

Operational resilience

The global deluge of incoming regulatory requirements
and the need for compliance

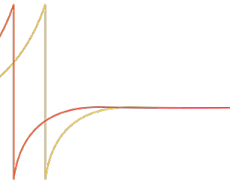
January 2024



Virginie O'Shea

fintechfirebrand.com

© 2024 Firebrand Research. All rights reserved. Reproduction of this report by any means is strictly prohibited.



The regulatory focus on resilience

Operational resilience is top of mind for every regulator and market participant in 2024. Cyberattacks and artificial intelligence-generated (AI-generated) misinformation and disinformation are both in the top five risks that industry participants believe are most likely to present a material crisis on a global scale in 2024, according to the World Economic Forum's latest annual Global Risks Perception Study¹. The regulatory prioritisation of operational resilience is understandable in the context of the rising threat vectors across the cybersecurity landscape and the impact of another top five WEF risk, extreme weather on operational centres across the globe. As noted in the European Securities and Markets Authority (ESMA) Trends, Risks and Vulnerabilities Report in August 2023², the financial services industry now accounts for 12% of all cyberattacks globally, up from 4% in early 2019.

The number of publicly acknowledged cyber-attacks hit a peak in the second half of 2022 at around 90, up from less than 10 in early 2019. The below graphic shows the threat vectors of most concern identified by the European Union Agency for Cybersecurity's (ENISA) Threat Landscape 2023 report³. Ransomware remains one of the largest threats overall and has increased in professionalisation and proliferation across the financial services sector due to ransomware-as-a-service models. However, technologies such as generative AI has also enabled basic phishing attacks to become much more targeted and sophisticated in approach, including social engineering.

¹ [WEF Global Risks Perception Study 2023-2024](#), WEF, January 2024.

² [ESMA TRV Risk Monitor](#), ESMA, August 2023.

³ [ENISA Threat Landscape Report 2023](#), ENISA, October 2023.



Ransomware



Malware



Social engineering



Threats against data and availability



Information manipulation and interference



Supply chain attacks

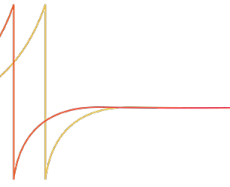
The geopolitical landscape has exacerbated the cyber threats, and the costs of these attacks are increasing year-on-year, according to research by the Ponemon Institute and IBM Security⁴. The average cost of a data breach in 2023 was US\$4.45 million, a 15% increase over the cost in 2020. The Federal Bureau of Investigation (FBI) also tracks the cost of internet crimes in the US and in its March 2023 report⁵, it noted that the FBI's Internet Crime Complaint Center received 800,944 complaints in 2022 with a potential total loss of more than US\$10.2 billion. Not only are cyber-attacks increasingly expensive, they can also impact the reputation of the financial institution in question, which can result in a drop in shareholder value, regulatory fines and a fall in client confidence.

The changing regulatory landscape

In light of these rising cyber-threats and the increased industry focus on decreasing operational risk related to disruptions of any kind, the Digital Operational Resilience Act (DORA) in Europe and numerous other similar regimes across the major markets are

⁴ [Cost of a Data Breach Report 2023](#), Ponemon Institute and IBM Security. July 2023.

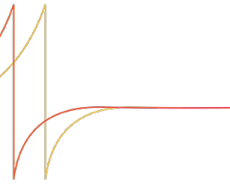
⁵ [2022 Internet Crime Report](#), FBI, March 2023.



targeted at increasing the resilience and transparency of the financial services sector in this area overall. Supranational bodies such as the Financial Stability Board (FSB) have also stepped in to try and establish a global baseline for these resilience requirements for critical third parties. In December 2023, the FSB published what it calls a “toolkit”⁶ to help regulators and market participants assess and monitor their mission-critical system providers. The FSB proposals include a wide range of operational resilience topics including:

- **How the industry should assess third-party risk management:** The global nature of the markets is emphasized here as any regulation is likely to be extraterritorial. Very few firms will have all of their critical third-party providers located in one regulatory jurisdiction, which means firms need to understand how each of the jurisdictions compare when it comes to third-party evaluation.
- **What firms should focus on when it comes to third parties:** The size of the provider isn't the most important factor in these assessments; it's also how impactful the service or technology is to the day-to-day running of a firm's operations. The critical providers of that technology or service are also extremely important to evaluate, especially if the provider is dependent on one particular cloud provider, for example.
- **An emphasis on regular and timely reviews and communication:** This is not a 'one and done' exercise, and regulators are being encouraged by the FSB to conduct regular assessments of industry compliance when it comes to monitoring and evaluating their critical services. The timeliness of notifications when incidents happen, as dictated by the various requirements in each jurisdiction, is also a focus of the supranational regulator.
- **Test, test and test again:** Business continuity plans and cybersecurity drills must be regularly reviewed and tested to ensure they keep up to date with current operational and technology set-ups and the latest cyber-attacks.
- **Minimize concentration risks and have exit strategies:** This might not be a big part of all of the regulatory proposals out at the moment, but the FSB has flagged the need for firms to minimize service provider concentration risk where possible.

⁶ [Enhancing Third-Party Risk Management and Oversight](#), FSB, December 2023.



The US markets have seen numerous proposals related to operational resilience over the last couple of years across the various market segments. In February 2022, the Securities and Exchange Commission (SEC) proposed new requirements and amendments to existing rules⁷ intended to enhance the operational resilience of the US securities markets, targeted at registered investment advisers and registered investment companies. The Commodity Futures Trading Commission (CFTC) also proposed a new set of operational resilience rules in December 2023⁸ focused on reducing the impact of disruptions on futures commission merchants (FCMs), swap dealers and major swap participants. The proposed rules, crafted by the CFTC's Markets Participants Division, were unanimously approved by the commissioners and will apply to the derivatives sector as a whole.

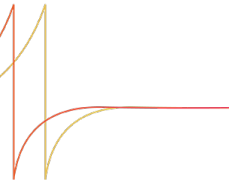
In March 2023, the SEC proposed new transparency-focused amendments to Regulation S-P⁹, which is focused on client data protection among other things. The proposals would require broker-dealers, investment companies, registered investment advisers and transfer agents to provide notice to individuals affected by certain types of data breaches that may put them at risk of identity theft or other harm. In the same month as the Regulation S-P amendments, the SEC also proposed two new rulemakings focused more generally on cybersecurity. The first would require key market participants to take measures to protect themselves and investors from the harmful impacts of cybersecurity incidents. The second proposal amends existing rules to expand the scope of entities subject to Regulation Systems Compliance and Integrity (SCI) and update requirements around next generation technology adoption and newer trading practices including more disclosures related to these items¹⁰.

⁷ [Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies](#), SEC, March 2022.

⁸ [Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants](#), CFTC, December 2023.

⁹ [Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information](#), SEC, August 2023.

¹⁰ [Regulation Systems Compliance and Integrity](#), SEC, March 2023.



In July 2023, the SEC adopted final rules requiring public companies to disclose material cybersecurity incidents on Form 8-K and provide enhanced disclosure of cybersecurity risk management, strategy, and governance in annual reports¹¹. These new rules amend a number of existing SEC regulations and they come into force for disclosures beginning with annual reports for fiscal years ending on or after 15 December 2023 for large firms and by June 2024 for smaller firms.

Turning back to Europe, 2023 was a busy year for the European Securities and Markets Authority (ESMA) and its fellow EU-level regulators when it came to DORA preparation, with the publication of multiple consultations containing proposed regulatory technical standards (RTS) for the incoming regime. These RTS proposals include a batch published in June 2023¹² that provide details of the requirements for incident reporting, third party provider risk management and templates for provider information that needs to be gathered under DORA and these were finalised in January 2024¹³. The second batch of DORA technical standards proposals for the year was published in December 2023¹⁴ focusing on the details for regulatory cooperation, incident reporting templates and how costs and losses should be calculated for incidents, among other items.

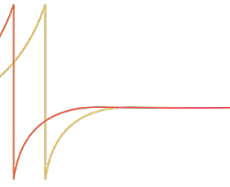
The next big item on the DORA proposal front will be the feasibility report on the EU hub for DORA data, which is expected sometime in the next 12 months with a view to being submitted to the European Commission by January 2025. The Commission will also be spending 2024 assessing all of the remaining DORA proposals and the public feedback ahead of publishing the final technical standards before the year end. These proposals already take into account the feedback of more than 50 authorities and once finalised,

¹¹ [Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure](#), SEC, July 2023.

¹² [ESAs consult on the first batch of DORA policy products](#), ESMA, June 2023.

¹³ [ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification](#), ESMA, January 2024.

¹⁴ [ESAs launch joint consultation on second batch of policy mandates under the Digital Operational Resilience Act](#), ESMA, December 2023.



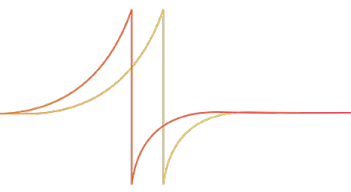
the standards will have to be translated into operational requirements by each impacted financial institution (essentially, every firm operating in the EU).

In the UK, the Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) are also consulting on rules related to critical third-party dependencies within the financial services sector. The three regulatory authorities issued the consultation in December 2023¹⁵ and firms have until March 2024 to provide feedback on the rules that include new reporting requirements for disruptions and annual self-assessments for third-party providers. They also introduce a new set of granular operational risk and resilience requirements for providers of mission critical systems, including supply chain risk management and incident management requirements.

The Monetary Authority of Singapore (MAS) issued its own guidelines for operational resilience back in 2022, but 2023 saw the regulator take some direct action on operational resilience enforcement. In November 2023, MAS took the relatively unusual step of barring DBS Bank from focusing on any of its non-essential activities to ensure that it makes improvements to its system resilience over the succeeding two quarters. The Singaporean bank had been beleaguered by system outages and disruptions over the course of 2023 and MAS felt the need to step in. The firm was granted six months to focus on fixing its various system resilience shortcomings and to introduce new and more robust incident management, change management and technology risk governance and oversight processes. Moreover, 2024 will see the regulator check that these changes have been made to its satisfaction.

The Hong Kong Monetary Authority (HKMA) also issued guidelines for operational resilience back in 2022 and 2024 will be a key year for firm implementation ahead of the May 2026 final deadline. Firms must introduce regular testing for critical operations resilience under severe scenarios and establish incident management programs, including third-party dependency management details. This is similar to the focus of the

¹⁵ [Operational Resilience Critical Third Parties to the UK Financial Sector](#), Bank of England, PRA and FCA, December 2023.



Australian Securities and Investments Commission (ASIC) regime, which came into force in March 2023 and requires risk-based reviews of cyber and operational resilience on a regular basis. ASIC is also keeping a close eye on the upgrade programme at the ASX for its Clearing House Electronic Subregister System (CHES), which has faced a rocky few years on the resilience front. Operational resilience remains one of ASIC's strategic priorities as part of its five-year corporate plan¹⁶.

At the international level, in December 2023 the International Organisation for Securities Commissions (IOSCO) published a consultation report¹⁷ listing best practices for handling outages, regardless of the underlying cause of the disruption. The main guidance from IOSCO comprises:


- **Establish an outage plan:** Make sure every impacted business line knows how to handle the outage and their responsibilities, particularly when it comes to client communication.
- **Provide clarity on next steps and notice before resumption of services:** There is a huge focus on timeliness of communication, even when trading, clearing or settlement is about to resume to ensure clients are kept aware of developments.
- **Have alternative backup processes where possible and show regulators that lessons have been learned:** This is about both planning ahead of disruptions (and providing these plans to regulators) and indicating that lessons have been learned through the experience and outages of a similar kind will not happen again.

The industry best practices

In light of these numerous regulatory changes, firms need to get a better handle on their existing estate of service providers and data and technology environments across the globe. In this endeavour they will need to identify any existing gaps and weaknesses that need to be addressed from a cybersecurity or operational risk reduction point of view. This could be a huge administrative burden on large financial institutions if undertaken

¹⁶ [ASIC Corporate Plan](#), ASIC, August 2023.

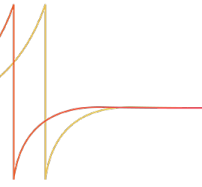
¹⁷ [Consultation Report on Market Outages](#), IOSCO, December 2023.



without experienced partners that understand where data protection, business continuity and resilience challenges may lie. Large firms tend to have multiple stores of siloed data and a multitude of different systems across their technology environments that could mask underlying data access weaknesses and potential exposure of sensitive data.

In order to address these challenges firms need to consider:

- **Conduct regular reviews:** Focus on assessing existing dependencies and the resilience of all technology and services environments, regardless of whether they are on premises or on the cloud, or internally or externally provided on a regular basis.
- **Install multiple layers of data protection:** There is a huge ongoing regulatory focus on data protection and cybersecurity is all about preventing those critical data assets in as robust a manner as possible.
- **Invest in attack detection capabilities:** The faster a firm can identify an attack, the quicker it can be addressed. Scanning for vulnerabilities should be table stakes and cyber-weaknesses can and do evolve as attack vectors change.
- **Focus on quick recovery:** The mirroring of mission critical functions in back-up environments that are the regulatory-prescribed distance away from primary sites is key.
- **Realise this isn't 'one and done':** Regulators and clients expect firms to conduct regular stress testing exercises and business continuity planning requires adequate oversight and governance on an ongoing basis.



Key Takeaways

- **Preparation for incoming reporting regimes is vital.** Though DORA comes into force in January 2025, it will take months of preparation for firms to get ready for reporting, especially when it comes to service provider data reporting. Buy-side firms in particular may need to build in extra time to query information received from their outsourced service providers. Regulators are prioritising operational resilience over many other areas, which means they are likely to come down hard on noncompliance to prove a point back to the industry about the importance of cybersecurity and operational risk reduction.
- **Outage planning will be key:** Whether it is down to a cybersecurity incident or a technical glitch, firms need to expect to be disrupted at some point. Regulators will demand that large financial institutions, centralised service providers and market infrastructures provide evidence of pre-planning and stress testing for evolving outage scenarios on a regular basis.
- **Cybercriminals will continue to innovate.** The geopolitical landscape is likely to ensure that criminals remain well-funded and motivated to cause both financial harm and disruption. The increased professionalisation of cybercrime combined with the rapid evolution of new technologies should ring alarm bells at every firm. AI has already improved the way that cybercriminals target firms with phishing attacks using social engineering. Even regulators have been compelled to warn firms of their own cybercriminal impersonators.
- **Ransomware in particular remains one to watch.** The success of ransomware attacks across the globe has proven to cybercriminals that this is a viable route to make significant proceeds. Ransomware-as-a-service continues to gain ground on the criminal mass market, so expect more of this in future combined with data theft. The large firms may be the focus of big game hunters but with mass availability, comes much more activity targeting firms of all sizes.



We're passionate about capital markets research

Our expertise is in providing research and advisory services to firms across the capital markets spectrum. From fintech investments to business case building, we have the skills to help you get the job done.

- The voice of the market
- Independent
- Built on decades of research
- Practical not posturing
- Diversity of approach
- Market research should be accessible

For more information visit fintechfirebrand.com or email contact@fintechfirebrand.com

