HOW TO MANAGE A CYBER SECURITY CRISIS: WHAT MARKET INFRASTRUCTURES CAN LEARN FROM EACH OTHER?

No issue is more topical or more universal than cyber-security, as a panel featuring an admiral, an air traffic controller, a central banker and a financial market infrastructure risk manager indicates. That is because the threat of cyber-breaches, and the costs of defending against them, affect not just the financial services industry, but every sector of every economy. The upside, as Marc Bayle, director general at the European Central Bank (ECB) in charge of market infrastructures, reminded the audience for his panel at Sibos in Toronto[1], is that, in matters of cyber-security, every business can learn from every other business. But how willing are businesses to share ideas, information and intelligence about the management and mitigation of cyber-threats?

"Both in the physical and the cyber domain we are in a pretty dynamic environment right now," warned Michelle Howard[2], an admiral in the United States Navy. "Our potential adversaries in the theatre vary in scope and scale, but what they have in common is that they are all able to rapidly harness technological change to their advantage. It is out there, it is unique, it is contested, [and] it decouples geography from effect."

Following the 2016 Warsaw summit at which NATO leaders declared cyber-space to be an operational domain in its own right, cyber-security is now part of the day-to-day operational responsibilities of military leaders everywhere. As commander of US naval forces in Europe and Africa, and a member of the NATO allied joint command in Naples, Admiral Howard is in a good position to judge the scale and nature of the cyber-threat.

This is a new responsibility for the armed forces, but less culturally unfamiliar to the military mind than the financial. After all, as Admiral Howard pointed out, a state of readiness is a routine condition in the military, from the strategic to the tactical level. She said that, as a commander, she has to understand the readiness of the people and the weapons under her command in the virtual as well as the physical domain, every day and all the time.

"As a commander, I have to be able to understand the readiness of every ship and submarine and aircraft that I have," said Admiral Howard. "On any given day, I should be able to ask, `How much fuel is on that ship? Are the people trained? They should be able to tell me how much food they have and how many days they could stay at sea. The people have to be able to report, and confirm, that all our patches are in place, and our networks are secure, just as we have to be able to say how much fuel is on board the ship. They have to be able to understand they own [the cyber-security] part of their ship, their aircraft, their submarine, just as they own the rest of the readiness - and that, at this level, we are interested in it. It means they are ready to operate."

Banks and financial market infrastructures can learn from military levels of readiness

Private sector companies would benefit from developing a similar culture of readiness among managers and employees. "User-awareness is the biggest bang for your buck in terms of investment," said Vas Rajan, chief information security officer for CLS Bank. "Good behaviour by the population of the organisation can really mitigate a lot of risk."

To create a security-conscious culture, he advocated personalisation. "You can do that in a number of ways," said Rajan. It can be as simple as tying a training exercise to someone's personal life. "One thing I have seen done very effectively is, when trying to train people on email or social media, ask, `What do you tell your children at home about these things?' Then, suddenly, people will listen. Or, when you talk about being careful about phishing, ask, `What would happen to you if this happened to you on your Gmail and it got into your bank account?' Making it personal is one big way to change the mind-set."

Admiral Howard advised working through a response to a potential cyber-threat with all the parties affected well in advance, outside as well as inside the organisation. "You have to force these conversations, so that before you start executing, the team has worked their way through it, and then communicated with all the potential stakeholders," she said. "You have a plan, and you have thresholds, so that you know what you are going to do if something happens."

[1] *How to manage a cyber-security crisis: what market infrastructures can learn from each other*, held on Monday 16 October, Sibos, Toronto 2017

[2] Admiral Michelle Howard retired from the US Navy in November 2017

> **“Both in the physical and the cyber domain we are in a pretty dynamic environment right now. Our potential adversaries in the theatre vary in scope and scale, but what they have in common is that they are all able to rapidly harness technological change to their advantage. It is out there, it is unique, it is contested, [and] it decouples geography from effect.”**
>
> **- Michelle Howard, Admiral,**
> **US Navy**

She pointed out that the Pentagon tests the readiness of its systems to respond effectively to cyber-attacks continuously, by paying hackers to attempt to penetrate them. Assessing the cyber-security readiness of contractors is equally routine, and the military offers advice and support to those who fall short. “Did we incorporate into the process other networks?” asked Admiral Howard. “Are their networks secure? We are all connected. If the guy who provides my supply chain management is not cyber-secure, then I am not cyber-secure in my day-to-day operations.”

Financial institutions are reluctant to share intelligence about cyber-threats

Much the same inter-connectedness is true of the financial services industry, yet similar levels of testing and knowledge-sharing are much less evident. Indeed, Admiral Howard said she was surprised by the relatively low level of readiness to respond to cyber-threats within the financial services industry, and by the suspicion of sharing information to improve security.

Patrick Mana, a project manager at the Eurocontrol air traffic management agency, which is responsible for the safe management of aircraft across 41 countries, thought organisational and budgetary complexities made it hard to match military levels of readiness. He said it was challenging for air traffic managers to build cyber-attack readiness even into core systems (such as radar) because they are ageing, must be readily accessible without complicated security protocols, and require investment by multiple countries if a change is not to disrupt the inter-operability of air traffic control systems.

Marc Bayle, head of the directorate general market infrastructure and payments at the European Central Bank (ECB), thought there was a cultural aspect to the unwillingness to share information. Business leaders, he thought, needed to reassure colleagues that they would not be blamed for cyber-breaches. “It is important that you are seen as a victim and not as an incompetent manager,” he said.

Yet commercial pressures inevitably suppress the willingness to share information about cyber-breaches, in case customers lose confidence or competitors seek to exploit the consequent vulnerability. Vas Rajan recalled that in 2012, when a number of retail banks suffered denial of service attacks, senior bankers communicated via personal email because they did not want to admit that their customers could not withdraw money or pay bills.

The importance of sharing information about cyber-threats

Ali Arasteh, a senior director at Fireeye-Mandiant, which advises companies on the management of cyber-threats and breaches, said information-sharing was vital because most cyber-attacks deploy tools that can be used to penetrate a variety of organisations. Most perpetrators, he said, are interested not in particular firms, but in firms vulnerable enough for them to steal money or secrets. “Campaigns target industries rather than individual organisations,” he said. “There is no significant variability in the attackers’ techniques. So there is a lot of value in sharing intelligence.”

Arasteh added that, although organisations in the financial services industry were now sharing information on cyber-attacks, both manually and in an automated way, there remained several worrying problems. First, few firms appreciate the risk associated with the timing of disclosure of information about a cyber-attack. Sharing of information too early, for example, can prompt a change in attack methodologies, complicating the response.

As it happens, firms are generally too slow to share information. This in turn delays a wider appreciation of changes in the methodologies used by cyber-attackers. “Threat intelligence sharing is viewed as an after-incident action, versus a step in the response,” said Arasteh. “It thereby introduces significant delays in the process. Also, we are finding that legal and privacy implications typically delay the process of sharing.”

Lastly, Arasteh noted that some organisations share information more readily than others, and are disappointed that they do not receive the same value back. “The reality is that members of a network will share intelligence if they perceive that, by contributing to the network, their intelligence is being augmented by other sources,” he said. “We need to reduce the bar, whether technologically or process-wise or resource-wise, so that the less mature, less well-resourced organisations will be able to add value in this sharing process.”

Patrick Mana pointed to a more practical limitation on information-sharing: information overload, making it impossible to discriminate between what matters and what does not.

The information management challenge

“It is like email,” he said. “You can spend your life on email. You can generate an entropy which is huge, just by sending out email. Sharing information can be like that. Now we are starting to subscribe to some sources, and receive a lot of information, sorting it out, assessing which one is relevant to us, is quite resource-consuming. The reality is that we are receiving a lot of information but not much of it is applicable to us.”

Vas Rajan observed that an effective threat management programme nevertheless had to make use of multiple sources of information about cyber-attacks, ranging from the publicly available, through commercial services, to government agencies, and the flood of information could and should be managed effectively. “What is important is to be able to take those various sources of information, and process them in a uniform way, and quickly,” he said. “There is a lot of redundancy in getting information, and also in sharing it out.”

On sharing information with peers and competitors, Rajan had concrete advice. Firms should always know which industry organisations, peers, competitors and government agencies they were willing to share information with, he

> **“User-awareness is the biggest bang for your buck in terms of investment. “Good behaviour by the population of the organisation can really mitigate a lot of risk.”**
>
> **- Vas Rajan, chief information security officer at CLS Bank**

said. “Whether you are willing to share it or not is one thing, but do you have the channels in place to share it securely?” he asked. “Is your response plan such that it includes, for example, your legal department, since it might be privileged and therefore protected? Do you know who you would want to share it with? Do you know how you can share it and avoid liability? One of the biggest things I have seen in my career is reluctance to share based on not wanting to admit something that may come back to haunt you and create liability down the road. That is the reality of the corporate world. Being able to have that planned out, and knowing how you would share it, if you were willing, is really important.”

Mana recognised another facet of the problem. He pointed out that the aviation industry shares information about cyber-threats through the International Civil Aviation Organization (ICAO)— a Montreal-based agency of the United Nations – but its effectiveness is mitigated by an understandable reluctance to share sensitive material with the authorities in some countries. “Do we want to share information with any state in the world?” asked Mana. “I am not going to name any, but I am sure you will have some in mind. We can impose systems at a worldwide level which embed some weaknesses.”

Cross-industry sharing of information is still limited

Rajan said that that financial market infrastructures (such as CLS) have now set up effective information-sharing groups. It was cross-sectoral and cross-industry collaboration that he saw as still relatively immature. “If I got something and it was analysed, and we did real forensics on it, might it target government or air traffic control?” asked Rajan. “I am not necessarily sure how I would get it into [the] hands [of other industries], other than lobbing it over the fence into the government agencies that support us.”

Marc Bayle said that in their 2016 guidance on cyber-resilience for financial market infrastructures (FMIs), the Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organisation of Securities Commissions (IOSCO) had insisted cyber-resilience “cannot be achieved by an FMI alone; it is a collective endeavour of the whole `ecosystem.’”

Rajan agreed that “inter-connectedness is a big theme in the CPMI-IOSCO guidance. A mind-set change that is happening, and needs to continue to happen, is for all of us to think about our organisations and then think of the role of the organisation in the broader eco-system, and look out for each other.”

Mana said that Eurocontrol lacked the systems and procedures to generate cyber-security information for the benefit of others. “To share information, you have first to have something to share, and of course for that you have to have the means to detect when something is going on,” he said. “I can tell you that, in our domain today, we are not at the right level. We do not have a lot of systems to detect what is going on and, more importantly, we do not have the time to analyse the data.” He added that, because control of airspace rests on national sovereignty, there is no natural appetite to share information across national and institutional boundaries anyway.

Sharing information with regulators is of course compulsory, so in theory regulators could compensate for the lack of information sharing in the private sector by pooling it among themselves. Marc Bayle did not rule this out. “There is a possibility in some specific areas,” he said. “At the same time, we have a forum where central banks can exchange information – but with some limitation, legally speaking. Anyway, sharing of information between regulators is not the best way to manage a crisis. We have first to manage the crisis with the actors within the market - the operators of the systems and the participants in the systems is where you need to share information. That is where the emergency is. The regulator comes a bit afterwards.”

Admiral Howard said that government agencies took a different view to this. They have no choice but to share, she said, because they use software and telecommunications infrastructures controlled by private companies, and incidents cannot be managed without sharing information with them. This raises contractual issues, she added, and can raise awkward questions about intellectual property. But Patrick Mana thought these issues were not major barriers to information-sharing. “The vast majority of information can be shared without reporting where it was found,” he said.

Rajan went further, arguing that firms need to share not only information about cyber-threats but details of their cyber-security policies, and even run joint cyber-penetration tests. In his view, all response plans needed to be tested across sectors and industries because, as he put it, all participants are, ultimately, “inter-connected.”

Responses to breaches of cyber-defences need to be tested and adapted

Rajan was also worried that response plans were becoming “academic.” He advised firms to exercise “in a real way.” In his view, that meant working to a plan which encompassed not only technology and operations but the legal department, investor relations, third party contractors, regulators and external board directors.

Rajan advised companies to prepare for ransom-ware attacks, for example, by defining whether the corporate policy is to pay or not to pay and, if it is to pay, working out how to obtain large quantities of crypto-currency within a matter of hours. These policies also need to be tested, he said, for legal and regulatory compliance.

Financial market infrastructures also change over time, added Rajan, so “red team” penetration tests should be repeated regularly. In running them, Rajan also argued that it is essential to define the “crown jewels” of the

How to manage a cyber-security crisis: what market infrastructures can learn from each other

This panel discussion took place on Monday 16 October 2017 at Sibos Toronto

Moderator

Marc Bayle de Jessé
Head of the directorate general market infrastructure and payments, European Central Bank (ECB)

Panelists

Ali Aresteh
Senior director, Freeye-Mandiant

Vas Rajan
Chief information security officer, CLS

Michelle Howard
Admiral, US Navy

Patrick Mana
Project manager, Centralised Services 6-6 & 6-7 (Cyber-security), Eurocontrol

organisation, and charge "red team" simulated attackers with capturing them.

"Let them get closer and closer and closer to the point where you say, `Okay, this is too risky because it is too close to our operational core,'" he said. "To that end, you should make sure that the gloves are off. Let them do what they need to do, so that you can really have that honest test." Culturally, he argued it was important that the sharing of the results be seen within the organisation as a learning exercise, and not a punishment routine.

Ali Arasteh agreed that it made sense for firms to be selective in what they chose to protect. "You cannot – and should not – protect everything at the same level," he said. "You need to understand the risk and the impact. So we always recommend identifying your crown jewels, understanding the risk profile of your crown jewels, and [identifying] who would be going after them. The executives and the business do not necessarily understand that the protection of the crown jewels is the mission of cyber-security, rather than reducing the number of incidents."

Take preparedness seriously

Because a firm cannot protect everything, Arasteh sets two key tests of readiness. First, not whether attackers can break into systems, but whether they can achieve their objectives. That depends, explained Arasteh, on assessing technical and operational vulnerabilities, and then addressing them.

The second key measure of readiness is to test the ability to identify a cyber-attack and respond to it, which means running regular and demanding "red team" simulated attacks. "The fact the `red team' is successful against your organisation is not necessarily a bad thing," said Arasteh. "The question is how well you were able to respond to them, and how well you rate over time against red teams."

Arasteh also cautioned companies to resist the temptation to focus on containing, or remedying, a cyber-attack as soon as it occurs. "From the organisation's perspective, you want to get rid of the attacker as soon as possible" he explained. "It takes a lot of effort on our side to make them understand that we should not implement any kind of remediation or containment actions until we figure out what kind of attacker we are dealing with, and what motivations they have, and what the scope of the incident is. If you do not understand the full scope of the incident, you will not be able to remove them from full access to your network."

View the entire panel discussion **here**.

Editor
Dominic Hobson
dominichobson@dominichobson.com

Head of Market Infrastructures, SWIFT
Juliette Kennel
juliette.kennel@swift.com

Design
Bim Hjortronsteen
bimhjortronsteen@gmail.com

Publisher
SWIFT
Avenue Adèle 1
B-1310 La Hulpe
Tel: +32 2 655 31 11
Fax: +32 2 655 32 26
SWIFT BIC: SWHQ BE BB
http://www.swift.com/

Disclaimer
SWIFT publishes MI Forum Magazine for information purposes only. Any personal views expressed in MI Forum Magazine are the contributors' own and do not necessarily reflect the views of SWIFT or its members.