

Becoming resilient

Navigating financial services regulation and the ransomware minefield

February 2024

Commissioned by



VERITAS™

Virginie O'Shea



fintechfirebrand.com

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



Why regulators care about resilience

The impact of just one cyber-attack on a whole segment of the financial services industry is much more evident in 2024 than it was just a few years ago. The first month of 2024 saw global securities trading and analytics platform EquiLend taken offline for a few days by a cyber-attack¹, which caused disruption to lending activities across the globe as banks had to switch from automated to manual processes. The Securities and Exchange Commission (SEC) also experienced a cyber-incident in the same month when the regulator's social media account on X was compromised and an individual posted an inaccurate statement to the account that caused the price of bitcoin to rise. Cyber-attacks can cause markets to move and significant disruption to businesses, incurring costs and heightened risks for the firms affected.

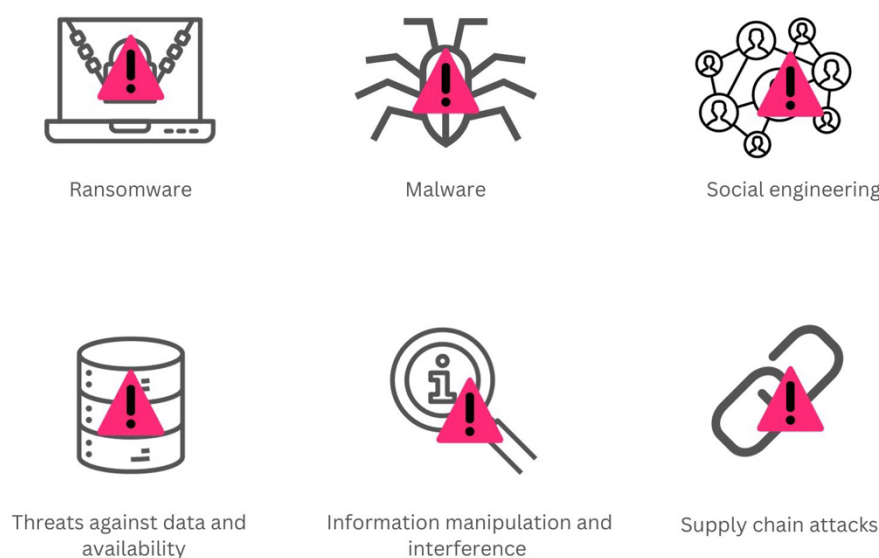
It is therefore easy to see why operational resilience is top of mind for every regulator and market participant in 2024. Cyberattacks and artificial intelligence-generated (AI-generated) misinformation and disinformation are both in the top five risks that industry participants believe are most likely to present a material crisis on a global scale in 2024, according to the World Economic Forum's latest annual Global Risks Perception Study². 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 2023³, the financial services industry now accounts for 12% of all cyberattacks globally, up from 4% in early 2019.

¹ [EquiLend outage hits some automated securities lending services](#), Reuters, January 2024.

² [WEF Global Risks Perception Study 2023-2024](#), WEF, January 2024.

³ [ESMA TRV Risk Monitor](#), ESMA, August 2023.

The below graphic shows the threat vectors of most concern identified by the European Union Agency for Cybersecurity's (ENISA) Threat Landscape 2023 report⁴. 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.



The geopolitical landscape has exacerbated the cyber-threats and the costs of these attacks is increasing year-on-year, according to research by the Ponemon Institute and IBM Security⁵. 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 report⁶, 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,

⁴ [ENISA Threat Landscape Report 2023](#), ENISA, October 2023.

⁵ [Cost of a Data Breach Report 2023](#), Ponemon Institute and IBM Security. July 2023.

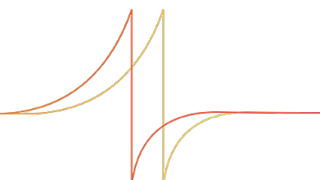
⁶ [2022 Internet Crime Report](#), FBI, March 2023.

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 targeted at increasing the resilience and transparency of the financial services sector in this area overall. The below graphic highlights the global view of existing and incoming regulation related to operational resilience.





The Canadian Office of the Superintendent of Financial Institutions (OSFI) published its consultation on revised operational resilience guidelines in October 2023⁷ and final guidelines will be published some time in 2024 with a view to strengthening firms' business continuity and crisis management, as well as their operational risk management. South Africa's banking authority issued a new proposed operational resilience directive in April 2023 with a view to introducing the new rules by December 2024⁸ based on the Basel Committee on Banking Supervision's (BCBS's) principles from 2021.

The US markets have seen numerous proposals related to operational resilience over the last couple of years across the various segments of the market. In February 2022, the Securities and Exchange Commission (SEC) proposed new requirements and amendments to existing rules⁹ 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 2023¹⁰ focused on reducing the impact of disruptions on futures commission merchants (FCMs), swap dealers and major swap participants. The proposed rules, which were 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-P¹¹, which is focused on client data protection among other things. The proposals would require broker-dealers, investment companies, registered investment advisers and

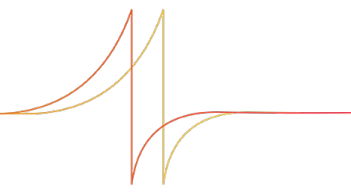
⁷ [OSFI launches consultation on draft Guideline E-21, Operational Resilience and Operational Risk Management](#), OSFI, October 2023.

⁸ [Principles for operational resilience](#), South African Reserve Bank Prudential Authority, April 2023.

⁹ [Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies](#), SEC, March 2022.

¹⁰ [Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants](#), CFTC, December 2023.

¹¹ [Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information](#), SEC, August 2023.



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 items¹².

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 reports¹³. 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 2023¹⁴ 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 2024¹⁵. The second batch of DORA technical standards proposals for the year was published in December 2023¹⁶

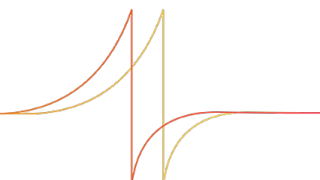
¹² [Regulation Systems Compliance and Integrity](#), SEC, March 2023.

¹³ [Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure](#), SEC, July 2023.

¹⁴ [ESAs consult on the first batch of DORA policy products](#), ESMA, June 2023.

¹⁵ [ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification](#), ESMA, January 2024.

¹⁶ [ESAs launch joint consultation on second batch of policy mandates under the Digital Operational Resilience Act](#), ESMA, December 2023.




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, 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 2023¹⁷ 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

¹⁷ [Operational Resilience Critical Third Parties to the UK Financial Sector](#), Bank of England, PRA and FCA, December 2023.



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 programmes, including third party dependency management details. This is similar to the focus of the 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 plan¹⁸.

The path forward

Regulatory changes are only one reason why firms need to focus on improving their resilience, the impact of significant downtime on clients, brand and sometimes the market as a whole can be severe. Financial services as an industry is built on a foundation of trust and part of maintaining that trust is continuously proving resilience and risk mitigation. Supporting business continuity is contingent on understanding the existing estate of service providers and data and technology environments across an enterprise and identifying any potential weak points as cyber-threats evolve. Recovery time objectives that have been established by market practices and regulations need to be achieved to maintain compliance and minimise disruption.

Firms need to both minimise their cyber-weaknesses and plan for how they will respond to a successful cyber-attack or operational outage. This entails multiple layers of

¹⁸ [ASIC Corporate Plan](#), ASIC, August 2023.



protection such as zero trust architectures and a good handle on where sensitive data that needs extra attention is stored and managed. 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 should:

- 🔥 **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.
- 🔥 **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.
- 🔥 **Develop zero trust architectures:** Establishing a perimeter of cyber-security isn't enough, firms need to recognise that attacks can get past a single layer of 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.
- 🔥 **Focus on automating recovery as much as possible:** The mirroring of mission critical functions in back-up environments that are the regulatory-prescribed distance away from primary sites is key. The recovery processes need to be automated as much as possible in order to meet regulator-prescribed recovery time objectives
- 🔥 **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. 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.
- 🔥 **Quick and automated recovery 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. They will need to automate as much of the recovery process as possible to meet regulatory prescribed recovery time objectives.
- 🔥 **Understanding evolving points of weakness will be challenging.** Cybercrime is constantly evolving and firms will need to keep on top of these changes over time. Working with an experienced partner may be necessary to ensure the latest developments are understood and the related risks are mitigated.
- 🔥 **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.
- 🔥 **Explore the partners in the market:** Firms don't need to go it alone, there are a range of partners with relevant expertise that can support their compliance journey.



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



