LEXOLOGY

The art of managing cyber risk

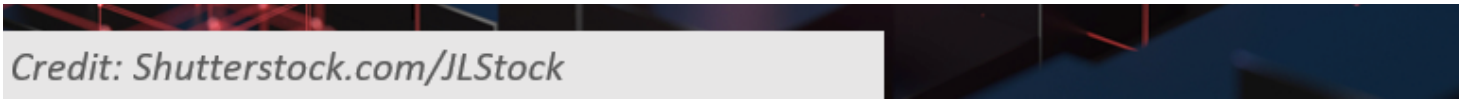
Updated as of: **12 June 2023**

GBRR | NOW PART OF LEXOLOGY PRO

Managing cyber risk has surged to the top of the supervisory concerns for financial regulators globally, implemented within a broader agenda of operational resilience, following increased attacks during the COVID 19 pandemic and geopolitical turmoil. Lexology PRO considers the changing landscape of cyber threats, the harmonisation of regulations across major jurisdictions, and what banks and fintechs need to do to achieve compliance.

For this discussion, Lexology PRO spoke with:

- **Mark Bailey**, partner at Charles Russell Speechlys in London
- **Yvonne Dunn**, partner and head of the financial services technology practice, and **David McIlwaine**, head of cyber at Pinsent Masons in London
- **Joep Gommers**, CEO of intelligence technology platform EclecticIQ in Amsterdam
- **Marcus Christian**, partner and co-leader of global cyber incident response at Mayer Brown in Washington, DC
- **Mike Nonaka**, co-chair of the financial services group at Covington & Burling in Washington, DC


Credit: Shutterstock.com/JLStock

The last year has seen cybersecurity leap to the top of the agenda for financial institutions and regulators alike. In January, the annual survey by the Institute of International Finance and EY of banks' chief risk officers (CROs) found over half name cybersecurity as their top concern for 2023, ahead of climate and financial risk, and regulators in the UK, EU and the US have been diligent in publishing new proposals to manage the risks surrounding third party service providers, as well as updating their cyber-attack response policies.

Most recently, on 6 June, the US federal bank regulators released their joint guidance for managing third party risk for banking organisations. That came a month after the European Supervisory Authorities (ESAs) also began to finetune their criteria for critical ICT third-party providers under the Digital Operational Resilience Act (DORA), adopted in November 2022.

In April, the UK's three principal regulators – the Bank of England (BoE), Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) – likewise released a discussion paper on the regulation of operational resilience and critical third parties, mapping out cost estimates for implementing and ensuring compliance with potential minimum resilience standards.

But while regulators have long covered these risks in "a disaggregated form", as the landscape of cyber threats changes and technology evolves, the industry has demanded stronger cybersecurity practices.. Moreover, harmonisation, is a constant drumbeat for practitioners, regulators, and technology companies – as seen in the reaction to the US Securities and Exchange Commission (SEC)'s newly- proposed cyber risk requirements in March, which saw demands for revision to bring them in line with other related proposals.

But are these concerns really so closely related and can they be lumped together within the same discourse?

UK and EU: vertical and horizontal harmonisation

Mark Bailey, a partner at Charles Russell Speechlys in London, says the discussion of regulators' oversight of third party technology providers has been ongoing for years. He says it is very material that regulators now consider such oversight appropriate.

The main concerns for clients regarding DORA, as an EU regulation, relate to how well it will harmonise with other regulations, he says, taking into consideration how institutions will comply within the UK, the US, and globally, and avoiding a patchwork of regulation.

"Harmonising to a global standard is very live, and that's live to both the customers and also for the suppliers," Bailey says.

"If you are dealing with global businesses, you will need that form of global consistency. The challenge for some organisations is that these regulations only affect financial services, while cyber risk is a global problem," he says.

“Global businesses have multiple sectors to supervise, not just financial services, so you would have to work out the implications of running infrastructure that is compliant with cyber regulations, against the cost of that to running other businesses,” Bailey says.

Those businesses are already well accustomed to dealing with global compliance, Bailey says, but they will have to assess the extent of their reporting obligations.

Yvonne Dunn, partner at Pinsent Masons in London and leader of its financial services technology practice, says that the post-Brexit discussion on which way to take with regulation and having to balance that with existing globally has been interesting. “Having wildly divergent rules isn't necessarily going to be that helpful for business, and obviously potentially quite unhelpful for things like equivalence,” she says.

“I think we're seeing this theme of operational resilience playing out across various jurisdictions,” she tells LexPRO.

“DORA is now on its timeline in Europe, and the UK has already got a regime that that has a number of similar aspects already in play,” Dunn goes on. “At the same time, looking at some of the newer aspects of DORA, such as the direct supervision of suppliers, I think that is definitely the direction of travel we can see the UK heading in as well,” she says.

Dunn says that will be interesting, because for the first time a number of key critical suppliers will be under regulatory supervision. She adds that she is looking forward to seeing how that will play out in those suppliers’ engagement with customers, as well as their approach to contracts.

Similar themes are coming through in the US as well, Dunn says, and on a global scale regulators are making efforts towards collaboration with sandbox exercises, with the intention of creating a path for financial institutions to develop ideas that they can be confident will meet cross-border regulatory obligations.

From a compliance perspective, the extent to which many fintech- and regtech-type solutions are looking to address the issue is impressive, Dunn adds.

Achieving compliance

In practice, managing cybersecurity isn’t just a tick-box compliance exercise, argues **Joep Gommers**, CEO of intelligence technology platform EclecticIQ.

Within the European Union, he points out, the legislative direction of travel has been more towards collaborating to understand a different landscape the continent is facing, rather than just achieving a certain established level of security.

One example of that is the Networks and Information Security 2 (NIS2) Directive, which entered into force in January, with member states set to transpose into national law before 17 October 2024. It was intended as an update to the EU’s existing NIS Directive, with the hope of responding to growing cyber-attacks with more stringent supervisory measures.

But companies will have to take action ahead of that implementation, Gommers says. “There is a kind of a sequence of companies of certain size and criticality to have all these mechanisms in place, to have the support of the national security centre of their country, to understand that if one organisation has an incident, they can share the information in such a way with others that they can be proactive against what you have reacted against,” he explains.

Gommers says that it helps companies to not just ensure their own security, but be part of a group of constituents or like-minded people within a sector, spreading the burden of analysing cyber threats or responding to them.

“There’s a big shift in legislation that’s driving ‘compliance’, but also the definition of critical infrastructure with this new legislation in Europe has dramatically expanded,” he says. “Critical infrastructure used to be, for instance, 200 organisations in the Netherlands; it’s now 20,000 in the Netherlands. So the scope of who has to abide with certain kind of legislation, and therefore comply with it, has significantly enlarged and improved.”

Simply complying with regulations is not *per se* going to make an organisation better able to defend itself against multiple cyber threats, Gommers warns.

“There’s a baseline of things you need to do to meet some minimum standard of compliance, but that’s not taking into the account the reality of the cyber threat landscape, which changes much faster, and that’s what operational security organisations inside organisations are dealing with.”

He adds that the nature of the threat has changed. While cybercrime used to be the main threat, Gommers suggests that this has fully shifted towards espionage in terms of sophistication and capability.

The head of Pinsent Masons' global cyber practice, **David McIlwaine**, says that cyber-attacks and their disruptiveness have been on the rise during the past three or four years, particularly during the COVID 19 pandemic.

“Since this is a known business risk, the regulators are not going to have a have sympathy just because the organisation has been a victim of a cyber-attack,” he says.

“And so, there's a big push on businesses to get cyber ready, to make sure they know what their obligations would be, to have a playbook to rehearse, a scenario test, and so on,” McIlwaine says.

He adds that while the scope of NIS2 in Europe is often considered to be a bit wider, primarily the same obligations apply in the UK.

“In the UK, it applies to cloud service providers, online marketplaces, et cetera, so it does cover certain digital service providers already, whereas the EU is going wider in terms of industries that it affects,” he says.

“In the UK, they're going vertically down, so they're saying, not only do these industries need to comply, but also so do IT service providers – effectively applying this regulation to the supply chain, and that's quite a significant change,” he says, adding that it is “causing some ruffles”.

The US

Marcus Christian, partner and co-leader of Mayer Brown’s Washington DC global cyber incident response practice, says “it’s amazing” that the cyber perspective is only now being considered when discussing operational risk.

He says that incorporation of cybersecurity into operational resilience discourse has shifted the culture from incident response toward a more everyday perspective, because it engages organisations at a high level.

This means that, as regulators call for adequate attention and resources to managing risk, organisations need to promote a culture that promotes cybersecurity as a part of their resilience.

Mike Nonaka, Covington & Burling partner in Washington DC and co-chair of the firm’s financial services group, agrees that that there are broader trends at issue both in operational resilience and increasing regulatory coordination, but he doesn’t necessarily tie all of them together.

“I think operational resilience is intended to be this broader umbrella to address different types of risk. It's not the only one, but this is clearly an area that they're focusing on, and cybersecurity is a component of it,” he says.

He notes that bank regulators have addressed these risks in “a disaggregated form for a very long time,” but now they expect banks to look at disruptions – from cyber security, geopolitical risk, or instability from a given counterparty – in a holistic way. That includes more intentionality from an internal controls perspective, he says.

The pace of regulation always lags behind the pace of innovation. “Sometimes people complain about that because they want regulation to keep up, or they think that it's too slow,” Nonaka says, but he argues Nonaka says there are positives.

Regulations that are too prescriptive might hinder technological innovation,” he says. Slower pace for developing and implementing regulation allows for thorough observation of how the regulated technology actually works, “and the things that you don't necessarily know before it's actually been launched”, Nonaka says.

“So there is that tension there, but there are pros to it,” he concludes.