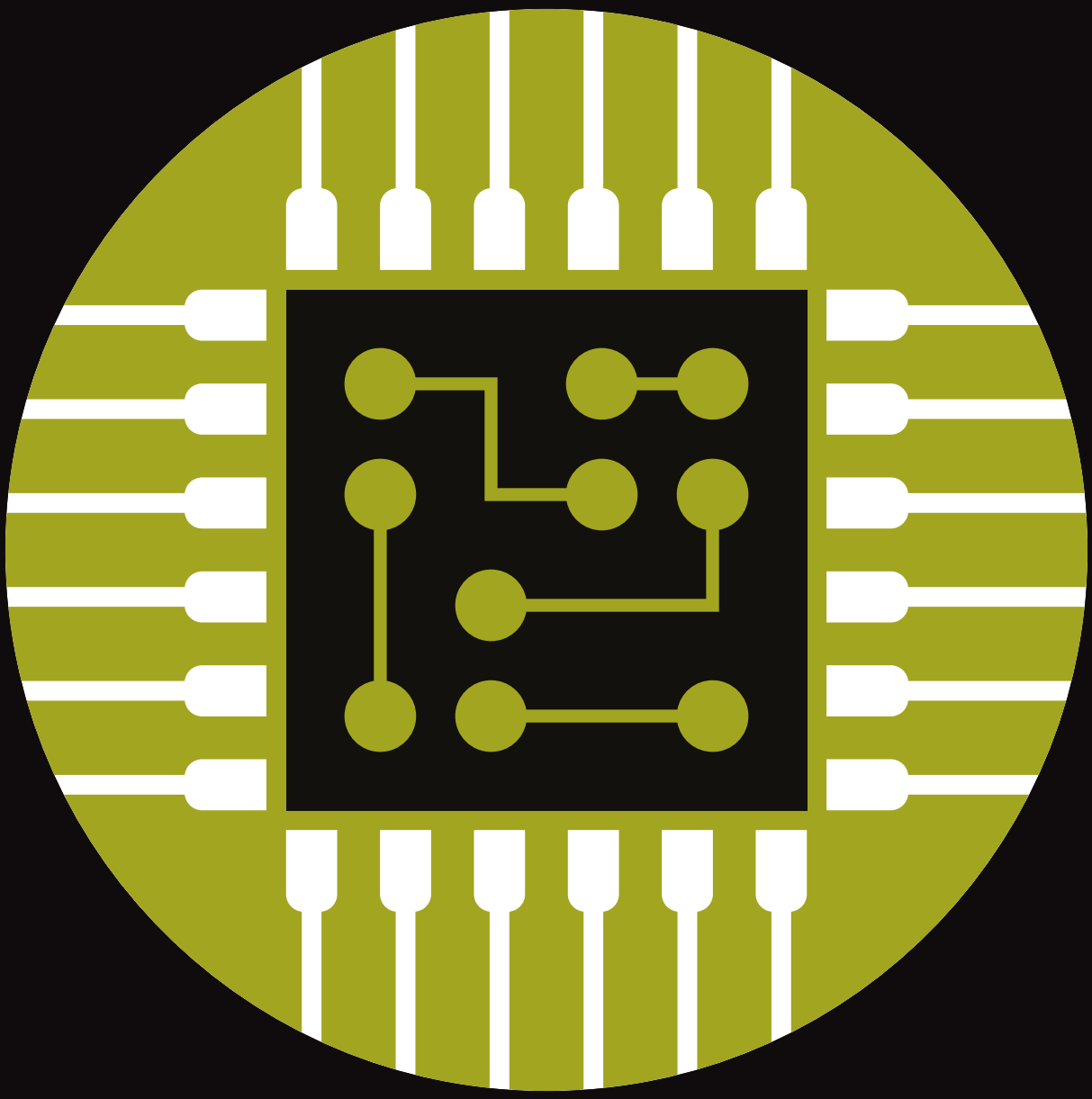
Deloitte.



Cyber risk and regulation in Europe

A new paradigm for banks

CENTRE *for*
REGULATORY
STRATEGY
EMEA

Contents

Introduction

Building resilience to cyber risk in financial services is a rapidly growing priority for all stakeholders. Although banks are doing a great deal to improve their ability to handle cyber threats, regulators are becoming increasingly active as well. Jerome Powell, who became Chairman of the US Federal Reserve in February, identified the cyber threat as 'maybe the single most important' risk to financial services today.[i]

72% of the Financial Stability Board's (FSB's) members[1] have indicated that they intend to release new standards or supervisory initiatives on financial services cyber security this year.[ii] In doing so, regulators are clearly signalling that they see a need to be involved in shaping cyber resilience for the sector.

As regulators get to grips with the nature and complexity of cyber threats, their approach to identifying unacceptable risks and desired responses by banks will become more sophisticated. Banks should expect to feel a growing level of scrutiny of how they deal with cyber risk and greater pressure to demonstrate that they are addressing emerging regulatory concerns in a timely way. Even though this is an area that banks are investing heavily in, the growing interest of regulators could mean that banks will have to modify their activities to suit the different priorities or pace authorities set.

Regulators face the challenge of operating in an almost entirely new and technologically complex environment. The regulatory framework, therefore, in most jurisdictions, is constantly evolving. Among the work already underway, three considerations stand out as key going forward:

1. **Bank stability:** regulators are increasingly concerned about the overall stability implications of a successful major cyber attack targeting a bank. Consumer data protection will remain an important focus, but cyber risk threatening the ability of a bank to continue to provide critical functions will lead regulators to broaden the scope of threats and vulnerabilities that they examine.

2. **System-wide risks:** as cyber risks begin to pose a greater danger to bank stability, the risk of contagion to other banks and financial services firms is also gaining more attention. Crucially this has also led regulators to focus on threats arising from links with financial market infrastructures (FMIs) and third party service providers.

3. **A greater ambition for resilience:** leading jurisdictions are now moving towards putting in place a regulatory and supervisory framework with baseline standards that will challenge banks to be more ambitious in pursuing their cyber defences and resilience.

Banks in the Eurozone should pay particular attention to the approach taken by the European Central Bank (ECB) within the Single Supervisory Mechanism (SSM). The case study on page 5 details how, since its inception in 2014, the ECB has increased its capabilities in cyber and IT risk supervision, and laid the groundwork for a more active approach in the future.

As regulators further develop their framework for strengthening cyber resilience, we see a number of cross-cutting challenges that they must address in order to ensure that new standards and expectations can be effectively applied. Two of the most pressing challenges are: how to codify standards for cyber resilience that can **keep pace with the rapid evolution of technology and cyber risks**; and whether regulators should develop **internationally consistent rules** for banks that have significant operations spread across multiple jurisdictions. We examine both of these issues.

The development of regulatory practices will have to progress quickly in light of the rapid pace of technological change, the mass digitisation of banking activities and the proliferation of new types of cyber threats. It is therefore crucial that senior risk and information officers as well as Boards get an early handle on how the regulatory framework is evolving and what expectations supervisors are developing for them. The final section of this paper explores a number of steps banks can take to get ahead of the game, including engaging early with regulators, focusing on accountability and talent, and taking stock of the cross-border rulemaking environment, among others. Taking steps such as these will help banks better embed emerging regulatory expectations as fully as possible into existing programmes.

1. FSB members include financial regulatory bodies from all G20 jurisdictions (19 member countries and the European Union), plus those from Hong Kong, the Netherlands, Singapore, Spain and Switzerland

What have regulators already done?

Regulatory activity to monitor and shape the cyber resilience of banks and other critical financial services firms is gathering pace, with the past twelve months seeing new initiatives from a number of authorities. The FSB indicates that all of its 25 jurisdictions report having at least one regulatory or supervisory initiative relating to the cyber resilience of financial firms (with some reporting as many as ten). Overall, the FSB counts 56 regulations or standards targeted at cyber security in the financial sector, and 35 publicly communicated supervisory practices (see Figures A and B for a breakdown of the areas of focus).

Further, significant work is expected in the near term as several pilot initiatives are transformed into routine supervisory programmes and expanded to cover a greater number of firms and areas of analysis.

Jurisdictions that demonstrate regulatory good practice in cyber resilience are likely to be copied by other jurisdictions seeking solutions that are demonstrably working. In this respect, taking stock of what has already happened is instructive in determining what the banking sector can expect to see next.

Three areas of regulatory focus for cyber resilience

Cyber risk identification: regulators are increasingly focused on the ability of a bank to understand and map its exposure to cyber risk. This includes risks arising from exposures to financial and non-financial third parties. The European Banking Authority's (EBA's) 2017 Guidelines on assessing Information and Communications Technology (ICT) risk in banks [iii] highlight the importance for supervisors of assessing the efficacy of a bank's ICT risk management framework, and also raise the question of what role additional (Pillar 2) capital could play if applied for deficiencies found in the management of cyber risk. The broader challenges a bank faces in terms of the coherence of its internal control framework are relevant here as well, especially with the growing focus on internal cyber controls between the different divisions and geographies of a group. Breach reporting rules under the EU's General Data Protection Regulation (GDPR)[2] add further impetus for banks to strengthen their ability to detect hacks and data breaches rapidly. Ultimately, being able to translate a strong understanding of cyber risk exposure into an accurate quantitative measurement – a nascent capability for much of the industry – may become a key expectation, and point of discussion between banks and their supervisors. More quantitative and interpretable management information can support the strategic decision-making of firms when considering their cyber risk exposure, particularly in enabling Board members and other non-IT-experts to engage with setting and effectively delivering against an institutional risk appetite for cyber threats.

Cyber risk governance: scrutiny of governance is growing. There is strong pressure from supervisors in most jurisdictions to avoid making cyber a siloed 'IT concern' and to take a whole-of-bank approach to minimising and responding to cyber risk. That, however, still leaves unresolved the question of where ultimate responsibility should sit between Risk, IT, and other functions. Developments, including the UK regulators' creation of a cyber risk function under the Senior Managers Regime – the Chief Operations function, with responsibility for managing all or substantially all the internal operations or technology of the firm or of a part of the firm – along with similar initiatives in other FSB jurisdictions point to a trend towards clear and focused lines of accountability for cyber resilience within a firm. Boards are also facing increasing pressure to demonstrate their ability to understand cyber risks and to take a larger role in setting risk appetite for cyber threats. While some firms have taken the route of appointing a Non-Executive Director with cyber risk experience to their Boards, many jurisdictions have indicated that it is sufficient to demonstrate that the Board has access to expert advice (with a number of firms creating a cyber advisory panel) that allows it to provide effective challenge on cyber risk issues.

Cyber risk resilience: significant progress has been made on developing a supervisory toolkit for testing the cyber resilience of individual institutions. In the UK, the CBEST framework and industry-wide initiatives such as the SIMEX 16 exercise that simulated an outage of the UK's Real-Time-Gross-Settlement payments system [iv], have set a model for cooperation between banks and supervisors in testing the resilience of individual institutions and the sector as a whole. These initiatives have laid the groundwork for measures being adopted in other jurisdictions, to increase scrutiny of the response plans and procedures that firms have in place. Consideration of the continuity of critical systems is a natural outgrowth of this. In 2016, IOSCO-CPMI published Guidance on Cyber Resilience for Financial Market Infrastructures [v] that recommended setting a two-hour downtime window for critical systems brought offline by cyber breaches. In the same year, US Federal banking regulators published an Advanced Notice of Proposed Rulemaking [vi] that suggested adopting this same standard for critical systems in significant banks (the New York Department for Financial Services' 2017 cyber rule, however, only required firms to develop an incident response plan that can demonstrate a prompt recovery, without specifying what is meant by 'prompt').[vii]

As regulators get to grips with the nature and complexity of cyber threats, their approach to identifying unacceptable risks and desired responses by banks will become more sophisticated.

2. From May 2018 the EU's GDPR requires firms to report data breaches to their data protection authorities within 72 hours of becoming aware of the breach. The GDPR allows regulators to fine firms which fail to meet these standards up to 20 million EUR or 4% of global turnover for the preceding financial year (whichever is the highest) (source: European Commission, General Data Protection Regulation)

Focus of regulatory initiatives on cyber

Figure A. Issues dealt with in the 56 existing regulations and guidance schemes targetted at FS cyber security issued by FSB members

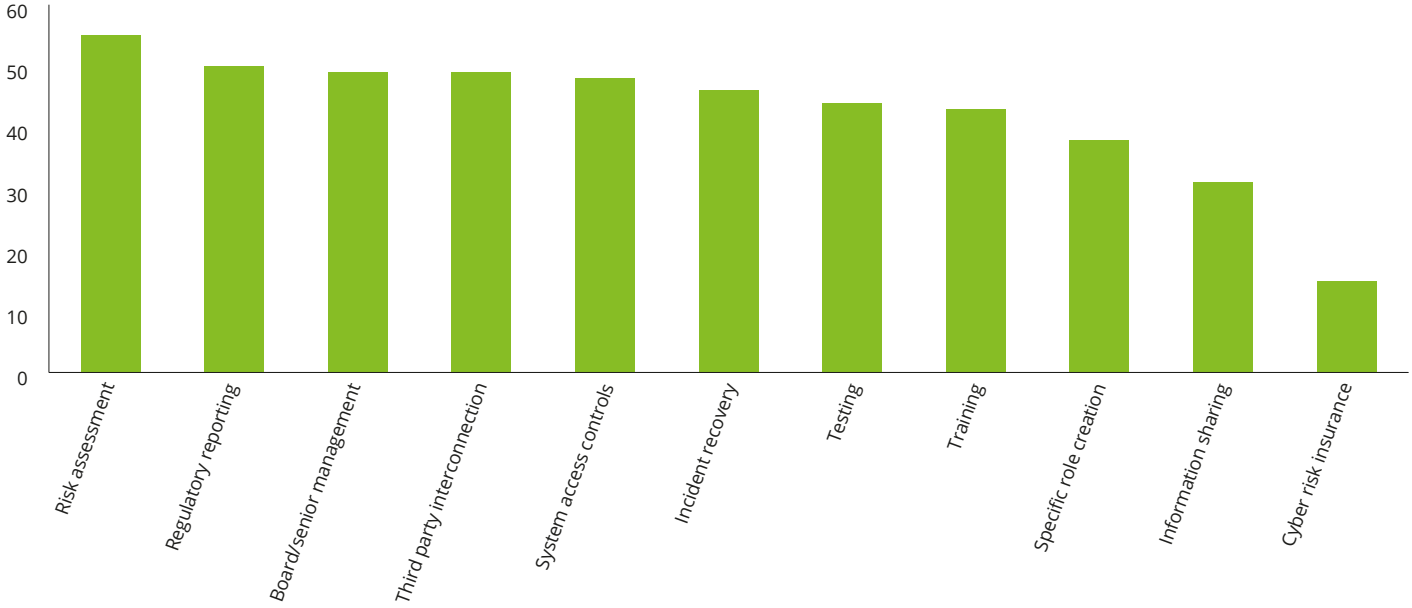
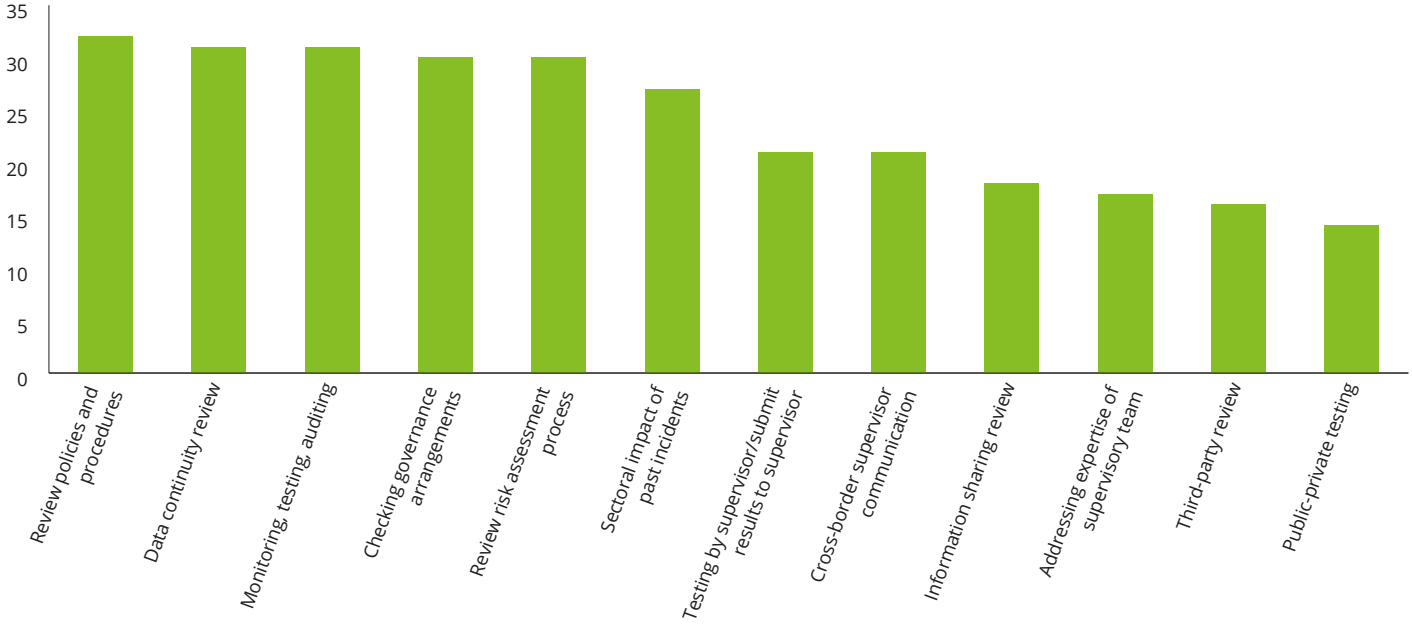


Figure B. Activities included in the 35 reported supervisory practices by FSB members targetted at FS cyber security



Source: Financial Stability Board

Selected cyber resilience regulatory initiatives across the EU and its Member States

European Union

- **Network Information Security Directive:** requiring national cyber resilience plans for critical sectors
- **EBA ICT guidelines:** supervisory operational risk assessment potentially affecting Pillar 2 requirements
- **EBA governance guidelines:** covering IT and outsourcing risks, and business continuity planning
- **GDPR:** data breach reporting requirements and associated fines for non-compliance
- **ECB:** growing supervisory interest, including incident reporting for banks and resilience testing for FMIs

United Kingdom

Financial Policy Committee: commitment to releasing 'clear baseline expectations' for cyber resilience of core firms

CBEST testing: Bank of England-led cyber resilience tests for 35 core firms

Senior Managers Regime: 'Chief Operations' function responsible for cyber and IT risks

Financial Conduct Authority (FCA) guidance on cloud computing: including expected controls around outsourcing

France

Autorité de Contrôle Prudentiel et de Résolution (ACPR): cyber-security self-assessment questionnaire for Less Significant Institutions

ACPR Guidance on Cloud Computing: expectation for risk management and senior management oversight

Spain

National Centre for Protection of Infrastructure and Cyber Security: expectations for the assessment of operational risk by critical firms

Italy

Bank of Italy (BoI) retail payment systems regulation: risk governance and analysis in IT management

BoI cybersecurity guidance: incident handling and reporting, outsourcing risk management

BoI/Commissione Nazionale per le Società e la Borsa (CONSOB) regulation of trading venues, banks, and investment firms: IT internal audit, business continuity and recovery plans

The Netherlands

TIBER: 'red team' scenario testing for the cyber resilience of critical firms

Germany

IT Security Act: measures to prevent breaches

Federal Financial Supervisory Authority (BaFIN)/ MaRISK: expectations for senior management's IT strategy and CISO responsibilities

Banking Act: IT contingency planning requirements

Focus: ECB and cyber risk – developing a supervisory framework

The ECB has made significant progress in developing its understanding and its capacity to intervene in cyber matters. Since the establishment of the SSM in 2014, supervisors have been exploring best practice in the area of IT risk supervision, through interactions with national supervisors and senior IT risk officers in banks.[viii] The ECB has also undertaken an information-gathering exercise to better understand cyber risk at both individual bank and systemic levels. Finally, it has used this knowledge to develop tools to address cyber risks, primarily through routine supervisory activities and authorisation decisions.

Outside of banking supervision, the ECB has pursued initiatives to understand better the cyber vulnerabilities inherent in the financial system, including the development of a number of sector and network maps focusing on interdependencies between FMIs, and creating more sophisticated scenarios for how a cyber attack could spread through financial markets. The ECB has developed a cyber strategy based on three pillars: the cyber readiness of FMIs, sector resilience, and strategic regulator-industry engagement. It has signalled that this workstream is now due to gather pace, with the expected development of an EU red-team testing framework for FMIs in 2018, and the refinement of several joint regulator-industry practices including crisis communication procedures and information sharing.[ix]

Building supervisory capabilities for banks

In 2015, the ECB established a SSM working group tasked with developing a better understanding of how supervisors dealt with cyber and IT risk at the national level.[x] A stocktake of IT supervision practices identified cyber risk, cyber resilience and operational resilience as the most important areas for most of the authorities involved. In the wake of this exercise, and to develop its supervisory capabilities further, the ECB launched a cyber incident reporting pilot phase in 2016 [xi], which was rolled out comprehensively in late 2017. This strengthened the foundation for much of the SSM's current work on cyber and IT risk, which has extended to include a dedicated methodology for on-site inspections and a greater role for off-site supervisory analysis. In the near term, the ECB has signalled that it will follow-up on this work by issuing harmonised supervisory expectations addressing how banks manage IT and cyber risks. Over the long term, the ECB may also consider establishing a cyber resilience testing framework for banks similar to the UK CBEST exercises.

The SSM has gradually developed capabilities that enable it to have a more dynamic understanding of how cyber risk is dealt with by banks. Through its on- and off-site analytical tools and cyber-incident reporting scheme it aims to play a more active role in the management of these threats. The upcoming work on cyber and IT risks that the SSM has signalled it will do in 2018 will also further refine its view on what measures banks should take to mitigate these risks. For banks, this constant policy evolution should be seen as moving towards a new norm, with significant potential for the SSM to use the information it gathers through cyber incident reports and inspections to warrant either specific action at the entity level, or the issuance of broader industry-wide expectations in response to new threats or vulnerabilities that it has identified.

ECB measures

Banking supervision	FMI oversight
• Cyber incident reporting framework	• Development of an analytical framework and methodology for sector mapping, to understand FMI cyber interconnectivities
• Cyber risk components added to on- and off-site supervision methodologies	• Expected development of a pan-European red-team testing framework
• ICT-risk evaluation as part of the operational risk component of the Supervisory Review and Evaluation Process	• Public-private cooperation through the establishment of a Euro Cyber Resilience Board
• IT-risk included in criteria for bank authorisation decisions	

What's on the regulatory horizon?

Regulatory activity looks set to gather pace in the year ahead. Indeed, in this period, regulators in the majority of the FSB's jurisdictions have indicated that they intend to publish new regulatory standards and practices. Signals given by senior regulators in Europe, in particular, show that they are pressing ahead with work that builds on early initiatives and looking at ways to make supervision of cyber risk more routine.[xii] [xiii]

As these developments come to fruition, a number of cases are likely to arise that demonstrate areas where the interests of authorities and firms might not be fully aligned. It is clearly in the shared interest of both banks and supervisors to have a high level of cyber resilience across the financial sector. However, because supervisors, particularly those with a financial stability mandate, are increasingly concerned with the systemic externalities that events in individual banks can cause, and their potential for direct spillovers to counterparties and FMIs, this difference in emphasis could also translate into a material difference in priorities.

For instance, mandating a minimum-downtime target for critical systems is one area where the appetite of supervisors for a quick recovery may be even higher than that of banks. Similarly, widespread use of common software, or third-parties by banks (despite appropriate controls being in place in each individual bank) could cause supervisors to identify systemic vulnerabilities. Concerns such as these will lead to banks feeling increased pressure to demonstrate that their incident recovery plans have been robustly developed and thoroughly tested against sufficiently severe scenarios.

We expect regulators in European jurisdictions to pursue a combination of the following measures:

- **Communicate clearer standards** for the level of cyber resilience they expect critical firms to demonstrate, increasingly reflecting new areas of focus such as application platform security, offline storage of critical backup systems, and controls supporting the segmentation of countries and businesses across a group where threats may arise.
- Assess where firm-specific **enhanced supervision or enforcement action** will be necessary in order to provide sufficient incentive to individual firms and the wider industry to comply with the remediation of identified deficiencies (e.g. ordering an external review of practices, imposing fines).
- Focus on the timeliness and effectiveness of firms' **breach reporting procedures**.
- **Increase pressure on bank Boards** to demonstrate that they are able to provide effective challenge to their management teams on cyber risk issues and that they have access to independent expertise on cyber threats and crisis management.
- Encourage the development of more sophisticated approaches to **quantify cyber risk** and design feedback mechanisms to continually improve this measurement.
- Potentially make a firm-specific supervisory decision to require **additional capital to be held in the form of Pillar 2 buffers** as a direct result of cyber risk deficiencies identified as part of the routine supervisory review of operational risk. (While additional capital will do little, if anything, to protect a bank against cyber risk or shorten its recovery times, it may act as an incentive for the bank to deal with the underlying deficiencies.)
- Expand and embed an increasingly mature programme of **resilience testing**, to occur on a more regular basis and focusing on a broader variety of firms and risks.[xiv] In particular, we expect the ECB to develop a red-team testing framework in 2018 for significant FMIs.[xv]
- Examine barriers to the **sharing of real-time threat intelligence** between firms (and potentially between countries) and make policy changes where necessary.

Key challenge: Rules keeping pace with technological change

Many have expressed concern that the pace of technological change – and the evolving nature of cyber threats – pose a challenge to traditional regulatory approaches, which might create frameworks that quickly become outdated.

The mounting sophistication and persistence of cyber crime, and the growing adoption of highly advanced nation-state type tools by cyber criminals, underscore the challenge both regulators and the industry have in trying to anticipate the kind of cyber threats they will face next.[xvi]

The threat of outdated regulatory standards is arguably greater in financial services than other critical industries. In nuclear energy, for instance, the regulatory approach to ensuring cyber resilience focuses on requiring a nuclear power plant's critical safety and security systems to be sufficiently isolated from the internet and also designed to shut down in the event of any detected disturbance.[xvii] Banks and many other financial services firms, by contrast, need to face new and evolved cyber threats in an environment of constant connectivity. A regulatory approach in financial services simply does not have the option of relying on isolating and discontinuing critical functions.

There is therefore a strong need to design standards that can cope with exposure to a responsive and evolving threat. One area where this challenge comes to the fore is the specificity of cyber risk standards published by regulators. Although the development of a common set of rules can serve to clarify the regulatory hurdle that firms face, private sector respondents to the FSB's 'Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices' noted that overly prescriptive standards could risk turning compliance into a costly and time-consuming 'box-ticking' exercise that protects against risks seen in the past instead of encouraging vigilance towards emerging and unanticipated threats.

On the other hand, broad regulatory principles may indeed give supervisors the discretion to let their expectations evolve over time, but could also deprive the banking industry of having a clear benchmark that their resilience needs to meet.

Taking minimum downtimes for critical systems again as an example, there is a clear logic to setting a high bar for the recovery of systems that underpin the effective functioning of markets. Setting a specific time window for their recovery (e.g. two hours), however, could create challenges over time as the nature of cyber threats and the complexity of disruptions they create evolve.

Another important consideration is the exposure of the financial services sector to new technological capabilities and third party platforms. Regulators recognise that increasing use of artificial intelligence (AI) capabilities such as machine leaning could amplify a range of threats to the cyber resilience of individual banks or the system as a whole. The use of AI outside of the traditional regulatory perimeter (e.g. by cloud storage providers), may also add to the challenge of understanding the extent of a bank's cyber exposure. Creating mechanisms and standards for effectively capturing third party risks is only one part of the challenge; keeping track of the non-financial platforms that could pose such risks to the financial sector, and understanding their own technology risks, could prove to be a significantly more difficult task over time.

The right answer to these challenges will not be a one-size-fits-all solution. The optimal mix of regulation and supervision, and level of specificity in common standards will depend on the threat in question and the maturity of the jurisdiction's supervisory approach. In general, however, the balance struck should be one that encourages a high degree of vigilance and holistic awareness, particularly in the adoption of new platforms, practices and technologies. Furthermore, outcomes-based standards will also work best when the supervisors that assess them demonstrate a strong understanding of the technical processes underlying the outcomes they describe.

Key challenge: International coordination

The 'WannaCry' ransomware attack in May 2017, infecting over 200,000 systems in more than 150 countries in less than a day, demonstrated the global impact that a single coordinated cyber attack can quickly have.[xviii] Cyber risks, and the systemic spillovers associated with those risks crystallising, are not limited by national borders and their spread cannot be easily controlled by national laws or authorities working in isolation, particularly not in the financial sector.

Equally, from a bank's perspective, emerging regulatory regimes for cyber resilience are developing unevenly. The FSB's 2017 Stocktake noted that the approaches taken in some jurisdictions, while similar in intent, often varied widely in their comprehensiveness. The potential for overlaps and gaps in supervisory approaches giving rise to significant complexity, costs and even new risks in banks is a real concern.

Regulators will have to confront the question of international cooperation and consistency, and whether developing a more joined-up approach to cyber resilience is feasible. This will be particularly challenging given strongly-linked national security concerns. Moreover, regulatory cooperation in other areas of financial services policy appears to have passed its post-crisis highpoint and political pressures are reducing the willingness of some countries to copy-out international rules.

Statements such as the 'Principles and Actions on Cyber' [xix] agreed by the G7 can help set the groundwork for creating complementary cyber frameworks that avoid crucial gaps in their terminology or focus. Equally, guidance issued by international standard-setting bodies provides a helpful benchmark for national authorities when designing a regulatory approach. These include the IOSCO-CPMI 2016 guidance on cyber resilience for FMIs [xx] and the Basel Committee on Banking Supervision's 2003 Risk Management Principles for Electronic Banking.[xxi] Meanwhile, exercises such as the FSB's Stocktake and a similar study published in 2017 by the Bank for International Settlements [xxii] usefully highlight the potential overlaps and inconsistencies between frameworks that need to be addressed.

There is, however, a strong need for more consistent terminology and incident-response standards to be adopted at the global level in order to match the global scope of the cyber threats that banks face. While this will undoubtedly be challenging, there are some clear opportunities for deeper international cooperation to be pursued in the near term. The International Monetary Fund, which has shown a growing interest in the threat cyber risks pose to the financial system [xxiii], could use its regular Financial Sector Assessment Programmes to promote the adoption of more consistent approaches between countries. At a more practical level, running joint cyber event simulations involving both the authorities and firms of key financial jurisdictions can help make cyber response plans and playbooks more closely match the reality of an actual attack.[xxiv] In this area, 'Operation Resilient Shield', the UK-US joint cyber attack simulation has set an early best practice. There may be an opportunity for a similar exercise to be held at the EU-level.

The sharing of real-time threat intelligence information on a cross-border basis is potentially far more difficult given a number of technical, legal, and security obstacles. This is likely to progress far more slowly than the running of joint tests, but again, the level of regulatory integration in the EU presents an opportunity to develop and put in place a working template for how this can function efficiently and reduce the financial sector's vulnerability to the spread of cyber threats.

If regulatory cooperation efforts in cyber are not successful, markedly different standards and practices across jurisdictions may weaken the trust public authorities have in each other's frameworks and could encourage them to try to limit the cross-border cyber risk exposure of their firms. In China, for instance, the Cyber Security Law implemented in June 2017 requires 'critical information infrastructure operators' (a term likely to capture most financial institutions) [xxv] to store all personal and important business data within China. Developments such as these could compound the challenge for firms, as the costs and complexity of cyber compliance rise and they face increasingly tailored requirements in the jurisdictions where they operate.

Next steps for banks

Executives with responsibilities for cyber and IT in banks need to anticipate what these regulatory and supervisory developments mean for their organisations and make decisions now on how best to align their cyber resilience activities and investments with them. Those in other roles including internal audit functions and Board members will also need to gain a better understanding of what to do next.

There are a number of key actions that need to be owned – by Chief Risk Officers (CROs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and Chief Operating Officers (COOs) and other executives in relevant functions. These include the following:

1

Engaging early

Senior executives should be in early contact with supervisors to discuss their emerging concerns and better understand how their bank's risk management practices can strike an equilibrium between commercial priorities and a supervisory view of good practice. This should be seen as particularly urgent where authorities are known to be developing new supervisory practices but have not yet published details of their intended approach. Given the challenges supervisors themselves face in grappling with the complexity of cyber risk as a relatively new competency area, these interactions will often be mutually beneficial.

2

Thinking globally

Although the first set of discussions is likely to be with a bank's home supervisor, interactions with host supervisors will also be important, particularly given the absence (for now) of a globally 'joined-up' approach. Banks need a comprehensive view of the regulatory and supervisory demands around cyber resilience that they will face in their main jurisdictions in order to understand where gaps or overlaps exist. Comprehensively mapping their ongoing compliance responsibilities and what they expect to have to comply with in the near-term will give banks a better view of where they may have work to do as rules evolve.

3

Measuring exposure

Strides will have to be made by banks in developing a system that can quantify or measure changes in their exposure to cyber threats in order to facilitate strategic decision-making and investments linked to their cyber risk appetite. This has to start with banks reporting risks against a range of indicators and using cyber incidents internally and across the industry as feedback mechanisms to constantly improve their picture of the potential losses they might face. This will be most beneficial if done collaboratively with supervisors with an understanding that such advances in risk identification ultimately enhance a bank's ability to manage its risk profile, rather than increase its perceived risk.

4

Getting the right talent

Dealing with cyber resilience regulation requires deep experience in both technology and regulatory compliance, a competency profile that is both rare and increasingly in demand. Bringing in people with the right background and experience and giving them the tools they need to facilitate a whole-of-bank approach to strengthening cyber resilience and responding to supervisory concerns will be crucial. Thinking innovatively will be a key strength for executives leading this function, as they are faced with the challenge of balancing demands from compliance activities and ensuring that they remain vigilant to the emergence of new threats.

5

Establishing clear accountability

Although many regulators and supervisors may not identify a preference for how cyber risk and resilience ownership is designed in a bank, having a clear ownership structure in place between the CRO, CIO, CISO and COO, with a single executive ultimately responsible for cyber, and a high level of involvement from the Board, will go a long way in giving supervisors the confidence that a bank's cyber governance arrangements have been well thought through.

6

Improving recoverability

Banks should explore ways to improve their ability to contain an incident and demonstrate to supervisors how they would recover from it quickly. This applies not only to incidents occurring within their own organisation, but also in a counterparty or an infrastructure provider, including processes in place for how they share information on an attack or breach with third parties shortly after it occurs. The concern from supervisors about how a bank manages its relations with third parties is a good indication that banks should think not only in terms of their own 'institutional silo', but also in terms of the interconnected cyber ecosystem in which they operate.

Endnotes

i. Senate Hearing on Jerome Powell's nomination as US Federal Reserve Chair, 28 November 2017.

ii. Financial Stability Board, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, October 2017

iii. European Banking Authority, Guidelines on information and communication technology risk assessment under the supervisory review and evaluation process, May 2017

iv. Bank of England, the Bank of England's approach to operational resilience, speech by Charlotte Gerken, June 2017

v. IOSCO-CPMI, Guidance on cyber resilience for financial market infrastructures, June 2016

vi. Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation, Enhanced Cyber Risk Management Standards, Advanced Notice of Proposed Rulemaking, October 2016

vii. New York State Department of Financial Services, Cybersecurity requirements for financial services companies, Proposed 23 NYCRR 500, March 2017

viii. European Central Bank, Stocktake of IT risk supervision practices, November 2016

ix. European Central Bank, Cybercrime: from fiction to reality, In Focus issue no 2, June 2017

x. European Central Bank, Cyber resilience – A banking supervisor's view, speech by Sabine Lautenschläger, June 2017

xi. Ibid

xii. Bank of England, Financial Stability Report, June 2017

xiii. European Central Bank, Cybersecurity for pan-European financial market infrastructures, speech by Benoit Coeure, June 2017

xiv. Bank of England, the Bank of England's approach to operational resilience, speech by Charlotte Gerken, June 2017

xv. Financial Stability Board, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, October 2017

xvi. SWIFT Institute, Forces Shaping the Cyber Threat Landscape for Financial Institutions, Working Paper, October 2017

xvii. Nuclear Energy Institute, Cyber Security for Nuclear Power Plants, Policy Brief, July 2016

xviii. Institute for International Finance, Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system, September 2017

xix. G7, Principles and Actions on Cyber, G7 Summit, 2016

xx. International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, Guidance, June 2016

xxi. Bank for International Settlements, Risk Management Principles for Electronic Banking, July 2003

xxii. Bank for International Settlements, Regulatory approaches to enhance banks' cyber-security frameworks, FSI Insights, August 2017

xxiii. International Monetary Fund, Germany: Financial Sector Assessment Program-Financial System Stability Assessment, 2016

xxiv. Institute for International Finance, Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system, September 2017

xxv. Deloitte, Cyber regulation in Asia Pacific: How financial institutions can craft a clear strategy in a diverse region, 2017.

Notes

Notes

Contacts

EMEA Centre for Regulatory Strategy

David Strachan
EMEA Lead
Centre for Regulatory Strategy
Deloitte UK
+44 (0) 20 7303 4791
dastrachan@deloitte.co.uk

Simon Brennan
Director
Centre for Regulatory Strategy
Deloitte UK
+44 (0) 20 7303 5267
simbrennan@deloitte.co.uk

Scott Martin
Senior Manager
Centre for Regulatory Strategy
Deloitte UK
+44 (0) 20 7303 8132
scomartin@deloitte.co.uk

Quentin Mosseray
Associate
Centre for Regulatory Strategy
Deloitte UK
+44 (0) 20 7007 3213
qmosseray@deloitte.co.uk

UK Cyber Risk Practice

Nick Seaver
Partner, EMEA Cyber Banking Lead
Deloitte UK
44 (0) 20 7303 7097
nseaver@deloitte.co.uk

Stephen Bonner
Partner
Deloitte UK
44 (0) 20 7303 2164
stephenbonner@deloitte.co.uk

CENTRE *for*
REGULATORY STRATEGY
EMEA

The Deloitte Centre for Regulatory Strategy is a powerful resource of information and insight, designed to assist financial institutions manage the complexity and convergence of rapidly increasing new regulation.

With regional hubs in the Americas, Asia Pacific and EMEA, the Centre combines the strength of Deloitte's regional and international network of experienced risk, regulatory, and industry professionals – including a deep roster of former regulators, industry specialists, and business advisers – with a rich understanding of the impact of regulations on business models and strategy.

Deloitte.

Designed and produced by The Creative Studio at Deloitte, London. J14773