

June 2023

Operational Resilience

The Evolving Regulatory and Financial Services Industry Dynamics

Virginie O'Shea

The data safekeeping imperative

Financial institutions have a wealth of internal and external data from which to derive important signals and insights to inform everything from hedging to regulatory reporting. However, the sheer volume and variety of data sets to manage are often problematic, as well as its dispersion across a firm's various business and operational silos. Finding the right data at the right time to make a decision in a volatile market where latency matters is far from a simple proposition. Add the necessity of keeping this data safe in an environment where cyber-attacks have become increasingly sophisticated, and you have a significant challenge on your hands.

Effective data controls are therefore important from a business, regulatory and client perspective. Faster time to insight provides a competitive advantage from a business perspective and a greater understanding of a client's activities can be gleaned from mining data from across the business. However, that data has to be kept safe at all costs, as well as still be easily accessible by the business and available to be downloaded to be provided to regulators or clients if requested.

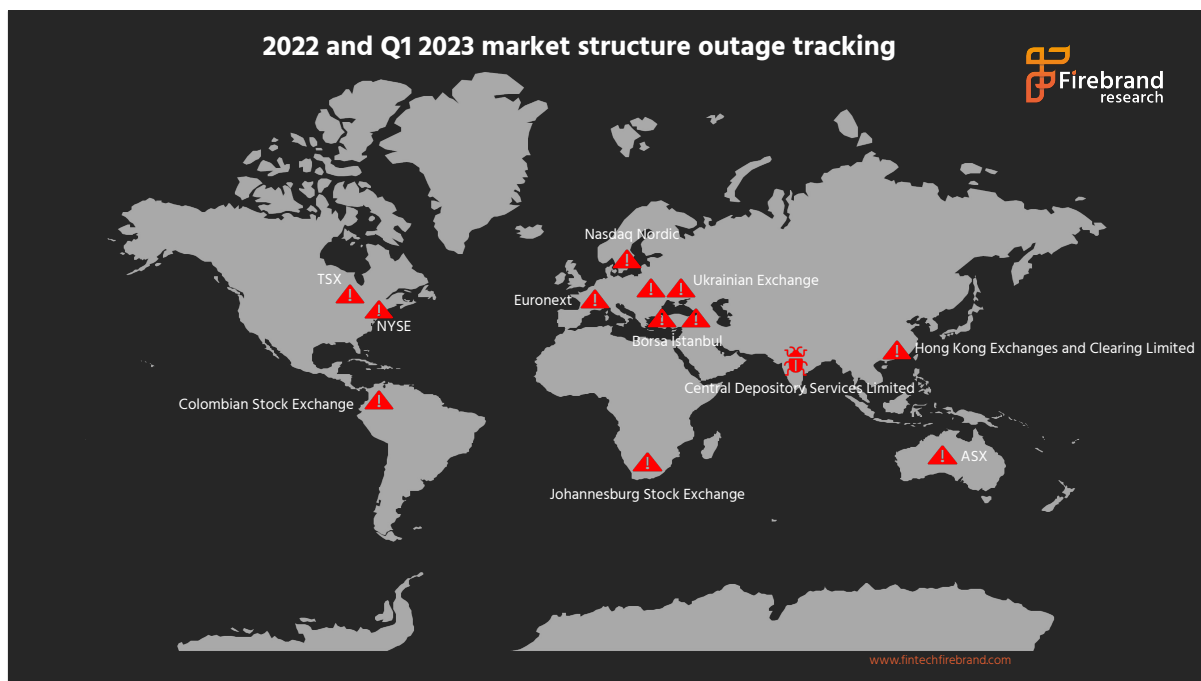
Poor data controls and recordkeeping can come with hefty financial penalties from the regulators as it is considered vital to the preservation of market integrity and investor protection. In September 2022, for example, 15 broker-dealers and one affiliated investment adviser had to pay penalties totaling US\$1.1 billion to the Securities and Exchange Commission (SEC) for what the regulator called "widespread recordkeeping failures."¹ Year after year, financial institutions of all kinds face increased regulatory scrutiny over their data management, governance and now, increasingly, their data privacy and protection practices.

A regulatory focus on resilience

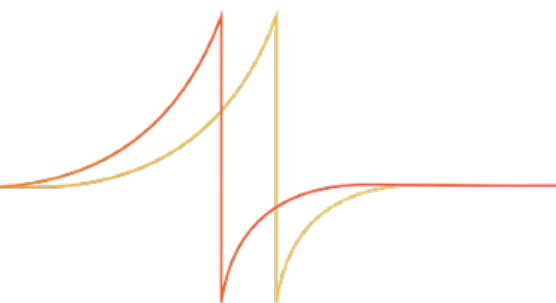
Regulators are keenly aware of the risks posed to the industry by cyber-criminals and various operational risks. Operational outages can severely impact the markets,

¹ [SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures](#), September 2022, SEC.

especially if market infrastructures, large financial institutions or service providers such as cloud providers are involved. Firebrand's research indicates that operational outages were relatively frequent throughout 2022 and bank and market infrastructure downtime varied in length from 20 minutes up to several days. The graphic below highlights some of the major market infrastructure outages throughout the year and into the first few months of 2023.



Stock exchanges, clearing houses and central securities depositories (CSDs) are all 'big game hunter' targets for cybercriminals as suspension of their operations can cause significant disruption to markets. If a stock exchange is unable to support its core function of trading, then multiple financial institutions will face direct financial and operational impacts. This is why these systemically important financial market infrastructures (SIFMUs) have been the focus of most regulatory proposals to improve cybersecurity market practices.

A decorative graphic consisting of several thin, curved lines in shades of orange and red, extending from the right side of the page towards the center, creating a sense of movement and flow.

Governments around the world are also emphasizing the need for better cybersecurity across industries. To this end, in March 2023, the White House issued a new national cybersecurity strategy² for the United States to increase pressure on firms, including financial institutions and SIFMUs, to invest further in their own cybersecurity. The focus of these efforts and those of industry regulators such as the European Securities and Markets Authority (ESMA) and the Securities and Exchange Commission (SEC) is on compelling firms to invest in supporting both defensive and recovery strategies.

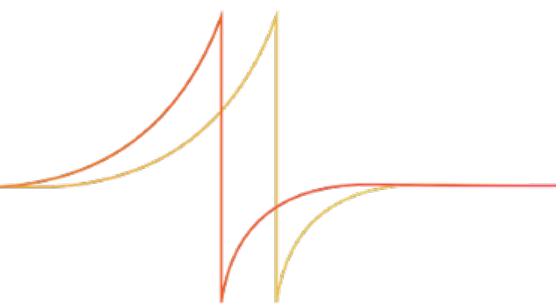
Operational resilience regulations such as ESMA's Digital Operational Resilience Act (DORA) include requirements related to incident response, vulnerability disclosure, supply chain security and encryption. European regulators are particularly keen to understand any potential risks that cloud technology arrangements may pose to the financial services industry globally, especially as more firms move to cloud-hosted arrangements as part of digital transformation programs. To this end, DORA includes rigorous reporting requirements on firms' information communication technology (ICT) solution and service provider relationships, including third-, fourth- and fifth-party arrangements.

The concentration risk at a systemic level posed by industry over-reliance on a small number of cloud providers is front of mind for many regulators. In response to these concerns, many firms are considering or actively adopting a hybrid or multi-cloud failover set-up to ensure that the impact of outages by its third-party providers and related downtime is minimized for clients. High availability environments and strong governance and oversight arrangements are integral components of this approach.

Resilience and recovery strategies

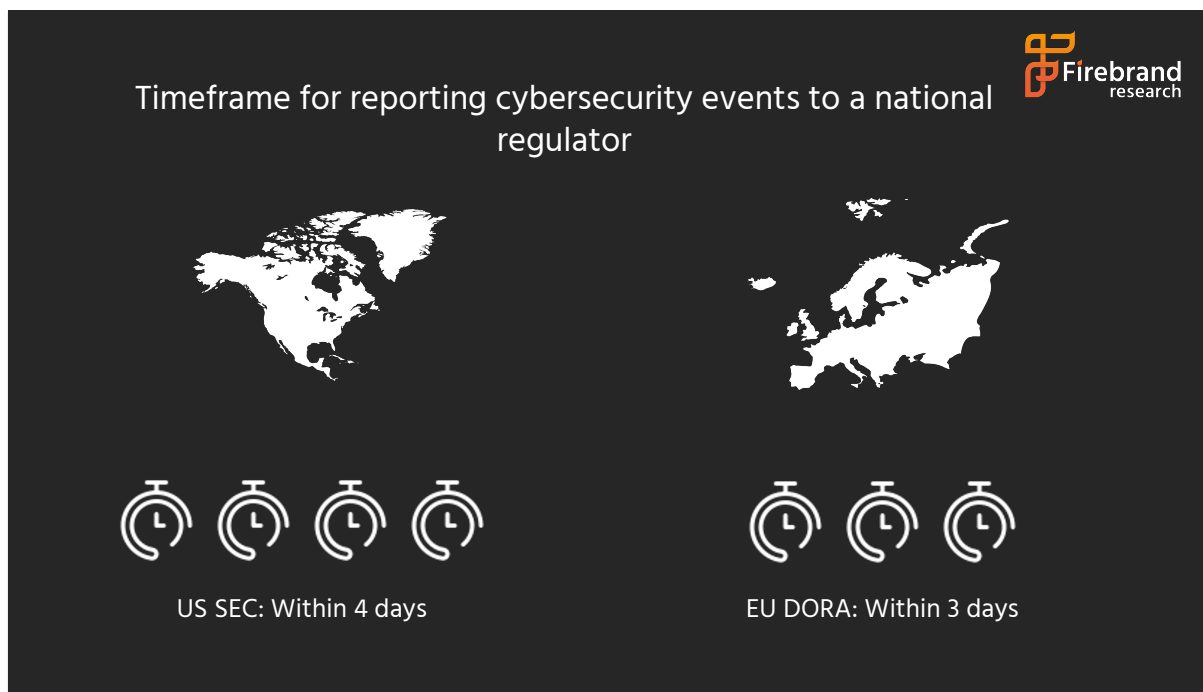
The assumption that a firm can build and rely on strong cybersecurity perimeters around its data alone is extremely outdated. Data rarely resides in one place and is shared across multiple technology environments, including legacy and next-generation platforms on-premises and in the cloud. Multiple lines of defense must therefore be

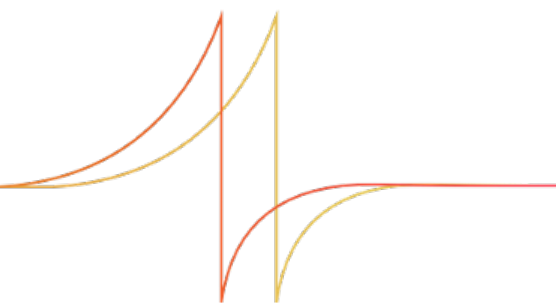
²[National Cybersecurity Strategy](#), March 2023, Biden Administration.



established across every environment and this entails a proactive approach to cybersecurity with zero trust strategies in place. Threat detection technologies have also evolved over the last few years and can be deployed effectively to identify any cyber breaches rapidly. Artificial intelligence-based monitoring tools are particularly helpful for chief information security officers that need support in their threat assessment tasks.

Data must be protected at all stages of its lifecycle and firms have to plan for the worst outcome. They need to assume that a cybersecurity breach can and will happen at some point, which means they need a plan to recover operations as quickly as possible. Regulatory obligations such as those within DORA to establish resolution and recovery plans for outages, whether caused by cybersecurity breaches or other operational errors, are targeted at improving these market practices. DORA and the US SEC requirements also provide timeframes within which financial institutions must report cyber-breaches (see graphic below).



A decorative graphic consisting of several thin, curved lines in shades of orange and red, extending from the right side of the page towards the center, creating a sense of movement and flow.


These tight timeframes for reporting place extra pressure on firms to add extra layers of governance and oversight to document the resolution and recovery process. However, the broader focus needs to be on coordinating a firm's people, processes and technology to analyze the attack, take the appropriate actions and report on the outcomes to the regulator. Regulators such as the SEC will be keen to understand the actions taken, particularly when it comes to dealing with ransom demands and recovering stolen data.

Though prevention is certainly better than a cure when it comes to cyber-attacks, firms must adapt to the inevitability of a successful cyber-attack impacting either their own institution or their assorted third-party providers. Therefore, preparation, planning and governance are the keys to future cybersecurity and operational resilience.

Key takeaways

The focus for financial institutions when considering data risk and operational resilience should be on the following:

- **Consistent investment in offensive and defensive strategies:** Firms need to stay ahead of the constantly evolving cyber-threat landscape by deploying best-of-breed tools for monitoring and assessment purposes. This may mean adapting existing capabilities as technology changes and newer tools become available to keep pace with cybercriminals' innovation.
- **Planning for recovery and resolution when an attack happens:** People, processes and technology are all the components of a successful recovery and resolution plan. Process governance and accountability must be established to ensure that should the worst happen, firms are able to return to operation as quickly and safely as possible.
- **Strong data access requirements and entitlements:** Making sure that regardless of wherever the data resides or moves to, it is only accessed by



individuals with the right permissions and entitlements. This includes cloud and hybrid cloud environments and on-premises-based data centers.

- **Keeping a good handle on external dependencies:** Internal and external dependencies must be assessed and any weaknesses must be addressed. The regulators are keen to see that firms have effective governance processes in place to resolve issues within their organizations and with their third-, fourth- and fifth-party providers. DORA mandates these activities and many other regulators are looking to adopt similar requirements.
- **Focusing on data immutability:** The need for advanced data protection and privacy will only increase over time, especially as financial institutions create and store more data.
- **Supporting rapid recovery via high availability environments and failovers:** Secure backup services for business continuity need to be readily available to lessen the impact of any cyber-related incidents.