IDC

SPOTLIGHT

Sponsored by: Capgemini

Reputational and regulatory risk of disruptions are driving the need for increased resiliency planning, necessitating a refresh approach to business, technology, operations, and cybersecurity.

Resiliency by Design: Strengthening Trust in Financial Services

April 2024

Written by: Dr Ashish Kakar, Research Director

I. Introduction

Financial services is a trust business and any disruption can impact confidence resulting in devastating repercussions for the organization, and financial stability within the ecosystem. Yet, developing trust is not easy in today's complex financial services environment. The financial services industry is evolving with rapid pace of technological advancements, increased frequency of regulatory updates, and changing customer expectations. Consequently, financial institutions need to possess a high degree of resilience.

Increasingly, we witness how a lack of resilience result in major disruptions, and some recent high-profile incidents illustrate this:

- The world's largest bank was subject to ransomware attack in November 2023 forcing it to resort to manual operations.
- A large equity trading platform with trillions of dollars of trade was subject to ransomware attack in January 2024.

Of the world's top 500 organizations that had been hit by ransomware, half of them (52%) paid off the attackers, IDC's Future of Enterprise Resiliency survey (November 2023) indicates. Yet, despite paying ransom, 20% of them were still unable to decrypt data.

The above disruptions may result from cyber-related incidents, but not all incidents are the result of cyberthreats. Consider the following recent cases:

- Two prominent Singapore-based banks witnessed prolonged downtime in their digital services. With Singapore going increasing cashless, many bank customers were left without funds to pay even for a train ride home.
- In February 2024, the link between datacenter and IT systems was impacted for Switzerland's second largest wealth management bank.

AT A GLANCE

Regulators are inclined to agree that the purview of operational resiliency is no longer limited to IT alone, but must rest with CXOs due to factors such as:

- Two-thirds of disruptions are caused by reasons other than a cyberattack.
- A third of outages are due purely to operational issues.
- The push for resiliency requires a new managerial framework.
- Management must recognize that disruptions are no longer a question of "if" but "when".

In each of these cases, there has been severe action by the board of directors and regulators, with them holding the CEO responsible. In one case, the CEO 's compensation was reduced by 30%, and in the other, the equity price fell by 1.1% in the aftermath of the disruption. In other instances, the CEOs were replaced.

II. Resilience defined

To understand the impact on the board, let us first understand the concept of resilience from a financial services perspective. The Basel Committee on Banking Supervision in 2021 defines operational resilience as the ability of banks to deliver critical operations through disruption. Robust operational resiliency enables a bank to identify and protect itself from threats and potential failures, and to adapt, recover, and learn from disruptive incidents to minimize their impact on the delivery of critical services.

The purpose of the Basel Committee is primarily to enhance financial stability in the banking sector by improving the quality of banking oversight. The committee's prioritization of operational resiliency was driven primarily by increased threats on financial services institutions, including the insurance sector and other allied services such as broking. The BASEL 3 regulatory framework was developed by the Bank for International Settlements to promote stability in the international financial system. BASEL 3 was initially implemented in January 2023 and will be progressively phased in over a span of 5 years.

Technology view of disruption

Financial services architectures have evolved from monolithic integrated software to microservices-led flexible architecture. Financial organizations often have a complex IT infrastructure, comprised of many endpoints, and interconnected and hybrid IT systems. This makes it hard for security teams to maintain visibility of their entire estate. Such flexible architectures increase vulnerability and provide opportunities for threat actors to disrupt the normal function of the banking industry.

Furthermore, advancements in technologies, such as quantum computing, could have a profound impact on the banking sector. Quantum computing is poised to potentially break conventional encryption techniques, significantly expanding the exposure to cyberattacks.

Regulatory view of disruption

Given the ramifications of a disruption on the financial ecosystem and its effect on customers in a digital age, regulators are increasingly making board of directors responsible for defining resiliency guidelines. The first major regulation stipulating this is the Digital Operational Resilience Act (DORA). DORA has been in effect since Jan 2023 and represents a contemporary European framework for the comprehensive management of digital risks within financial markets. This framework ensures that financial institutions maintain resilient operations even in the face of severe operational disruptions arising from cybersecurity and ICT issues. Security and resilience are now part of the board-level agenda, and board members have the responsibility to assign these overall priority.

Similarly, in recent cases in Asia, regulators in India, Singapore, Korea, and Australia to name a few, have held the executive team responsible for the downtimes.

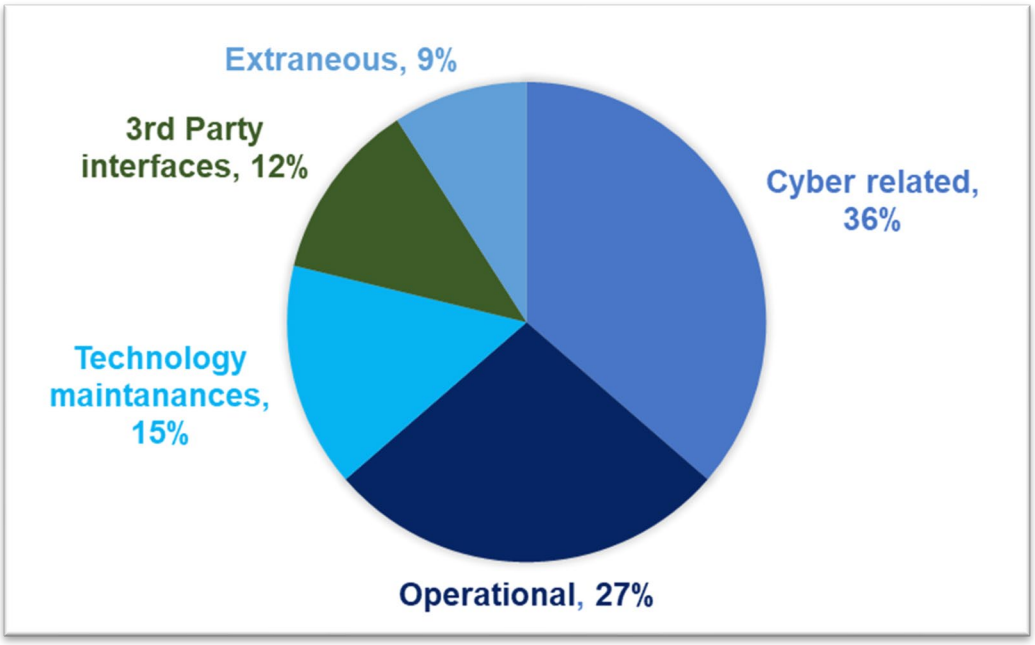
Given these realities, it is important to draw up a framework for financial services resiliency. But before we dive into the framework, let us first state the following on operational disruptions:

1. They are more frequent than most of us assume.
2. The pivotal paradigm shift is to adopt a "when" and not "if" approach to business continuity and disaster recovery planning. Rapid recovery is essential, and plans must be centered on the ability to recover quickly. Delayed recovery can lead to financial, reputational, and regulatory repercussions.
3. In this context, a strategic framework must be regularly monitored, tested, and updated to ensure it remains effective.

II. Disruptions come in all shapes, and causes

When looking at operational resiliency disruptions, it is often assumed that most of these stem from cybersecurity related issues. IDC studied a sample of 33 global disruptions between 2022 and 2023 to identify trends and the key causes of failure in the organization's operational resiliency plans. Looking at Figure 1, the contributing factors for outages are wide-ranging, and not limited to operational areas.

FIGURE 1: ***Reasons for downtimes***



Cyber-related outages constitute only about a third of the downtimes indicating to CXOs that investments in cybersecurity alone will not be sufficient in meeting a bank's operational resiliency requirements.

Source: IDC

- Cyber-related outages constituted only about a third of the downtimes indicating to CXOs that investments in cybersecurity alone will not be sufficient in meeting a bank's operational resiliency requirements.
- 27% of the disruptions resulted from operational procedures, and the rest from technology planning processes.
- In the area of technology planning, third-party interfaces proved to be a significant cause of disruptions, and often were the conduit used by hackers for cyberattacks.

Table 1 contains some examples of non-cyber-related disruptions to highlight the need for a holistic planning approach.

TABLE 1: ***Examples of non-cyber-related disruptions***

Operational	Technology maintenance	3rd party Interfaces	Extraneous
• Incomplete infrastructure testing processes led to failure during changes. • System misconfiguration led to database deletion.	• Architecture conversion disrupted 19 datacenters. • Incorrect maintenance implementation disrupted systems.	• 3rd party fund registry systems provided access to hackers. • APIs proved to be the conduit for hackers.	• Datacenter cooling not planned for high temperatures resulting from global warming.

Source: IDC

The data from these case studies also highlights the extent of the issue.

1. Data was affected or stolen in 27% of the cases.
2. The downtimes are ecosystem agnostic. In 42% of the cases, it was outsourced datacenters or cloud providers that were affected. In 58% of the cases, it was their own datacenters.
3. Government agencies or regulators were involved in 18% of the cases. A critical case involved an operational mistake at the New York Stock Exchange (NYSE) leading to significant valuation drops. One of the European regulators' websites was subject to digital denial of services (DDOS) attack.

Data was affected or stolen in 27% of the cases…. In 42% of the cases, it was outsourced datacenters or cloud providers that were affected. In 58% of the cases, it was their own datacenters.

The intensity of attacks is also increasing. IDC Cybersecurity Strategy Survey 2021 noted that annually,

1. almost 100% of the respondents found at least one case of malware; and
2. 3% of the respondents lost personally identifiable information, 5% lost significant intellectual property information, and 4% identified fraudulent transactions in their network resulting from some form of hacking.

These examples elucidate the fact that resiliency and disruption planning require specialized technical and operational skills. It can no longer be confined to an annual testing of business continuity.

III. Strategic framework: resiliency by design

While many regulators have suggested frameworks and there are global standards that partially address resiliency planning, these frameworks have market specific or partial process limitations. The following framework has been created to provide a holistic resiliency planning tool, inspired by the Basel Committee to develop a more global approach.

TABLE 2: ***Financial services resiliency framework***

Resiliency by Design

Given the significance of downtimes and its reputational, regulatory, customer, and financial impact, we recommend that board members adopt a holistic approach to resiliency that is termed "resiliency by design" as they lay out the guidelines for their resiliency policies. The policies should include people, process, and technology components, and must be proactive rather than reactive. The suggested approach would be:

- **Identify:** Identification of critical business services and their dependencies on people, processes, and technology
  - Analysis of the impact tolerance of services/systems through thorough testing and monitoring
  - Expression of resilience levels for each service/system and categorizing them based on the levels
  - Evaluation of their impact on customers and other stakeholders
  - Review of digital capabilities and define metrics for recovery (E.g., mean time between failures, mean time to repair, total hours of outages annually)
- **Adapt**: Implementation of adaptive technical resilience through innovative approaches
  - Secure cloud migration of legacy systems or create a backup infrastructure that includes resiliency
  - Implementation of a zero-trust architecture and comprehensive dependency mapping

- Utilization of sophisticated encryption methodologies to prevent unauthorized data access. This would include APIs as orphan APIs lead to vulnerabilities. Open-source software, if used, should be constantly upgraded to the current version
- Regularly test business continuity and disaster recovery plans
- Adequate preparedness for post-quantum cryptography

» **Adopt**: Establishment of a resilient organizational culture

- Implementation of effective business processes and robust reporting mechanisms
- Maintenance of an impactful resilience program with transparent practices and a forward-looking framework
- Articulation of clear objectives and expectations from bottom to top levels, with defined accountability
- Cultivation of a collective understanding that resilience is a shared responsibility

» **Collaborate**: Revitalization of cooperation with policymakers and ecosystem

- Collaborative efforts with the ecosystem to fortify resilience in response to various technological innovations
- Transition finance to stimulate investment in 'brown' infrastructure, coupled with transition plans aimed at expediting climate adaptation and mitigation financing

V. Benefits

Recent incidents such as banking downtimes in Singapore led to negative press and regulatory mandates. Every CXO would want to avoid these repercussions. The suggested framework provides a solution to robust resiliency planning helping to avoid these outcomes.

About the Analyst

Dr Ashish Kakar, *Research Director, IDC Financial Insights*

Based in Singapore, Ashish is the lead Financial Insights analyst responsible for all aspects of banking and insurance research. Ashish's own interest is in customer centricity, artificial intelligence (AI)/machine learning (ML) use cases in banking, retail banking, insurance, alternative investment management, digital and human interface, and credit and operational risk management.

MESSAGE FROM THE SPONSOR

Capgemini's 4R framework is a framework for analyzing industry trends and creating a strategic direction for financial institutions. At the core of the framework is Risk and Resilience, with the 3 other Rs corresponding to Regulation, Reformation, and Reinvention.

With rising concerns over cybersecurity, financial crime, and climate change, security, stability, and standardization will become pivotal to managing efficiency, resilience and mutualization for banking institutions. Zero-trust architecture, cryptography, threat intelligence, and advanced AI and analytics capabilities will enable banks to navigate the emerging risk landscape with resilience.

Capgemini also has a structured approach to analyze resilience applications and suggest corrective actions from pilot to scale. The IT Resiliency Framework involves analyzing the criticality and complexity of business and technology services, stage gates and assurance checks for architecture and design patterns, resiliency spectrum over data application and workforce, and, finally, the repeatability and scalability through a life-cycle approach. This helps in identifying and prioritizing critical business applications and interlinked technology services that need to be resilience tested.

The Capgemini Framework considers the different layers of resilience involving technical services and business functions by spanning over data and cyber resilience, workforce resilience, software resilience and enterprise business continuity management. It provides an accurate view of resilience across all different layers of the application stack including infrastructure and network, orchestration and integration, data and business logic, partners and connection, and interfaces and experience.

To find out more, contact: Sudir Pai, Chief Technology & Innovation Officer - Financial Services Global Business.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Asia/Pacific
83 Clemenceau Avenue
#17-01 UE Square, West Wing
Singapore 239920
T 65.6226.0330
Twitter @IDC
idc-insights-community.com
www.idc.com