# Cybersecurity Regulatory Radar

## Five Top Trends in Cybersecurity Regulation

# Cybersecurity Regulatory Radar

## Five Top Trends in Cybersecurity Regulation

Cyber risk and information security is considered by some to be the biggest challenge organizations collectively face today. A recent study conducted by Juniper Research predicts the cost of data breaches to reach $2.1 trillion globally by 2019. [1] These incidents – whether they are caused by criminals, foreign governments, or hacktivists – can be costly for organizations, distressing for consumers, and create the possibility of real systemic damage to whole industries; even nations. So, it's hardly surprising that regulators and legislators around the world are moving into action.

The statistics are sobering. For example, a new government study in the UK [2] found that just under half (46%) of all UK businesses identified at least one cyber security breach or attack in the last 12 months. The incidence of breaches rises to two-thirds among medium-sized firms (66%) and large firms (68%). Around the globe, big names have been targeted over the past year, including the UK's National Health Service, Lloyds Bank, Tesco, US nuclear power plants, shipping giant A.P. Moller-Maersk, the Polish Financial Supervision Authority and FedEx.

In fact, in a new report by Lloyds of London, [3] an extreme scenario involving a cyber attack on a cloud service provider triggered an average of $53.1bn of economic losses. This is a figure on par with catastrophic natural disasters such as the Japanese earthquake and tsunami of 2011. Even more disturbingly, in the scenario exercise in the July 2017 report, the losses ranged as high as $121.4 billion.

With companies outsourcing a wide variety of activities today, more often than not, the most significant areas of exposure do not sit within the four walls of an organization. Instead, these risks are spread across their extended enterprise – the Ponemon Institute recently estimated that 63% of data breaches can traced to the actions of third parties. [4]

**$2.1 TRILLION**

*predicted cost of data breaches globally in 2019*

**68%**

*of large UK firms have experienced a cyber-security related data breach in the last 12 months*

**63%**

*of data breaches can be traced to the actions of third parties*

**13%**

*of all businesses require suppliers/ third parties to adhere to any cyber standards*

**36%**

*of all businesses rare worried about their supplier/ third party cyber-standards*

Even with these boding statistics, organizations seem to be failing to take action. In the UK government study, only 13% of all businesses said they require suppliers to adhere to any cyber standards – which is about the same level as the study showed in 2016. This is higher in the finance or insurance sectors (30%) and among education, health or social care firms (22%), [5] which probably reflects the regulatory initiatives that are beginning to take hold in those industries.

In the study, even among businesses who indicated that they are specifically worried about the low standard of suppliers' cyber security, only a fifth (19%) set standards for suppliers to follow. This rises to over a third (36%) among large businesses who are worried about supplier standards, but is still a fairly low number. The authors of the study conclude that this "suggests businesses may not recognize the potential they have to set and change supplier behavior by insisting on certain minimum standards – and this could be an effective way of driving up cyber security across supply chains."

The reality is, that while news reports may make cyber attacks seem like Acts of God, most can be traced back to basic human error and bad practice. A 2017 Verizon Data Breach Investigations Report found that nine vulnerabilities accounted for 88% of successful breaches. The report indicated that 1 in 14 users were tricked into following a link or opening an attachment — and a quarter of those respondents clicked on these kinds of emails more than once. Some 80% of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords. [6]

In fact, according to the UK government report, the most common types of breaches involve staff receiving fraudulent emails – in a colossal 72% of cases where firms identified a breach or attack. The second most common breach involved viruses, spyware and malware (33%), people impersonating the organization in emails or online (27%) and ransomware (17%). It's clear from these statistics that employees play a very key role in preventing cyber attacks. [7] So it's little wonder that this fact has become of key importance for regulators.

In the wake of the profusion of attacks that have occurred across a range of organizations in 2016 and 2017, governments are stepping up, through a range of legislative and regulatory initiatives. These are aimed broadly at cyber risk, and in certain industries and jurisdictions, call out the fact that companies need to be managing these across third party relationships as well. The expectation is that the focus on cyber risk in third party relationships will only continue to expand.

## Top 5 trends in cyber security regulation

Overall, the five top trends in cyber security regulation – across organizations and their third parties – are:

1. Focus on getting business continuity right – There is a recognition that no amount of prevention will result in 100% safety from either cyber or information security risks potentially erupting and causing business disruption. Regulators – with an eye firmly on potential systemic risks as well as the safety and soundness of individual financial services organizations, are focusing on business continuity and disaster recovery. In some jurisdictions, such as the US, regulators are looking to enhance standards with more robust testing, especially with third parties.

2. New urgency to reporting cyber attacks – Regulators are either putting event reporting programs in place or beefing up the programs that they already had. An example is the UK's FCA, which launched a new webpage in mid-May that consolidated all of the regulator's pronouncements on cyber risk and explained event reporting procedures. The European Central Bank announced in June 2017 that EU banks will now have to register "major incidents" of cyber attacks with the body. Organizations will need to ensure they have tested protocols in place for identifying and reporting cyber attacks that involve their third parties.

3. "Broken windows" approach to prevention – The UK's FCA says that firms could eliminate up to 80% of the cyber risks that they face if they managed their IT infrastructure in a more effective way, conducting proper patch management and employee training. It advocates programs such as 'Cyber Essentials' or the '10 steps to cyber security'. This is similar to law enforcement approaches that improve crime rates by focusing on addressing low level issues. Organizations will be asked to demonstrate how third parties are implementing or have programs to address these basics.

continued..

Over the course of the remainder of this paper we will explore these themes and how they are evidencing themselves in key jurisdictions around the globe for the financial services industry. This industry – often the focus for cyber incidents – is perhaps the furthest ahead in terms of having a formal regulatory regime. The infrastructure being developed here is expected to be duplicated for other highly-regulated industries, and to become general best practice across all industries – in particular in the way that third parties are being incorporated into all cyber frameworks.

## International Approaches

In June 2016, the Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) published their Guidance on cyber resilience for financial market infrastructures. This document was the first internationally agreed guidance on cyber security for the financial industry.

Originally drafted with clearing, settlement, exchange and other "infrastructure" organizations in mind, the document contained a number of key principles, which have become foundational to how regulators are bolstering their approach to cyber risk in their own jurisdictions, across financial services firms more broadly. These are:

- Sound cyber governance is key. Board and senior management attention is critical to a successful cyber resilience strategy.
- The ability to resume operations quickly and safely after a successful cyber attack is paramount.
- Financial market infrastructures (FMIs) should make use of good-quality threat intelligence and rigorous testing.
- FMIs should aim to instill a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience at every level within the organization.
- Cyber resilience cannot be achieved by an FMI alone; it is a collective endeavor of the whole "ecosystem". [8]

This document emphasized both the need for robust business continuity in the face of cyber threats, as well as the concept that cyber risk management is not a niche discipline performed by the IT department in isolation. Rather, it should form a part of the firm's overall enterprise risk management framework and have governance support at the board of directors' level. Subsequent cyber risk rule-making in the financial services sector supports, and expands upon, these two concepts.

4. Information security is a priority – The EU's GDPR is the most obvious example of how governments and law enforcement are very keen to ensure companies protect their data. But there is no mistake – more regulation around information security is a global trend. Protocols and processes around information security will be fundamental to third party relationships that involve personal data.

5. Cyber and information security are "risks" – Regulators – particularly in financial services – are publicly stating that cyber and information security issues should be part of an organization's enterprise risk management program, with all of the governance and infrastructure that is entailed. For example, the US banking regulators are looking to embed cyber risk into organizations' overall enterprise risk management framework.

## European Union

### Cyber Risk Directive

In legislative and regulatory terms, the EU has been fairly aggressive. The Cyber-Security Directive (also known as the Network and Information Security Directive) [9] was published in the Official Journal of the EU in July 2016. Member States must transpose the Directive into national law by 9 May 2018, and apply their national measures from 10 May 2018.

The Directive creates security and notification requirements for "operators of essential services" – organizations which provide a service which is essential for the maintenance of critical societal and/or economic activities – which include certain banks and financial market infrastructures as well as other industries. A pilot phrase of the cyber incident reporting framework was conducted over 2016. Sabine Lautenschläger, member of the executive Board of the ECB and vice-chair of the Supervisory Board of the ECB, announced in a June 2017 speech that financial institutions will have to report major incidents as of later in the summer. [10]

Overall, her remarks give an interesting insight into the supervisory mindset around cyber risk. Said Lautenschläger, "This [reporting framework] will help us to assess more objectively how many incidents there are and how cyber threats evolve. It will also help us to identify vulnerabilities and common pitfalls." She also announced that regulators would be continuing to perform thematic reviews on cyber security and IT outsourcing. She added, "These reviews help us to assess the risks facing each bank as well as the risks that might affect the entire sector. And they also help to raise awareness of cyber risk at Board level."

Lautenschläger was frank about how the Central Bank and regulators have used insights from cyber risk reviews conducted in 2015 and 2016. "First, they informed a dedicated section in our methodology for on-site inspections," she said. "Second, they were used to create new analytical tools for our off-site supervisors. And third, they were used to produce a cyber risk profile of each bank. So, we are taking a close look at our banks to see whether they are following the relevant standards and best practices. And there are plenty of these; I cannot stress this enough."

The Central Bank and European Banking Authority (EBA) are planning to issue guidance on how EU regulators should supervise cyber risk and IT risks in general, according to Lautenschläger. "What we expect clearly goes beyond basic IT hygiene. This will be an important step for two reasons. First, it will help to forge a common understanding of IT risks between supervisors and banks. And second, it will help to ensure a harmonized treatment. To increase awareness and to communicate our expectations, we will organize seminars and discussions with banks." The first draft of this guidance is expected before the end of 2017.

**GDPR**

The General Data Protection Regulation (GDPR) is another significant piece of EU regulation, focused on improving the way organizations manage cyber risks specifically associated with personal data. The regulation, which will come into effect in May 2018, has the potential for new and aggressive penalties – in this case, 20 million euro or 4% of global annual revenues in the event of misuse or breach.

The new requirements of the GDPR are significant – some build on previous EU requirements while others are new. The UK's Information Commissioner's Office (ICO) has developed a 12-point summary of GDPR requirements, [11] which includes:

- Document personal information the organization holds, potentially through an information audit.
- Review current privacy notices and update for the GDPR's new requirements.
- Look at how the organization harvests, retains, and disposes of personal data. The GDPR has a range of new requirements around these activities.
- Ensure that the organization has the right data breach notification procedures in place, including a new 72-hour notification requirement.
- Examine if and how your organization needs to implement "privacy by design" in its products, and perform Data Protection Impact Assessments.
- Appoint a Data Protection Officer, if you are required to.

National regulators across the EU, as well as the Article 29 EU Working Party, will be producing guidance over the next few months for firms to use when they are implementing these requirements, according to Rob Luke, deputy commissioner for policy at the ICO, in a May 2017 speech in London.

For example, the ICO recently updated a paper on big data, artificial intelligence, machine learning and data protection. [12] The UK regulator also recently published a consultation paper on profiling under GDPR. [13] Responses will be fed into the European Article 29 Working Party.

The GDPR's data security rules will also apply to the third parties that organizations work with – this is particularly true in highly regulated industries, where there is likely to be supervisory focus on this issue. So it is important for organizations to thoroughly assess the impact the GDPR will have on their own governance structure and processes, and to ensure third parties are doing the same.

## United Kingdom

The UK has a significant number of legislative and regulatory irons in the fire when it comes to cyber risk. A flurry of recent speeches and activities followed the widely-reported cyber event that shut down portions of the National Health Service for several days, in May 2017.

For example, the Bank of England's Charlotte Gerken, director, supervisory risk specialists, gave a speech in mid-June 2017 in which she noted that cyber risk has a number of features that make it distinct from other operational risks banks face:

- It is an activity undertaken by individuals, groups, and sometimes states. It is not a natural or error based risk. There is a human protagonist.
- The threat is adaptive. Attackers adapt, adjust and scale their activities to discover what works.
- Detection and identifying the attacker is complex. It is often hard to detect that an operation is under attack and it can be difficult to trace the source.
- Recovery may be threatened. The Bank of England's standard approach to business continuity involves operating with common systems environments between primary and secondary sites, mirroring data between the two. This could, in the face of a successful cyber-attack, be vulnerable to complete loss of applications or destruction or corruption of data.

She also, in the same speech, placed cyber risk firmly in the regulator's overall "operational resiliency" framework, and said that the firms that did well in testing of systemically important firms for cyber risk (called CBEST testing) had strong defences as well as strong detection, response and recovery capabilities. She said these firms understood the need to approach resilience as a people, process and technology issue – echoing the definition of "operational risk". [14]

The Bank of England's Financial Policy Committee outlined a range of initiatives in June 2017 that it will be taking in the months ahead, including:

- Considering the financial system's tolerance for the disruption to important economic functions provided by financial services firms. Supervisors are then planning to issue cyber guidance for firms consistent with this tolerance.
- Initiating regular testing of firms' cyber resilience. This will build on the first round of CBEST testing and ensure the most systemic firms are subject to regular checks. The frequency and scope of checks are to be determined. Regulators will also conduct sector-wide simulation exercises – next year, the Bank of England will run another sector-wide exercise, similar in scope and scale to last year's SIMEX16 sector-wide exercise.
- Looking specifically at third party providers of goods and services to the financial sector, to understand their vulnerability to cyber attack. Regulators will have to provide updates to the Financial Policy Committee on the cyber resilience of key third parties.
- Putting "clear and tested arrangements" in place to respond to cyber attacks, coordinated by the UK government and regulators. These arrangements will be regularly tested, reviewed, and updated. [15]

The Bank of England's Prudential Regulatory Authority is also taking a range of steps – it finalized its new Senior Managers Regime in May 2017, which includes the definition of the Chief Operations senior management function, covering 'responsibility for managing the internal operations and technology of a firm'. Essentially, this means the buck stops with the COO in financial services firms for cyber risk.

The Financial Conduct Authority – another banking regulator that focuses on conduct and culture issues – is also stepping up a gear. The regulator launched a new website page shortly after the NHS cyber attack, which gathers together various FCA resources and underscores the need for financial institutions to report attacks. [16]

The regulator's staff has also been giving speeches recently on the topic, including one in late April 2017 by Nausicaa Delfas, executive director. In her remarks, she noted several key areas of focus that the FCA wanted firms to address, including:

- Getting the basics right: This includes implementing the 10 steps to cyber security, which if properly implemented, could eliminate around 80% of the cyber threats.
- Considering specific cyber risks: Financial institutions should carry out robust and comprehensive risk assessments focused on the impact of a DDoS attack on their systems.
- Avoid concentration risk with third parties: Consider concentration risk when subscribing to a given service, to avoid contamination in the event of widespread sector attacks. Due diligence of third party suppliers should include a review of their cyber resilience. Firms should have controls in place to swiftly recognize when an attack has happened in a third party supplier and have plans in place to correct or reduce undesirable outcomes.
- Rethink employee cyber training: Firms need to stop using a staff "policy" as the sole baseline for security training. Policy is important, but for employees it can be a corporate document that is easily disregarded. Training should empower staff to make secure decisions themselves.
- Begin tracking metrics: Consider ways to capture KRIs and KPIs for cyber risks and the mitigation strategies the firm puts in place. Regularly report the metrics to senior management and the board.
- Share threat information: Within financial services, many banks are already doing this, either through industry associations or through their regulatory body. However, other industries should also find ways of sharing this crucial information.

The approach the FCA and Bank of England are taking to cyber risk is very much along the same pathway that the UK's new National Cyber Security Centre is taking. [17] Launched in February 2017, the website contains a large number of guidance documents aimed at companies generally and also specific sectors.

## United States

Regulators are updating rules here, too. In October 2016, the US banking regulators issued an advance notice of proposed rule-making on new cyber risk standards for institutions with $50 billion or more in assets, as well as the third parties that worked with them. Comments were due back in February 2017, and a further release from the regulators is expected before the end of 2017. [18]

The thoughts the regulators had on cyber risk management fell into five categories:

- Cyber risk governance: Organizations would need to develop and maintain a formal cyber risk management strategy, as well as a supporting framework of policies and procedures to implement the strategy, that is integrated into the overall strategic plans and risk governance structures of the organization.
- Cyber risk management: Firms would have to implement a "three lines of defense" approach to cyber risk management. This would include giving the business lines specific responsibilities for managing cyber risks, making cyber risk part of an overall, independent enterprise risk management infrastructure, and requiring the internal audit function to explicitly evaluate the organization's approach to cyber risk.
- Internal dependency management: Organizations would have to ensure they have effective capabilities in place to identify and manage cyber risks associated with their business assets – including their workforce, data, technology, and facilities – throughout their lifespans. A specific internal dependency strategy would be required, and adequate controls would need to be put in place. Firms would also need to maintain an inventory of all their business assets, prioritized according to the assets' criticality to the business functions they support, the firm's mission and the financial sector.
- External dependency management: This includes outside vendors, suppliers, customers, utilities, and other third parties that organizations depend on to deliver services, as well as the information flows and interconnections between the entity and those external parties. This also includes the management of interconnection risks associated with non-critical external parties that maintain trusted connections to important systems. The proposed requirements are similar to those for the internal dependency management section, and include being able to monitor all relevant external dependencies and trusted connections in real time.
- Incident response, cyber resilience, and situational awareness: Firms would be required to establish and maintain effective incident response and cyber resilience governance, strategies, and capacities so that they could anticipate, withstand, contain, and rapidly recover from a disruption caused by a significant cyber event. Specifically, it would require firms to implement FFIEC IT Examination Handbook, Business Continuity Planning, Appendix J. [19] The ANPR is looking at adding specific cyber elements to these requirements around issues like preservation of critical records, transition plans, and testing. There is also a substantial intelligence requirement being considered – firms would be required to have threat profiles for identified threats to the firm, threat modeling capabilities, and to gather actionable cyber threat intelligence and perform security analytics on an ongoing basis. Firms would also need to perform ongoing vulnerability management.

There are a range of other cyber-related activities taking place in the US as well. In June 2015, the FFIEC issued the Cybersecurity Assessment Tool for financial services firms to use to help assess their cyber risks and determine their cybersecurity preparedness. The body also issues threat information and other information for firms. [20]

More broadly, the NIST Cybersecurity Framework (CSF) – a voluntary framework for managing cybersecurity risk – can be customized by different business sectors and individual organizations. [21] Originally published in February 2014, a draft update was circulated in January 2017. Materials from a May 2017 workshop can also be found on the website.

Even the White House is involved in cyber risk – it issued a US Presidential Executive Order in May 2017 designed to ensure government entities – and key industries – improved their cyber resilience. [22]

The US approach to cyber risk – particularly in the financial services sector – is more rules-based than the European approach, but this is a very traditional difference in regulatory style between the two jurisdictions. However, the general direction in both regions is the same, and there is little doubt that the focus both have on the impact that third parties have on cyber risk will only continue to grow.

## Summary

Cyber risk for all types of organizations – but especially systemically important ones such as financial services firms – has become so great that governments and regulators are in the process of preparing and implementing a wide range of new rules.

These new rules have a significant third party emphasis – both directly and indirectly. The need to implement frameworks and processes that encompass third parties is both explicitly stated and strongly implied throughout most of the new rules and regulations being issued.

Organizations – no matter their industry – need to consider their third party relationships as an inherent component of their overall approach to managing cyber risk. If they do not, there is the risk the organization will one day become just another headline casualty in the ongoing cyber warfare that is raging around the globe today.

## References

[1].https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
[2].https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf
[3].https://www.lloyds.com/news-and-insight/risk-insight/library/technology/countingthecost
[4].https://www.ponemon.org/local/upload/file/Data%20Risk%20in%20the%20Third%20Party%20Ecosystem_BuckleySandler%20LLP%20and%20Treliant%20Risk%20Advisors%20LLC%20Ponemon%20Research%202016%20-%20FINAL2.pdf
[5].https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf
[6].http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/#report
[7].https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf
[8]. http://www.bis.org/cpmi/publ/d146.pdf
[9]. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG
[10].http://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp170619.en.html
[11].https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
[12].https://iconewsblog.wordpress.com/2017/03/03/ai-machine-learning-and-personal-data/
[13].https://iconewsblog.wordpress.com/2017/04/06/profiling-under-the-gdpr-feedback-request/
[14].http://www.bankofengland.co.uk/publications/Documents/speeches/2017/speech979.pdf
[15].http://www.bankofengland.co.uk/publications/Documents/fsr/2017/fsrjun17.pdf
[16].https://www.fca.org.uk/firms/cyber-resilience
[17].https://www.ncsc.gov.uk
[18].https://www.occ.gov/news-issuances/news-releases/2016/nr-ia-2016-131a.pdf
[19].https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx
[20].https://www.ffiec.gov/cybersecurity.htm
[21].https://www.nist.gov/cyberframework
[22].https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

First Published August 2017

ARAVO

## The Definition of Better Business

Better business is built on acting with integrity. It commands better performance, delivering better efficiency, collaboration, and financial outcomes. It inspires trust. But better business is more than that – it's about lifting the ethical standard of an entire business ecosystem to build a better world.

## Contact

For more information:

visit us at aravo.com

email us at info@aravo.com

call us at +1.415.835.7600 [US]