THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

TECHNOLOGY

Data-driven operational resilience

THADI MURALI | REBECCA SMITH
SANDEEP VISHNU

20
YEAR ANNIVERSARY

OPERATIONAL RESILIENCE

#53 MAY 2021

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

OPERATIONS

TECHNOLOGY

MILITARY

DEAR READER,

Welcome to this landmark 20th anniversary edition of the Capco Institute Journal of Financial Transformation.

Launched in 2001, the Journal has followed and supported the transformative journey of the financial services industry over the first 20 years of this millennium – years that have seen significant and progressive shifts in the global economy, ecosystem, consumer behavior and society as a whole.

True to its mission of advancing the field of applied finance, the Journal has featured papers from over 25 Nobel Laureates and over 500 senior financial executives, regulators and distinguished academics, providing insight and thought leadership around a wealth of topics affecting financial services organizations.

I am hugely proud to celebrate this 20th anniversary with the 53rd edition of this Journal, focused on 'Operational Resilience'.

There has never been a more relevant time to focus on the theme of resilience which has become an organizational and regulatory priority. No organization has been left untouched by the events of the past couple of years including the global pandemic. We have seen that operational resilience needs to consider issues far beyond traditional business continuity planning and disaster recovery.

Also, the increasing pace of digitalization, the complexity and interconnectedness of the financial services industry, and the sophistication of cybercrime have made operational disruption more likely and the potential consequences more severe.

The papers in this edition highlight the importance of this topic and include lessons from the military, as well as technology perspectives. As ever, you can expect the highest caliber of research and practical guidance from our distinguished contributors. I hope that these contributions will catalyze your own thinking around how to build the resilience needed to operate in these challenging and disruptive times.

Thank you to all our contributors, in this edition and over the past 20 years, and thank you, our readership, for your continued support!

Lance Levy, **Capco CEO**

DATA-DRIVEN OPERATIONAL RESILIENCE

THADI MURALI | Managing Principal, Capco[1]
REBECCA SMITH | Principal Consultant, Capco
SANDEEP VISHNU | Partner, Capco

ABSTRACT

An organization's operational resilience efforts have traditionally focused on business process recovery and minimizing system downtime. This article posits that data, both transactional and contextual, is not only essential for resilience planning and avoiding peril but can also result in substantial investment savings. It presents three risk scenarios – catastrophic event, cybersecurity attack, and pandemic – to highlight the value of data classifications in determining the relevant elements of resilience. The article shows how taking a data-centered approach strengthens an organization's ability to plan, anticipate, detect, correct, and build a sustainable operational resilience culture.

1. INTRODUCTION

Operational resilience is the ability of a firm to deliver critical operations and services through disruption. This ability enables a firm to identify and protect itself from threats and potential failures, as well as respond, adapt, recover, and learn from disruptive events to minimize their impact on the delivery of critical services.

In an increasingly uncertain world, with the threat of catastrophic events, cyber attacks, or global pandemics, maintaining operational resilience is more important than ever. Traditionally, financial institutions have focused operational resilience or business continuity planning efforts on the recovery of essential processes or operations in the case of a disaster. While this approach takes into consideration the necessary people, processes, and technology involved in those essential operations, it often fails to fully address the role, relevance, and importance of the underlying data.

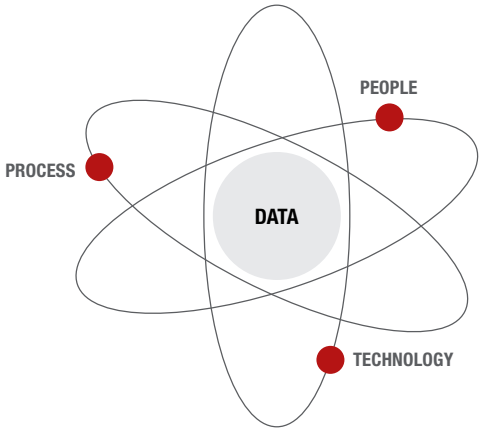
Business operations (people, process, technology) revolve around, and are reliant on, data (Figure 1). Consequently, understanding data flows is critical for defining the elements of resilience and in developing mechanisms to manage them. Business continuity and disaster recovery plans that do not effectively address data confidentiality, integrity, and availability during recovery, can put an organization at risk. Sustainable operational resilience cannot be achieved without a deep understanding of the interconnected nature of data and its potential risk impact on people, processes, and technologies. According to a Verizon data breach study [Verizon (2020)], following a major data disaster, 93 percent of companies without an effective data plan are out of business within one year. The following sections address how to examine, incorporate, and prioritize data to drive robust operational resilience.

2. WHY, WHEN, AND HOW TO INCORPORATE DATA AS PART OF OPERATIONAL RESILIENCE?

Managing data risk is complex, as data proliferates and flows throughout an organization. Data has rapidly become ubiquitous and covers every identity, entity, repository, and interaction, making it difficult to determine where to start or how to prioritize. A recent International Data Corp (IDC) report notes that the world's collective data will grow at a rate of 61 percent over the next few years, to reach 175 zettabytes by 2025 [Patrizio (2018)]. It is imperative, therefore, that organizations

[1] The authors gratefully acknowledge and sincerely thank Capco's Amanda Adaire and Tyler West for their diligent research, critical analysis, and content contribution.

Figure 1: Data is the nucleus



decide what information to collect and store based on business need, usability, and regulatory requirements, as the boundaries and parameters of resilience may eventually be defined by what data exists in the organization.

Data identification is an important first step in data lifecycle management, and includes determination of key data, along with the applications that use and store the data. A common misconception is that data classification is too time-consuming or complex. Although the initial classification does take some time, the periodic subsequent classification for new data does become easier. When one considers how the classification helps in simplifying and speeding data governance in general, or how it helps save costs in operational resilience plans, this effort is easily justified. While there are certain solutions in the market, including deep-learning tools, that identify and classify data at the point of creation, they still require significant manual participation. In many ways, technology solutions are better leveraged after the organization reaches a certain maturity in data management and classification.

The sheer abundance of data at most financial institutions may deem data classification overwhelming, but it does not have to be that way; this is truly a case of a journey of a thousand miles beginning with one step. It is important to start small and simple. The two important factors to consider when classifying data are criticality and sensitivity of data. This will become clearer as we apply them in the context of operational resilience.

Two key metrics for managing operational resilience are **"recovery time objective"** (RTO) and **"recovery point objective"** (RPO). Recovery time objective is best defined as the amount of time a business process or application can be down without causing significant damage to the business. Recovery point objective, on the other hand, refers to the amount of data that can be lost before significant negative business consequences are incurred.

Processes such as money transfer or payment transactions are very high frequency, hence even a few moments offline may represent thousands of dollars in lost revenue. On the other hand, processes such as HR-related functions, can be down for hours on a given day with less impact on the organization. In this example, money transfer or payment transactions have a low recovery time objective, meaning organizations need these processes re-operationalized in the shortest time possible. Processes with low required recovery time objective need to be the focus of continuity planning, and failover systems often need to be in place to mitigate against down-time for critical processes. When time is money, it is important for organizations to minimize time lost on high-revenue-earning processes.

Many students are likely, and unfortunately, familiar with nearly completing an important assignment only to have the computer crash before they could save their work. In many cases, hours of work are lost with no net benefit to the student. The same is true with financial organizations, except at a much larger scale. Systems can go down, data can be lost, and organizations can be negatively affected by that loss. As a teacher requests their students to save work as frequently as possible, organizations must determine how often to back up their important data as well. Business processes with

Figure 2: Overview of RPO and RTO

Table 1: Data criticality and sensitivity

TYPES OF DATA CLASSIFICATION	DEFINITION	SCENARIOS WHERE RELEVANT	IDENTIFICATION	EXAMPLES
CRITICALITY	Subset of data that is vital to the execution of organization's processes.	Availability scenarios, high-frequency processes, and high-priority processes for maintaining effective operations.	1) Examine the process to provide context, 2) determine criticality of the process, 3) identify the critical data required to run that process.	If the cash register is down, organizations may still be able to sell products, but cannot generate revenue – i.e., factors without which operations cannot continue.
SENSITIVITY	Subset of data that must be safeguarded with extra care due to legal, financial, or intellectual capital reasons.	Confidentiality and data loss prevention scenarios where there is a danger of internal and external threat of data misuse.	1) Understand the internal and external regulations around data (e.g., CCPA, SOX, privacy, intellectual capital), 2) categorize and handle data according to regulations.	Coca Cola's recipe is considered highly valued intellectual capital and guarded very carefully to prevent data misuse.

low recovery point objective, meaning that high amounts of data loss cannot be tolerated before they negatively impact the business, require more frequent backups to protect operational resilience. Recovery point objective measures data lost between the most recent backup and the time in which disaster occurred. If an organization backs up all or most of its data in regularly scheduled 24-hour increments, they can anticipate losing 24 hours of data in an absolute worst-case scenario. Some data, however, have more far-reaching implications if lost in even small amounts, and will need to be backed up more frequently to avoid extreme negative impacts to the business.

In an ideal world, organizations would deliver near-zero recovery point objective and recovery time objective. Even organizations with the deepest of pockets, however, cannot afford this for all applications, nor is it necessary. To achieve this, organizations would need zero failover applications across all systems, which in many cases is not feasible from a cost perspective. To optimize recovery point objective and recovery time objective, organizations must prioritize critical data when determining optimal backup frequencies across applications. If data is critical to supporting key business processes, backups for this data should occur more frequently.

Now that recovery point objective and recovery time objective have been introduced, and these metrics should be minimized to the greatest feasible extent, it is important to introduce the concepts of data criticality and sensitivity – two very important factors to consider when classifying data.

Data criticality reflects how vital data is to the organization's missions and processes. Data criticality can be thought of, and leveraged, as a measure to demonstrate that all data are not equal, and that some data are more important than others. Criticality always requires a context, which could be a process or function, a report, or a model. Once a business process is identified, the answer to the question, "What information is vital for the process to produce the desired output?" helps identify the critical data. As outlined in the introduction of recovery point objective and recovery time objective, no organization can reasonably afford to establish minute-by-minute backups on all systems, but must prioritize systems based on the criticality of underlying data.

Data sensitivity on the other hand, does not require a business process context. This refers to the subset of data that must be safe guarded with extra care due to one of the following reasons:

- **Legal/privacy:** regulatory requirements such as the Privacy Act, California Consumer Privacy Act (applicable to California residents only), and GDPR (Europe) define various types of data that must meet specific minimum levels of protection for the organization to be compliant and avoid fines or other regulatory repercussions. Examples include customer data, which falls into the category of personal identifiable information (PII), relating to social security numbers or credit card information.
- **Financial fraud:** this is data that has not been made public and materially informs a trading decision. All publicly traded institutions have data that is considered "material and non-public information" (MNPI). An example

of this is earnings or balance sheet items that are not yet known to public, but if a bad actor were to get hold of it, could purchase a related security. An interesting aspect of this information is the time context, meaning information that was considered material and non-public information before 10-K/10-Q release may not be considered so after that news has been made public.

- **Proprietary or intellectual capital related:** for financial institutions this is usually intellectual capital data or model related data that helps to measure market risks and credit risks. For example, certain board level reporting metrics, internal ratings, and scores on financial assets developed from proprietary models. In the retail industry, Coca Cola's drink recipe would be considered proprietary data and is safeguarded accordingly.

3. THREE SCENARIOS TO ILLUSTRATE HOW TO INCORPORATE DATA TO PROMOTE OPERATIONAL RESILIENCE

In a digital, interconnected world where financial institutions hold large amounts of legally sensitive, financially sensitive, and proprietary data, operational resilience is continuously tested and requires a data-centric strategy to protect, detect, and correct threats. Data threats can come from a wide range of internal and external parties, and these threats can affect an organization in a variety of ways.

To illustrate threat management, we examine three data-centric risk scenarios that an organization should consider in continuity planning and maintaining operational resilience:

1. **Catastrophic event scenario:** relates to weather-related catastrophic events, such as hurricanes, tornadoes, or earthquakes and terrorist-related disasters like 9/11. For example, Hurricane Sandy caused U.S.$74.8 billion in economic damage [Amadeo (2020)].
2. **Cybersecurity scenario:** refers to cyber-criminal attacks on an organization for the purpose of extracting customer data for financial gain. For example, the Equifax attack resulted in cyber criminals selling the personal data of 147.7 million customers in alternate markets [Ng (2018)].
3. **Pandemic scenario:** while different from the scenarios highlighted above, this is a relevant scenario to discuss, as the remote work solution related to the current pandemic has displaced employees to uncontrolled work environments, thereby making organizations more susceptible to inadvertent data loss and elevated risk.

In considering and preparing to maintain operational resiliency in these scenarios, it helps to examine the questions highlighted in Table 2[2]:

- What is the asset at risk?
- What are the threats to that asset?
- What is the intent of the actors?
- What are the implications if the threat is realized?

Table 2: Illustrative operational resilience risk scenarios

TYPES OF DATA CLASSIFICATION	WHAT IS THE ASSET AT RISK?	WHAT ARE THE THREATS TO THAT ASSET?	WHAT IS THE INTENT OF THE ACTORS?	WHAT ARE THE IMPLICATIONS IF THE THREAT IS REALIZED?
CATASTROPHIC EVENT	✓ **Information** ✓ **Infrastructure** ✓ Facilities	Natural disaster and terrorism: leading to a non-availability of data and systems, which halts business operations.	Natural disaster: non-malicious Terrorism: malicious	✓ Availability
CYBERSECURITY	✓ **Sensitive data** ✓ **Information** ✓ Infrastructure	Cyber criminal – leading to data loss.	Malicious	✓ Availability ✓ Confidentiality ✓ Integrity
PANDEMIC	✓ **Sensitive data** ✓ Information	Insider threat: including well-meaning insiders that inadvertently cause data loss due to alternative remote working model.	Non-malicious	✓ Confidentiality

* Bolded assets are the targets most at risk in each scenario

[2] Although there are multiple ways to define risk scenarios, we have found the risk scenario definition outlined by the FAIR methodology, developed by the FAIR Institute, to be the most comprehensive (https://www.fairinstitute.org/about).

3.1 Scenario 1: Catastrophic event scenario

Scenario recap
In the event of a disaster, information, infrastructure, and facilities are all at risk to non-malicious weather-related or malicious terrorist-related impacts. As a result of this scenario, data and systems are unavailable for an unforeseen period, halting business operations altogether due to a lack of data availability.

How can controls be implemented to mitigate risk?
Controls are focused on availability of various assets, including data.

Which classification criteria should be used?
Data criticality.

What is the value of considering data in this scenario?
Focusing on the right data will help reduce cost related to availability.

Since criticality needs a context, organizations will benefit from initially identifying the high priority, or critical, processes and operations, and then the underlying data required by these processes. High-priority processes are normally high-frequency transactional processes, which need to be operationalized immediately to prevent significant loss in revenue. Operationalizing data associated with lower priority business processes, such as HR databases used to onboard new employees, can occur later as they are not inherently associated with revenue generation and the ability of an organization to operate effectively in the short term.

Even with high-priority processes, only a subset of the information or applications may be required. For example, if payments are a high-priority process for an organization, the minimum data required to execute a payment is the payment amount and payee details. If the high-priority process is a 10K annual report, important data can relate to loan amounts, instead of customer or property details. This is the data that must be made available immediately. Identifying not only the critical business processes, but the critical data supporting those processes helps an organization plan and prioritize systems with the highest criticality, rather than focusing on non-essential data when time is of the essence and revenue is lost by the second. Once an organization has determined their high-priority processes and data, processes can be categorized according to those highlighted in Figure 3.

Prioritizing data using the aforementioned framework helps organizations focus their investments and implementation of controls. As previously mentioned, making all applications in an organization 100 percent failover safe to provide high availability is cost-prohibitive for even the largest of organizations. Prioritizing processes helps organizations focus their investments on highest-priority data and better manage cost.

Figure 3: Data criticality scoring criteria for prioritizing availability

3.2 Scenario 2: Cyber attack scenario

Scenario recap
In the event of a cyber attack, sensitive data and information are at risk to malicious cyber criminals. As a result of this scenario, data is lost and information confidentiality, as well as integrity, are impacted.

Which classification criteria should be used?
Data sensitivity.

How can controls be implemented to mitigate risk?
Controls focus on confidentiality, integrity, and availability.

What is the value of considering data in this scenario?
Focusing on the right data will help reduce costs related to security.

In the cybersecurity scenario, resilience includes data confidentiality, integrity, and availability. Legally sensitive customer information – names, addresses, phone numbers, employers, bank accounts, credit card information, and social security numbers – are the focus of cyber attacks, as individuals often use this information to process transactions under the guise of an affected customer. In the event of a cyber attack, organizations must prioritize the recovery point objective and recovery time objective by looking at data criticality, as in the catastrophic event scenario, to maintain data availability after an attack. Additionally, in a cybersecurity scenario, organizations must also focus on data sensitivity to prioritize data. Focusing on legally sensitive data will allow an organization to prioritize data that is most important and the likely target for breaches, potential theft, and misuse.

Cyber criminals use organized, advanced techniques to penetrate organizational systems to misuse data for their personal advantage. Cyber criminals pose a grave threat to operational and data resilience, as these attackers have malicious intent and experience with penetrating an organization's critical data assets. While cyber criminals intentionally threaten legally sensitive data, opportunistic insiders are a threat that organizations must consider as well. Opportunistic insiders have access to an organization's data assets and can have similar malicious intent to harm or exploit critical data. Opportunistic insiders may come in the form of disgruntled employees aiming to harm the organization through a cyber attack or individuals seeking personal gain at the expense of an organization. Regardless of their motive, their intent is the same: malicious. While the opportunistic insider's intent certainly makes them a threat, their ability to successfully orchestrate an attack is not as advanced as the cyber criminal. In preparing for a cyber attack, organizations must account for both cyber criminals and opportunistic insiders to minimize losses and impact to an organization's resilience.

Figure 4: Data sensitivity scoring criteria for prioritizing confidentiality

Identifying sensitive data is the first step, as this informs which assets or containers have these data and directs an organization's focus to protecting these assets or containers. These containers could be applications, databases, or file systems like LAN or SharePoint drives. Although identifying sensitive data is the first step, by itself, it is not a sufficient control. Additional factors must be considered, such as the location of the data, whether data is internet-facing or not, and whether the data is externally hosted or not. In many cases, internet-facing, and externally hosted data, are more vulnerable to attack. Figure 4 is an illustrative framework for classifying the sensitivity of data and guiding investment decisions based on the organization's risk tolerance.

Identifying sensitive data based on risk scenarios helps the organization focus its investments and build controls around the specific information assets that contain higher sensitivity. Organizations should develop a prioritization framework like the one highlighted in Figure 4, which examines data sensitivity and applications based on where they are located. More controls could be implemented based on the scoring criteria above – from 1 to 9, with 1 requiring a higher level of control. These controls may include security access (e.g., multi-factor authentication), as well as encryption at-rest and in-transit. Implementing effective, prioritized controls will help reduce the risk to sensitive data in an organization.

3.3 Scenario 3: Pandemic scenario

Scenario recap

In the event of a pandemic, sensitive data and information are at risk to non-malicious insiders. As a result of this scenario, data is lost due to inadvertent mishandling resulting from an alternative remote work model, which compromises the information integrity of an organization.

Which classification criteria should be used?

Data sensitivity.

How can controls be implemented to mitigate risk?

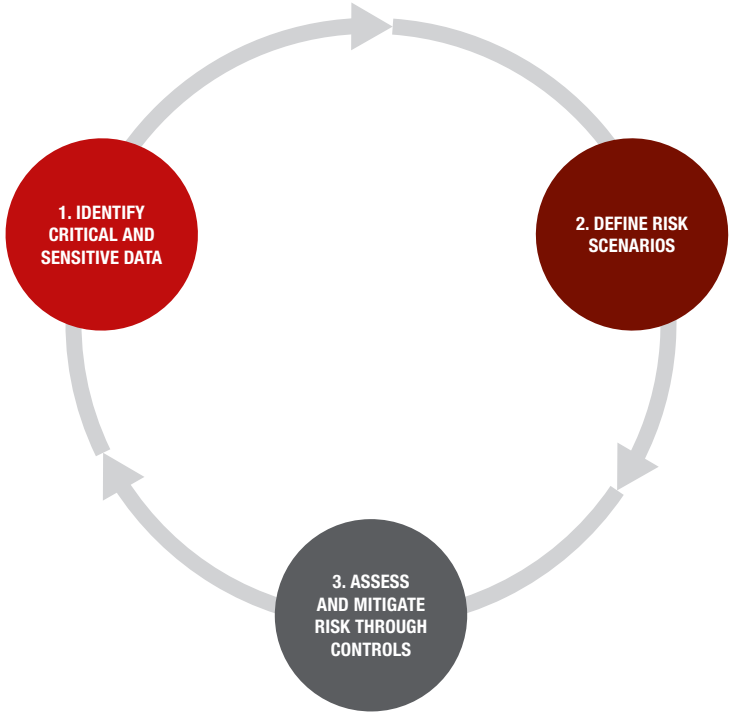
Controls are focused on confidentiality.

What is the value of considering data in this scenario?

Focusing on the right data will help prioritize personnel training efforts.

In the pandemic scenario, the focus is again on sensitive data, but the threat is now internal. Since data availability is not at risk, prioritizing data on recovery time objective and recovery point objective is not required here. In a remote and uncontrolled environment, an organization's well-intentioned, everyday employees are at risk of improperly mishandling data. In contrast to cyber criminals and opportunistic insiders, the prominent threats in a pandemic scenario have no malicious intent. The largest threats to an organization's

Figure 5: Data framework for managing operational risk



data during the pandemic are well-meaning insiders. While a well-meaning insider means no harm to an organization, their remote location presents an elevated risk for data mishandling. Whether a computer is left unlocked, private conversations are overheard, or proprietary data is sent to an inappropriate recipient, this information is at a greater risk of being accidentally and unknowingly exploited, or even destroyed, in an uncontrolled environment. Privileged insiders also present a great risk in the pandemic scenario. These individuals have greater access to sensitive proprietary data which, if mishandled, can present significant negative impact on an organization.

The sensitive data at risk in this case is also different from the sensitive data in the previous scenario. Employees, while working in an uncontrolled environment, may inadvertently leave their laptops unlocked or while speaking over a phone in an uncontrolled office let out proprietary or financially sensitive information. Even this unintentional compromise of data assets can create substantial loss.

4. DATA FRAMEWORK FOR SUSTAINABILITY

Figure 5 presents a data framework that focuses on three capabilities, which if developed by the organization, will not only help in operational resilience, but also in the overall management of information risk.

Since data is continuously changing in an organization and so are regulations, the framework can be part of a repeatable process with periodic reviews on data identification and classification, based on criticality and sensitivity. This may result in identifying new data that is sensitive because of new regulations. For example, data that is considered sensitive based on privacy laws are variable, as states have their own laws (e.g., California Consumer Privacy Act). Risk scenario libraries must be reviewed and updated as we learn of new threats. New scenarios emerge and must be factored in – for example, the pandemic scenario was largely ignored until recently, when it became a fast-moving reality and organizations had to rapidly adjust to a large shift in behavior.

The risk scenarios presented above help identify not only the data at risk, but the threats that have access to this data. Understanding the different risks presented by the above scenarios allows organizations to focus on at-risk data, employees, and institute controls to reduce the risk at hand (e.g., additional training to prevent inadvertent mishandling of data in the pandemic scenario).

This process of risk assessment and data classification must be repeated for new scenarios or changes to existing scenarios. In today's world of "big data", leveraging data classification and building risk scenarios around data will help businesses better manage risk, as well as drive value for organizations in their journey towards harnessing data as a source of competitive advantage.

5. CONCLUSION

Operational resilience is well expressed by the adage: "If you fail to prepare, you are preparing to fail." The key to operational resilience is planning, anticipating, preventing, detecting, and correcting – continuously! This planning to minimize disruption to business activities spans people, process, and technology, all of which are connected through data flows. Leveraging data helps build effective, efficient, and sustainable operational resilience, because it allows for differential handling of assets and provides a mechanism for continuous tuning and improvement.

Data-centric operational resilience manifests itself in determining control frameworks and activities. The three scenarios discussed above demonstrate the variation in controls based on the risk scenario and the classification of data. For the catastrophic event, the controls were directed towards data availability. For the cyber attack scenario, the controls covered data confidentiality, integrity, and availability. Lastly, for the pandemic scenario the controls were more directed towards confidentiality.

Figure A1: When to classify in the data lifecycle

APPENDIX

A.1 Top 7 activities to make an organization's operational resilience plan more data-centric:

1. Identify high priority processes
2. Classify data used by these processes based on criticality
3. Classify data in the organization based on sensitivity
4. Define disaster scenarios that place data at risk
5. Leverage classification in the scenario to classify data based on risk
6. Guide investment decisions based on classification
7. Repeat the process above on a periodic basis.

A.2 Operational resilience and data lifecycle management

The data lifecycle represents all the stages of data throughout its life from its creation or collection to its disposal. Data lifecycle management is not a specific product, but a comprehensive approach to managing an organization's data. It operates according to a policy-based system that manages the flow of information throughout its useful life across different applications, systems, databases, and storage media.

Operational resiliency challenges span the entire data life cycle, from creation through use and sharing, to eventual deletion. However, a critical stage for managing resiliency is the "collect" phase, in which data is identified and classified. Once the data is classified it informs the governance and controls not only for the "store" phase but all subsequent phases namely "share" and "purge".

REFERENCES

Amadeo, K., 2020, "Hurricane Sandy facts, damage and economic impact," The Balance, December 29, https://bit.ly/3r6iMqG

Ng, A., 2018, "How the Equifax hack happened, and what still needs to be done," CNet, September 7, https://cnet.co/3dVi2Rv

Patrizio, A., 2018, "IDC: expect 175 zettabytes of data worldwide by 2025," NetworkWorld, December 3, https://bit.ly/3kyJq9o

Verizon, 2020, "2020 data breach investigations report," https://vz.to/2MButXu

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO