A WHITE PAPER PRODUCED BY FINEXTRA
IN ASSOCIATION WITH SERVICENOW
FEBRUARY 2019

CYBER SECURITY IN FINANCIAL SERVICES: ORCHESTRATING THE BEST DEFENCE IN AN EVOLVING THREAT LANDSCAPE

servicenow™ | Finextra

01 INTRODUCTION

Data, IT and business security have always been paramount for financial organisations. But in an increasingly digitised world, more data is being produced faster than ever. Financial organisations are encouraged to share customer data while at the same time being expected to safeguard it with progressively stronger measures. Data they are responsible for often resides outside their organisation and can be accessed by a multitude of systems and devices.

Data breaches increase in scale, sophistication and regularity with each passing year as new regulation pushes organisations to improve defences and be more transparent about incidents. Penalties for failure are significant and threefold - direct and indirect cost of attacks and breaches, fines and reputational damage.

In 2018 the World Economic Forum (WEF) surveyed more than 12,000 executives around the world about what they considered to be the biggest risks to doing business, ranging across political, societal and technological concerns. Cyber-attacks were considered the number one risk by executives in Europe and advanced economies.[1]

At Sibos 2018 in Sydney, 79 per cent of a keynote audience of financial professionals said they believed a globally significant cyber terror attack could happen within the next ten years, with a worldwide systematic attack on professional services, including businesses, banking and financial systems, one of the more likely scenarios.

[1] https://www.weforum.org/press/2018/11/from-unemployment-to-growing-cyber-risk-business-executives-in-different-regions-have-different-worries

Financial Services has been, and continues to be, a targeted sector, and cybercrime is becoming sophisticated on an industrial scale. A more strategic and wholesale approach needs to be adopted industry-wide to fend off the threat, particularly as detection and response times are increasing. Of course the challenges this presents are myriad. While external threats are increasing in scope and complexity, organisations face internal challenges in dealing with them. Education to address security weaknesses due to human behaviour is required and transparency is critical. But fixing the manual processes associated with simple IT hygiene such as patch management, and orchestrating and automating across multiple security solutions, processes and teams within the organisation are equally important.

Other factors play into this as well, such as new business models brought about by digitisation and the progression towards an open, interconnected world. Open banking and API-driven ecosystems create vast new opportunities for fraudsters, while also extending significant pressure on organisations to comply with ever-changing regulatory updates. Now more than ever it's time for siloed organisations to leverage technology to get a holistic view of their entire business. IT, security and business teams need to be working together, as interconnectedly as the emerging digital world in which they operate.

> "At Sibos 2018 in Sydney, 79 per cent of a keynote audience of financial professionals said they believed a globally significant cyber terror attack could happen within the next ten years, with a worldwide systematic attack on professional services, including businesses, banking and financial systems, one of the more likely scenarios."

02
INCREASED THREAT AND SECURITY CHALLENGES

FINANCIAL SERVICES IS AMONG THE MOST ATTACKED SECTORS.

The 2018 X-Force Threat[2] Intelligence Index identified the financial services sector as experiencing the highest number of security incidents requiring deeper investigation, globally accounting for 27 per cent of security incidents and 17 per cent of attacks. Similarly, a 2018 report by security company Mandiant said that 24 per cent of its investigations in EMEA[3] involved organisations from the finance sector, which made finance the most targeted sector, ahead of government (18 per cent) and business and professional services (12 per cent).

Phishing attacks, malware, malicious code, insider attacks, and attacks by nation states all pose persistent and deepening threats. Attacks range from those aimed at stealing money from individual customers via their devices, to tactics and technology aimed at exploiting vulnerabilities within organisations. The latter can be for the purpose of mass data theft, use of internal systems and payment infrastructure to steal financial institutions' money, use of IT systems to conduct cryptomining (a recent trend), or outright disruption and sabotage.

INDUSTRIALISATION AND PROLIFERATION OF THREATS

Cyber crime is becoming industrialised. For-profit criminal organisations have specialist roles from leadership down to frontline workers, technical and infrastructure administrators and money handlers. They can pay monthly salaries and offer "career" advancement opportunities. State-sponsored groups are even better resourced.

Just as government agencies and the legitimate private sector have information sharing and detection systems in place to keep up-to-date with emerging threats, criminals, too, share information and tools on dark marketplaces. They also benefit from automation as bots constantly scan for known and new vulnerabilities.

[2] https://www.ibm.com/security/data-breach/threat-intelligence
[3] https://www.securitymea.com/2018/04/09/4258/

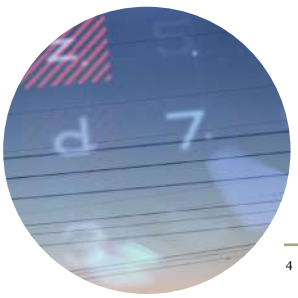
The risks for these criminal enterprises are low, due to their ability to disguise their operations and take advantage of limited global law enforcement cooperation and low-regulation jurisdictions for their infrastructure. The barrier to entry for new groups is also low, as they can leverage easily accessible tools, recruitment channels and "crime-as-a-service" available on the Dark Web.

One group, Carbanak, active since 2013, has hit more than 100 banks worldwide causing total economic damage of US$1.2 billion with an average one-time theft of US$5 million. Although the alleged leader of the group has been detained, it has many members and appears to still be active. There are many other similar groups being tracked by security specialists and law enforcement.[4]

In the face of advancing threats, there are plenty of examples to demonstrate that there are deficiencies in the overall competence and capacity of large companies, including financial services organisations, to currently deal effectively with cybersecurity, with billions of records lost in 2018.[5]

Not all attacks may become public knowledge — some countries don't yet have mandatory data breach notification for customer data, many non-European banks won't have EU citizen customers, and not all bank attacks relate to customer data. Recent reported examples include not only small domestic banks in developing countries, but also tier-one banks and technology partners in major economies.

"Criminals, as well as government agencies and the legitimate private sector, have information and tools, shared on dark marketplaces. They also benefit from automation as bots constantly scan for known and new vulnerabilities."



[4] https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

[5] https://blog.gemalto.com/security/2018/10/09/breached-records-more-than-doubled-in-h1-2018-reveals-breach-level-index/

RECENT CYBER ATTACK EXAMPLES

Stolen data of 20,000 customers from 22 Pakistani banks became available for sale over the Dark Web in November 2018, and the banks had to be notified by an external security vendor. As cyber criminals cashed out at least US$2.6 million from foreign ATMs, the State Bank of India reported days later its surprise that some of the compromised banks still hadn't suspended the use of debit cards internationally.

The Pakistan case followed an attack against Cosmo Bank in India in August, although in that case the money taken was from the bank's operating accounts, not customer accounts. Through compromised card payment infrastructure, which did not have end-to-end encryption, the attackers were able to modify normal fraud and transaction controls and rapidly withdraw a total of about US$11.5 million from ATMs in 28 countries, while at the same time initiating a single US$2 million transfer.

In Canada, Bank of Montreal and online bank Simplii Financial also saw data on 90,000 customers compromised via a simple hacking attack, although in that instance the attacking group — believed to be Russia-based — attempted to hold the data ransom, promising to publish it if not paid US$1 million. The group also detailed the relatively simple methods they were able to use to learn identifying account and social security numbers and reset security questions.

> "The cybersecurity solution market is fragmented. Even with all these technology solutions available in the market and implemented, it is still a combination of insecure practices by customers and staff, and deficiencies in fundamental IT hygiene, that are behind most attacks."

03 MORE STRATEGIC VISION BUT OPERATIONS STILL PIECEMEAL

Following established best practices and frameworks being promoted by governments, regulatory bodies and security experts, organisations are trying to improve their effectiveness at every stage of the cybersecurity cycle. This includes strategies to: identify, protect, detect, respond, report and recover from any kind of attack.

But the cybersecurity solution market is fragmented, with different point solutions addressing particular requirements of the overall lifecycle at varying degrees of effectiveness. Some solutions installed at any given organisation are likely to be outdated, but even with extensive coverage and modern solutions, it is still a challenge to tie it all together operationally and fit within an evolving cybersecurity strategy. Even with effective monitoring, alerts could come from multiple systems at different times, and responsibility for those systems and alerts are often spread across siloed teams responsible for different IT platforms and security operations, as well as regulatory compliance.

Even with all these technology solutions available in the market and implemented, it is still a combination of insecure practices by customers and staff, and deficiencies in fundamental IT hygiene, that are behind most attacks.

IT HYGIENE CAN'T DEPEND ON MANUAL PROCESSES

A 2018 Ponemon Institute survey that included 467 cybersecurity professionals from financial services institutions[6] found that 47 per cent of financial services breach victims said they were breached due to a vulnerability for which a patch was available. This highlights an overwhelming need for more effective vulnerability response, closing down these attack vectors before hackers strike.

[6] https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ar-ponemon-financial-report.pdf

Figure 1: Just some of the categories of software and service solutions available to banks to meet particular cybersecurity requirements

Identify	Protect	Detect	Respond
• Threat intelligence & analysis • Application vulnerability assessment • Security information and event management (SIEM)	• IoT security • Transaction security • Mobile security • Web security • Identity & access management (IAM) • Messaging security • Network firewall • Intrusion prevention systems • Unified threat management (UTM) • Web application firewall (WAF) & application security • Endpoint protection & antivirus • Data security • Cloud security	• Security information and event management (SIEM) • Endpoint detection and response (EDR) • Network monitoring	• Security operations & incident response • Vulnerability response • Endpoint detection and response (EDR)

While financial services professionals recognise the importance of cybersecurity, 74 per cent said they find it difficult to prioritise what needs to be patched first. Furthermore, they struggle to respond in a timely manner because they spend, on average, 12 days or more coordinating patching using manual processes.

The combination of rules-based system solutions complemented by paper-based processes and referrals based on capturing a raft of data through emails, spreadsheets and other manual methods is outdated. This is no longer acceptable.

Without orchestration and automation across existing security tools, it is very difficult to quickly prioritise and respond to the most critical incidents and vulnerabilities. And the longer it takes to detect and remediate a threat, the greater its impact on an institution, its customers and the marketplace.

MEAN TIME TO DETECT IS INCREASING, AS IS COST OF BREACHES

There are a multitude of reasons for delays, but at its core, delay is caused by the inefficiency of traditional, manual processes that are incongruous with the way companies must respond at an enterprise level in the real-time digital environment the world and its fraudsters inhabit.

According to the Ponemon Institute, the mean time to detect an intrusion has grown over the past several years, and for the financial services industry this now stands at 163 days[7], up from 98 days in 2015.[8] The longer it takes to detect a breach, the more the costs add up. Across all industries if the average time to identify a breach (MTTI) was under 100 days, the estimated average total cost of that data breach was US$3.11 million. If the MTTI was over 100 days, the estimated cost was US$4.21 million, representing US$1.1 million additional cost.

> "While financial services professionals recognise the importance of cybersecurity, 74 per cent said they find it difficult to prioritise what needs to be patched first. Furthermore, they struggle to respond in a timely manner because they spend, on average, 12 days or more coordinating patching using manual processes."

[7] https://www.ibm.com/security/data-breach
[8] https://www.businesswire.com/news/home/20150519005417/en/New-Ponemon-Institute-Survey-Reveals-Time-Identify

04
ENVIRONMENTAL CHALLENGES

As the threats become more advanced, and financial institutions struggle to improve their cybersecurity capabilities, a number of other business and environmental trends are complicating matters further.

COMPREHENSIVE DIGITAL TRANSFORMATION ACROSS ALL CHANNELS AND PROCESSES

The World Economic Forum describes the planet as now being ruled by four super forces: mobile technology, internet of things, cloud computing and machine learning/artificial intelligence. In a business context, they are transforming more than just customer-facing interactions — as was the case in the first wave of digitisation enabled by the internet with online banking transactional and information channels.

They are now shaking up long-established industrial structures, breaking down business models and spawning new ones. And, as we become more dependent on IT, there are more business risks in its implementation, and the security function becomes more critical, requiring all parts of the organisation to contribute.

From the attacker's perspective, this increased complexity is an opportunity but also a challenge. The potential rewards for a successful attack are high and the risks are low; therefore, attackers see the sense in making the investment in their own research, professionalism, team building and criminal operating models.

OPEN BANKING AND API BUSINESS MODELS

Open banking is a concept notably being championed in Europe, where it has been enabled by the Payment Services Directive 2 (PSD2). At its heart, the concept is about unbundling the account and customer data and the financial services that have previously been tightly held by banks. Banks must then make the data and services available via API to a wider ecosystem of financial services organisations, particularly in payments.

As connectivity and opening up systems for use by third parties becomes compulsory, the operational architecture that needs to be assessed for

security weaknesses becomes more complex, reaching outside the traditional boundaries of the organisation.

Banks must have an understanding of the security policies and practices of all third parties they deal with. They also need to ensure, when sharing customer data with third parties, that it can't become compromised during transit, storage or use, or they risk losing the consumer trust that is critical for any successful financial institution.

SECURITIES AND MARKET INFRASTRUCTURE ALSO AT RISK

While much of the focus and media attention on cyber risk in financial services considers retail and corporate bank customers and payment infrastructures such as ATMs, card networks and SWIFT, there is growing concern within the industry that the securities market may be next.

The high concentration of high value assets, complexity with many entry points and reliance on centralised critical functions make the custody and securities value chain particularly susceptible to disruption/ransom, asset theft, information theft and/or market manipulation.

Many of the standard approaches to managing the cybersecurity lifecycle are geared towards banking and payments. But, prompted by the output of the International Securities Services Association (ISSA), market infrastructures and securities players are increasingly collaborating beyond their own security arrangements, sharing threat information and tailoring security best practices to meet the needs and address vulnerabilities within their own business operations.

REGULATORY PRESSURE, QUALITY STANDARDS, REPORTING AND ENFORCEMENT

Demonstrating compliance is a headache for all financial institutions, and it is a burden that continues to grow. Government, industry and financial services regulators get involved in cyber security in a number of ways, including promoting best practices and establishing non-binding frameworks and self-assessments, quality inspections and fines, and mandatory reporting of customer data breaches or any significant cyber attack.

The frameworks and guidance can be quite broad, such as the G7 Fundamental Elements of Cyber Security for the Financial Sector, or detailed and specific, such as the US Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool, or the NIST Cybersecurity Workforce Framework.

This kind of non-binding advisory content is helpful to the sector as a whole and to individual organisations, particularly small to medium sized ones that don't have the same experience and resources in cybersecurity as the

global tier one banks. But eventually these suggested frameworks can become minimum operating standards, subject to reporting or inspections and fines.

An example of this can be seen in China's cybersecurity law, passed in 2017, which required IT products used by "critical infrastructure operators," including financial services, to be subject to review. It also dictated that data collected in China, including by multinational banks operating trade finance business in the country, had to be stored locally.

This law was strengthened in 2018 with additional inspection and investigatory powers granted to Public Security Bureaus (PSBs) — China's local and provincial law enforcement.

Singapore passed a similar law in 2018, requiring financial services companies to report any cyber incidents or modifications of system design or security to the Commissioner of Cybersecurity. Lack of compliance can result in fines of up to SGD$100,000 or up to 10 years imprisonment.

The New York Department of Financial Services' (DFS) 23 NYCRR 500 cybersecurity regulation also came into force in 2018. Any business within the banking, insurance and other financial services industry within New York City, or those who provide a service or are on contract as a vendor to these industry firms, have 72 hours in which they must report any cyber incidents that could compromise data including disruptions by ransomware or DDoS attacks. Banks are also required to have a robust cybersecurity plan in place and employ someone who oversees its processes and maintenance, in accordance with the NIST framework.

PRIVACY AND MANDATORY DATA BREACH NOTIFICATION

In 2018 the EU's General Data Protection Regulation (GDPR) regulation attracted much media attention and business awareness due to the scope of the regulation and the sizeable fines for violation. Mandatory notification of data breaches was just one element introduced by GDPR, which also includes stringent rules about access, storage and limitations on use of data.

GDPR is spurring other countries, as well as states within the US, to strengthen existing laws and adopt new regulations to strengthen privacy and cyber security requirements. For example, California has already enacted the first IoT security law in the US, in addition to the California Consumer Privacy Act (CCPA).

Australia introduced its first regulation for mandatory data breach notification at the start of 2018. Other countries in Asia-Pacific with new or updated data privacy laws (either general or financial services specific) include

Japan, Korea, China, Hong Kong, Taiwan, Macau, New Zealand, Malaysia, Philippines and Singapore.

In Canada, there is comprehensive data privacy legislation at both federal and provincial levels, which is deemed to meet EU standards. Meanwhile, in Latin America, consumers have traditionally had the right to access and correct data that companies hold about them. Countries that now have even stronger omnibus data protection legislation include Mexico, Brazil, Argentina and Chile.

PRESSURE TO REPORT QUICKLY COULD LEAD TO ERRORS

As regulators begin to demand timely reporting of breaches and quick response to threats, it is becoming apparent that the current infrastructure at many financial institutions does not enable them to efficiently get full visibility into threats to be able to identify and respond quickly. There is also a risk that new rapid-reporting mandates could lead to could lead to inaccurate or incomplete reporting, as a result of panic and pressure.

RESOURCE CRUNCH

Unfortunately, at the same time organised crime is increasing its capacity and capabilities for attack, and regulators are demanding demonstration of preparedness and increased reporting on all incidents, the financial services sector finds itself fighting for the required talent and resources.

The most recent annual survey of members from the UK's Institute of Information Security Professionals (IISP)[9] highlighted the problem of skills shortages, with the proportion of respondents reporting a dearth of skills as a challenge growing to 18 per cent, up from just 8 per cent in 2015.

Another report from the Information Security Systems Association International (ISSA)[10] and ESG found that IT workers with specialist cyber security skills are approached with a new job offer at least once a week, and 45 per cent of organisations claim to be severely lacking in this specific area.

With the fierce competition for talent, recruitment, retention and internal training efforts need to be concentrated at the high end of security knowledge and analytical capabilities. Strategies for increasing automation of routine manual tasks required for security management, including the use of machine learning, can help free up headcount in security teams to focus on higher value activities.

[9] https://drive.google.com/file/d/1CpmbsvNADZ04sBCXlzGRTkvT0c1-n-ib/view
[10] https://www.esg-global.com/esg-issa-research-report-2017

05

POINTS FOR ACTION – LEVERAGING TECHNOLOGY

An effective cybersecurity strategy needs to be built on a solid foundation. Aside from ongoing education of all staff to minimise people-related security weaknesses, one of the fundamental improvements that can be made is to break down any data and process silos that exist between IT departments, security teams and the directors and officers charged with handling privacy-related incidents and personal data compliance.

The requirement for these business points to be joined up flies way under the radar all too often. Different departments have been built up by different teams with different budgets at different times. Many organisations have let their IT departments drive security decisions, with a lack of input from business heads and a lack of knowledge interpreting the regulation. IT departments have rich information about assets and systems. Security knows where the problems are. Together, they can prioritise the most impactful problems to the financial institution so limited resources are always working on the most important problems first.

In the ideal scenario for improving an organisation's ability to detect and protect itself from attacks, security alerts should be fed from multiple security products onto a single platform, preferably one that is shared with IT.

This sharing should also provide transparency to the directors and officers charged with handling privacy-related incidents and personal data compliance. Particularly when it comes to managing the response to a detected security breach, they need to be the first point of contact. But these directors and officers, and others such as legal and compliance teams and public relations that are responsible for reporting, are not necessarily technical experts, so the format of the security alerts and the business processes around them need to be carefully considered and transparent.

Organisations reviewing their security arrangements to improve efficiency across the security lifecycle should start small but take a common security problem and document (or create) an end-to-end process for how the problem should be solved and then implement it.

For processes that range from identification to detection to protection and response, this would involve both security and IT as each team has a specific role in solving the problem. Once this process is finely tuned, look for portions of this process to potentially automate to help this process run faster.

With less scrambling to keep up with basic IT hygiene such as updates and patches, and the right orchestration and cooperation across silos in place, financial organisations will find it easier to reduce the time it takes to detect and respond to cyber attacks. This will result in lower costs in the event of breaches, better quality regulatory response within the required timeframes, and improved protection against future attacks.

"A 2018 Ponemon Institute survey that included 467 cybersecurity professionals from financial services institutions[6] found that 47 per cent of financial services breach victims said they were breached due to a vulnerability for which a patch was available. There is an overwhelming need for more effective vulnerability response, closing down these attack vectors before hackers strike."

[6] https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ar-ponemon-financial-report.pdf

06 ABOUT

Finextra

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology (fintech) news and information source. Finextra offers over 100,000 fintech news, features and TV content items to visitors to www.finextra.com.

Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra's unique global community consists of over 30,000 fintech professionals working inside banks and financial institutions, specialist fintech application and service providers, consulting organisations and mainstream technology providers. The Finextra community actively participates in posting their opinions and comments on the evolution of fintech. In addition, they contribute information and data to Finextra surveys and reports.

For more information:
Visit www.finextra.com, follow @finextra, contact contact@finextra.com or call +44 (0)20 3100 3670

About ServiceNow

ServiceNow (NYSE: NOW) is making the world of work, work better for people. Our cloud-based platform and solutions deliver digital experiences that help people do their best work. Transform old, manual ways of working into modern digital workflows, so employees and customers get what they need, when they need it- fast, simple, easy.

When people work better, business works better.

For more information, visit:
www.servicenow.com/finserv

Finextra Research Ltd
1 Gresham Street
London
EC2V 7BX
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com