Cybersecurity: Risks and management of risks for global banks and financial institutions

Received (in revised form): 11th December, 2016

Mark Camillo
joined AIG in 2001 and is Head of Cyber, EMEA, having previously led the cyber team for the Americas. He has held positions across the organisation, including the Affinity Group, Accident & Health, Professional Liability and the Fidelity team. Prior to AIG, Mark worked in sales, marketing and product development for Dun & Bradstreet (D&B) and SITEL Corporation. He has an MBA from SUNY Buffalo and a BSc from the University of Wyoming.

Head of Cyber, EMEA, AIG, 58 Fenchurch Street, London, EC3M 4AB, UK
Tel: +44 207 651 6304; E-mail: Mark.Camillo@AIG.com

Abstract The frequency, severity and sophistication of cyberattacks against global financial institutions continues to increase, even though the vast majority of such breaches remain unreported. Financial institutions need to embark on a holistic risk management strategy if they are to combat effectively the renewed threat, ensuring that a tripartite approach that embraces rigorous internal procedures, the adoption of external professional support and the utilisation of appropriate insurance cover is in place. In particular, working in tandem with the insurance market here can play a key role in not just offsetting costs when an event happens at a financial institution, but in preventing an attack in the first place and responding correctly to mitigate when cybersecurity does fail.

Keywords: *cyber risks, cybersecurity, cybercrime, malware, risk management, intelligence*

INTRODUCTION

The threat posed by so-called 'cyberattacks' to global financial institutions, which once may have been viewed as nothing more than media-generated hyperbole, is now undoubtedly being taken very seriously as both the scale and ambition of such attacks continues to escalate.

A recent report by IBM[1] found that thefts against the financial sector using malware or other nefarious means have increased by 80 per cent in 2015 compared to the previous year, while attacks like these represented 38 per cent of reported incidents in 2015 — up from 23 per cent in 2014.

Similarly, a study conducted by the Ponemon Institute and Hewlett Packard Enterprise[2] in 2015 found that in terms of the average cost of cybercrime companies have suffered in any particular industry, financial services topped the global list. Last year, the annual average cost of cybercrime in the financial sector was US$13.5m, followed by the utilities and energy sector (US$12.8m).

Indeed, such is the extent of the cyberthreat in 2016 that every major financial institution is likely to be hit by significant cybercriminal activity this year, according to the latest ThreatMetrix Cybercrime Report.[3]

Analysis of more than 15 billion transactions over a 12 month period by the ThreatMetrix Digital Identity Network revealed a 40 per cent increase in cybercriminal activity targeting the financial sector, with a record 21 million fraud attacks and 45 million bot attacks detected in the last three months of 2015 alone.

The analysis also revealed that the financial sector is facing the highest number of organised attacks and multi-channel threats in 2016, with the biggest

emerging threat for financial institutions being bot attacks, which increased 10 times in the last three months of 2015 compared with the same period in 2014. A worst-case attack scenario could see a major bank or financial institution completely paralysed for days, leading to billions in potential lost revenue.

Unfortunately, according to research by Hewlett Packard, financial institutions top the list when it comes to the cost of cybercrime, with over US$28bn in costs in 2015.

Although the vast majority of cybercrime remains unreported, occasionally some attacks against financial institutions make the headlines. In February 2016, for example, hackers gained access to the Society for Worldwide Interbank (Swift) codes of the Bangladesh central bank and attempted to transfer US$951m from its accounts at the US Federal Reserve — although they were only partially successful, transferring US$81m.

In December 2015, hackers made a similar, unsuccessful attempt to steal more than US$1m from Vietnam's Tien Phong Commercial Joint Stock Bank, while internet security specialist Symantec subsequently reported the discovery of a third case involving similar hacking techniques at an unnamed bank in the Philippines in October 2015.

In the UK, customers were locked out of internet banking for several hours at the start of 2016 after a major bank was targeted by online criminals in a denial of service attack, where a cyberattack overwhelms a website with traffic, taking it offline and is sometimes used as a smokescreen for other attacks. The bank, which has 17 million personal banking and business customers in the UK, said its website had been attacked, but it had successfully defended its systems. Customers were unable to log into their accounts until late in the afternoon. The bank stressed there were no indications of customers' data having been stolen.

In November 2016, another UK bank made the headlines when it was subject to an online attack in which money was apparently stolen from half the customer accounts targeted. The incident is understood to be the first time that such a large number of a bank's customers actually lost money as a result of a single, targeted fraudulent attack.

The bank immediately froze online transactions and has pledged to refund the customers whose current accounts were targeted, in what was one of the largest targeted cyberattacks on a UK bank to date.

THE DARK WEB

Companies want absolute confidentiality when an incident occurs and they do not want it to hit the headlines; however, one of the greatest challenges to financial institutions facing the threat of cybercrime comes from the so-called 'dark web', a network of untraceable online activity and hidden websites. Often, there is a wide range of activity being conducted via the dark web, which targeted companies can be unaware of. In this arena it is possible to post peoples' data as a link, which can then be exploited, with bank account and credit card details available. This is a real headache for many companies, given that the dark web itself is relatively easy to access — once criminals are on there, it is easy for them to disappear as their activities leave very little trace.

It should also be noted that this is a slightly shadowy arena, as financial institutions that have been targeted are often reluctant to let people know how they have found out, which can sometimes be through the monitoring of the dark web. Sometimes criminals will put up a teaser there to say 'we have the data' (which they have discovered) and at other times they will send an e-mail.

At AIG, we see that all sorts of financial institutions can be affected by ransomware, which is where a piece of malware is introduced into a system and starts to encrypt files until a payment or payments are handed over. We are also seeing a surprising amount of mistakes by employees, for example, where they think an e-mail asking for payroll details is from the CEO of the company, where in fact it is from a malicious outside party. Often these sorts of attacks will target someone relatively junior in an organisation.

RISK MANAGEMENT GUIDANCE

It should be emphasised that financial institutions cannot be accused of lagging behind in their management of cybersecurity issues, and — especially when compared to some companies in the

retail sector — are indeed adopting a sophisticated approach. For example, the Central Bank of Ireland (Bhainc Ceannais na hÉireann) recently published guidance on IT risk management and cybersecurity for financial services firms in which it warned that cyber risks are now a key concern.[4] According to the guidance, incidences of cyberattack-related business interruption are increasing and firms should assume they will be successfully targeted. As such, the security and resilience of IT systems, their governance and management must improve to reflect this reality. The Central Bank of Ireland expects boards and senior management of regulated firms to fully recognise their responsibilities for cyber risk issues and to put them among their top priorities; robustly address key issues such as alignment of IT and business strategy, outsourcing risk, change management and cybersecurity. Firms need to make sure that they understand these risks and that they are managed effectively.

In the US, interagency security guidelines[5] implementing sections of the Gramm-Leach-Bliley Act (1999) and the Fair and Accurate Credit Transactions Act (2003) state that financial institutions must develop and maintain an effective information security programme tailored to the complexity of its operations; and require, by contract, service providers that have access to customer information to take appropriate steps to protect the security and confidentiality of this information.

According to the Conference of State Bank Supervisors (CSBS)[6] there are a number of key ways in which banks can take such steps. One is to protect critical information assets by using data encryption tools. Data encryption tools are used to protect sensitive data in transit over communications networks or at rest in storage. It says these tools should be considered a first line of defence from cyberthreats, although banks should be aware that even when encryption is used, there is always the risk that a sophisticated hacker can exploit vulnerabilities in the encryption algorithm or attack underlying processes and protocols.

The CSBS also suggests that if a bank provides a wireless network for customers in physical branches or offices, they should ensure that the public network is separate from the bank's private network and that all connected devices with critical data are connected solely to the private network.

For financial institutions, ensuring that they have the right resources to manage cybersecurity risks is vital; after all, the sophistication of contemporary attacks requires a sophisticated response. As a result, many financial institutions, some of whom effectively used to self-insure with respect to cyberattacks, are increasingly looking to the commercial market and the expertise of underwriters to help them better manage risk.

THE IMPORTANCE OF CYBER INTELLIGENCE

From AIG's perspective, effective risk management is a key part of its overall strategy, as evidenced by the investment made in 2015 in K2 Intelligence, one of the leading players in the assessment and management of cyber risk, enabling clients to respond to cyberthreats with actionable cyber investigations and remediation, as well as helping financial institutions defend themselves through managed detection and response.

According to K2, which works with a range of clients including private and retail banks, international banking institutions, investment funds and sovereign wealth funds, its typical involvement is on the cyber intelligence side — a service offered to AIG policyholders. What this intelligence entails can vary from the monitoring of organised crime to dark web intelligence, or even assessment of Russian-related cybercrime threats. Typically, this is the sort of detailed intelligence and assessment that is of great value to financial institutions, but not the sort of information they would ordinarily have access to.

Indeed, the importance of cyber intelligence cannot be underestimated here as a key tool for effective risk management. Whether through the use of professional external parties or internally, financial institutions much ensure that they know their enemy and are able to obtain as much information as possible about the different types of attack targeting their industry. Banks, insurers, asset managers and suchlike should also ensure that they have effective alert systems in place so that

they know as and when possible cyber breaches are occurring, including log aggregators that are able to work with big data and sophisticated analytics. Such devices can help to minimise threatening probes.

It should be stressed that having a methodology in place to ensure that the focus is on what is important is also crucial, as it can be all too easy to become distracted and miss the most serious threat that is right under your nose.

Equally important is the need not to become overly reliant on technology to do the job for you. Making sure you have the right people is essential, because without the right people who know what to look for and properly assess cybersecurity issues, technology is only ever going to be partially useful. Humans are often the most important link in the cybersecurity chain.

MANAGING CYBERSECURITY THROUGH RISK TRANSFER

Looking more broadly, therefore, as AIG has indicated in its recent Captains of Industry white paper 'Cyber: Joined up?', [7] insurance can play a key role in not just offsetting costs when an event happens at a financial institution, but in preventing an attack in the first place and responding correctly to mitigate when cybersecurity does fail. Put simply, the underwriting process helps different parts of a company unify and focus on what their vulnerabilities are and where they can work together to mitigate them.

The scale and sophistication of cyber insurance products offered to clients is also on the increase. According to analysis by AIG, the global cyber insurance market is growing significantly at around 25–30 per cent per year and has a value of around US$1.5–2bn. Thomas Blunck, head of Special and Financial Risks at (re)insurer Munich Re agrees, noting the cyber (re)insurance market is finally starting to achieve a substantive level of capacity, with programme-specific limits for major clients of up to US$500m now being seen.[8] Blunck adds that he had no doubt that cyber (re)insurance is now a product with a 'long-term growth potential', adding that his company, one of the world's largest (re)insurers, is trying to maintain cyber as a stand-alone cover as this enables better modelling of exposures and more accurate pricing — a practice which is now being seen across the insurance market as cyber insurance reaches maturity.[8]

With increasing maturity comes the prospect that the cyber insurance market could face a significant expansion of the types of coverage possible. At present, cyber (re)insurance tends to relate to loss or theft of data, privacy breach protection, cyber extortion, first or third-party property damage as a consequence of a cyber event and contingent business interruption. We are, however, now seeing the first offerings of product liability, bodily injury and property damage for cyber, as well as reputational damage-related cyber products, relating to loss of profit resulting from reputational damage as a consequence of a cyberattack. In the future, the market could even extend to an organisation's loss of first-party intellectual property, where today such coverage has been limited to third party liability.

What this means is that insurers' view of cybersecurity has changed from being a pure IT risk to one, which has much wider implications for enterprise risk management and one that requires board-level attention.

Fortunately, recent research undertaken by AIG also suggests that senior management, including those at major financial institutions, have a high degree of confidence in such risk management. AIG commissioned Ipsos MORI to investigate attitudes and behaviour as part of its *Captains of Industry* study at the end of 2015.[6] AIG also partnered with Airmic to understand how the board view of our findings fits with the risk manager perspective. According to the findings, 97 per cent of those surveyed believed that the board discusses risk issues as part of any conversation about strategic planning for the company. Nevertheless, as the UK government's *Cyber Governance Health Check Report*[9] also found, over 40 per cent of boards stated they do not have the right skills and knowledge to manage innovation and risk in the digital world.

Indeed, there are still worrying gaps in the risk management landscape of financial institutions that need to be taken seriously if we are to tackle cybersecurity issues effectively. As AIG's *Captains of Industry* survey[6] also indicated, while 82 per cent of senior business

leaders stated they know either a great deal or a fair amount about their company's cybersecurity governance and risk management framework, their cybersecurity policy is not discussed regularly at board meetings.

Perhaps of more concern, only just over a quarter of companies (26 per cent) discussed their cybersecurity policy regularly (defined as always or more often than not), while over half (52 per cent) discussed rarely (ie less often than not or never).

Undoubtedly then, although banks, regulators, legislators and associated bodies in the financial institutions arena are keenly aware of the threat posed by cyberattacks, that threat continues to grow as hackers and associated criminals think of ever more ingenious ways to bypass even the most intelligent security systems. What is required to combat the threat in 2017 and beyond is a full solution which not only embeds cyber risk management at board level, but also a mature conversation with external parties, not least insurers, to ensure the risk is being addressed at the required level of sophistication.

References

1 Schwartz, J. (2016) 'Show me the money: Financial sector a big target for cyberattacks', available at: https://www.mediapro.com/blog/financial-sector-target-cyberattacks/ (accessed November 2016).
2 Ponemon Institute and Hewlett Packard Enterprise (2015) '2015 cost of cyber crime study: United Kingdom', available at: http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf (accessed November 2016).
3 ThreatMetrix (2015) 'ThreatMetrix cybercrime report, Q4 2015', available at: https://www.threatmetrix.com/whitepapers/threatmetrix-cybercrime-report-Q42015-en-us.pdf?_ga=1.105819655.526295316.1479140011 (accessed November 2016).
4 Central Bank of Ireland (2016) 'Cross industry guidance in respect of information technology and cybersecurity risks', available at: https://www.centralbank.ie/publications/Documents/Cross%20Industry%20Guidance%20Information%20Technology%20Cybersecurity%20Risks.pdf (accessed November 2016).
5 Board of Governors of the Federal Reserve System (2013) 'Interagency guidelines establishing information security standards', available at: https://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm (accessed November 2016).
6 Conference of State Bank Supervisors (2015), 'Cybersecurity 101: A resource guide for bank executives', available at: https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf (accessed November 2016).
7 AIG (2015) 'Cyber: Joined up? 2015', Captains of Industry, available at: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/captains-of-industry-cyber-white-paper.pdf (accessed November 2016).
8 Blunck, T., addressing the (2016) 'Monte Carlo Rendez Vous de Septembre', Monte Carlo, Monaco address.
9 HM Government (2016) 'FTSE 350 cyber governance health check', available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521484/Cyber_Governance_Health_Check_report_2015.pdf (accessed November 2016).