firms increasingly use cyber exercises to test their response capabilities and expose their weaknesses in a simulated environment, so they can strengthen their defences before a real-world attack hits. Exercises occur at firm, sector, and cross-sector levels and practise responding to many different scenarios. The goal is not to predict exactly what might happen, because no attack happens exactly the same way twice. Rather, the objective is to help firms build frameworks for response so the organisation is well-prepared for what may come.

For example, Locked Shields, the world's largest international live-fire cyber exercise run by The North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence, puts countries' cyber defence systems to the test with sophisticated cyberattacks on complex networks that accurately mimic the cross-border nature of today's cyberthreats and the tools, techniques, and procedures of relevant real-world threat actors. Large-scale exercises such as Locked Shields facilitate systematic, cross-border, multi-industry, public-private cyber defence collaboration and information sharing to build cyber resilience globally.

As the only global cyber intelligence sharing community solely focused on financial services, the Financial Services Information Sharing and Analysis Center (FS-ISAC) participates in and runs cyber exercises on a variety of industry sub-verticals such as payments systems and insurance. These exercises not only enhance firms' understanding of their vulnerabilities and help improve incident response plans, but also help firms benchmark their responses against peers to see where their capabilities stack up.

Post-exercise, After Action Reports help spread key learnings and recommendations among participating institutions and beyond. Exercises are therefore part of a virtuous cycle of information sharing that help financial firms increase their cyber resilience and preparedness.

INFORMATION SHARING IS ANOTHER KEY PILLAR OF CYBER RESILIENCE. In today's cyberthreat landscape, no one firm can predict all threats all the time. It is imperative for firms to share not only threat intelligence on new tools, techniques, and procedures being used by cyberthreat actors, but also best practices to defend against them.

DARE TO SHARE

Information sharing is another key pillar of cyber resilience. In today's cyberthreat landscape, no one firm can predict all threats all the time. It is imperative for firms to share not only threat intelligence on new tools, techniques, and procedures being used by cyberthreat actors, but also best practices to defend against them.

Both finance and cyberthreats are inherently cross-border by definition. In our sector, information sharing must happen at a global level so that a threat that begins in one part of the world can be prevented and defended against in another. Further, having a network of peers helps support knowledge building of the threat landscape and known prevention and mitigation measures, which is especially crucial given the global cybersecurity talent shortage. Finally, information sharing on trusted platforms allow well-resourced cybersecurity programmes to share their expertise with less mature ones. This is critical because even attacks on smaller institutions can damage public trust in the larger financial system. Therefore, it is incumbent on the entire sector to help protect and defend all participants.

NEVER TRUST, ALWAYS VERIFY

In a rapidly digitising world where financial firms rely on a wide array of third- and fourth-party suppliers, a zero-trust model helps put in place protocols that ensure constant vigilance. Zero trust means that access to applications and data is denied by default and is only granted through continued multifactor authentication and risk-based verification among users and devices.

Adoption of the zero-trust model has seen a slow start in Asia-Pacific, amid a unique cultural context that is built on trust and consensus as well as a highly competitive business landscape. However, a survey cited in a March 2022 report shows that zero trust is gaining momentum; while only 8% of Asian organisations had adopted a zero-trust strategy, 82% had plans to implement one in the next 12 to 18 months.

NOT IF, WHEN

Since we can no longer assume that it is possible to prevent all cyberattacks, we must therefore develop robust incident response and business continuity plans that help us respond to and recover from attacks as quickly as possible with minimal disruption to business services. Having integrated tools that allow for smooth and efficient incident response throughout the chain of command, from the front line defenders up to the executive level, is increasingly critical to business success.

BOARD-LEVEL PRIORITISATION

Cybersecurity is no longer just a back office cost; it is a critical business risk and must be treated accordingly. To date, many boards have seen the importance of cybersecurity but do not understand it and so give the chief information security officer (CISO) whatever budget is asked for in the hope that money will 'fix it'. That approach will no longer suffice. Regulators are increasingly demanding accountability at the board level; therefore, boards must educate themselves on cyber risks. More and more CISOs will be invited to corporate boards to incorporate the required cyber expertise into board compositions. But CISOs too must understand how to quantify cyber risks in financial terms that boards know how to work with.

If there are lessons to be taken from the Covid-19 pandemic for cyber defence, it is that black swan events – unexpected, outlier events with severe impact – can hit any institution. While mitigation measures are essential, it is crucial not to stop there. Cyber resilience comes with regular participation in cyber exercises, playing an active role in cross-border intelligence sharing, and maintaining well-drilled incident response teams to be able to keep operations running even if faced with cyberattacks. ✱

In a rapidly digitising world where financial firms rely on a wide array of third- and fourth-party suppliers, a zero-trust model helps put in place protocols that ensure constant vigilance. **ZERO TRUST MEANS THAT ACCESS TO APPLICATIONS AND DATA IS DENIED BY DEFAULT** and is only granted through continued multifactor authentication and risk-based verification among users and devices.

■ *Christophe Barel is the Managing Director for Asia-Pacific at FS-ISAC, the only global cyber intelligence sharing community solely focused on financial services. Serving financial institutions and in turn their customers, the organisation leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate and, respond to cyberthreats. Headquartered in the United States, the organisation has offices in the United Kingdom and Singapore, and members in more than 70 countries.*

Prior to joining FS-ISAC, Christophe was Managing Director at data and intelligence provider Acuris Group where he has set up their risk & compliance business for Asia-Pacific, focusing on areas such as AML/KYC screening, cybersecurity and enhanced due diligence. Christophe has been based in Asia for about a decade, starting off in Hong Kong before moving to Singapore in 2015. Previously, he worked for a variety of consulting and tech companies.