Technology and Operational Resilience

Building capabilities to give you confidence in recovery

pwc

PwC provides organizations with the ability to protect and sustain core business functions when experiencing a state of disruption to technology, infrastructure, or operational processes supporting mission-critical business services.

As the evolving threat landscape, pandemics, climate events, and geopolitical events create uncertainty and exposure, organizations require technology-enabled resilience plans and tools to understand their enterprise-wide resilience posture and shore up their ability to quickly recover from a disruption.

Mission assurance

Understand at-risk systems and dependencies that could be impacted during downtime

Operational sustainment

Recover operations quickly in a non-compromised environment through robust recovery strategies

Financial stability

Prevent financial losses due to downtime and reputational damage

Compliance

Meet legal and regulatory requirements

Strategic alignment

Establish an integrated view of security and resilience based on risk

Workforce flexibility

Develop staffing plans to redeploy workforce during a disruption

The impact of a disruption can be costly

Many organizations have created some level of resilience, but have not adequately tested their resistance to disruptions. According to PwC's Global Digital Trusts Insights 2021 survey, 40% of executives plan to increase resilience testing to ensure that, their critical business functions will stay up and running.

A disruption can create an array of impacts on your company:

- Operational impacts can create an inability to maintain your business operations.
- Legal and regulatory impacts can lead to a breach in compliance.
- Financial impacts can result in lost sales and market share.
- Reputational impacts can cause customer dissatisfaction and loss.
- Health and safety impacts can affect the lives of your employees and customers.

Real examples of the impact of a disruption

The lack of resilience puts business operations at risk and can generate negative financial impact in the form of lost sales, brand dilution, PR/Legal battles, penalties and more.

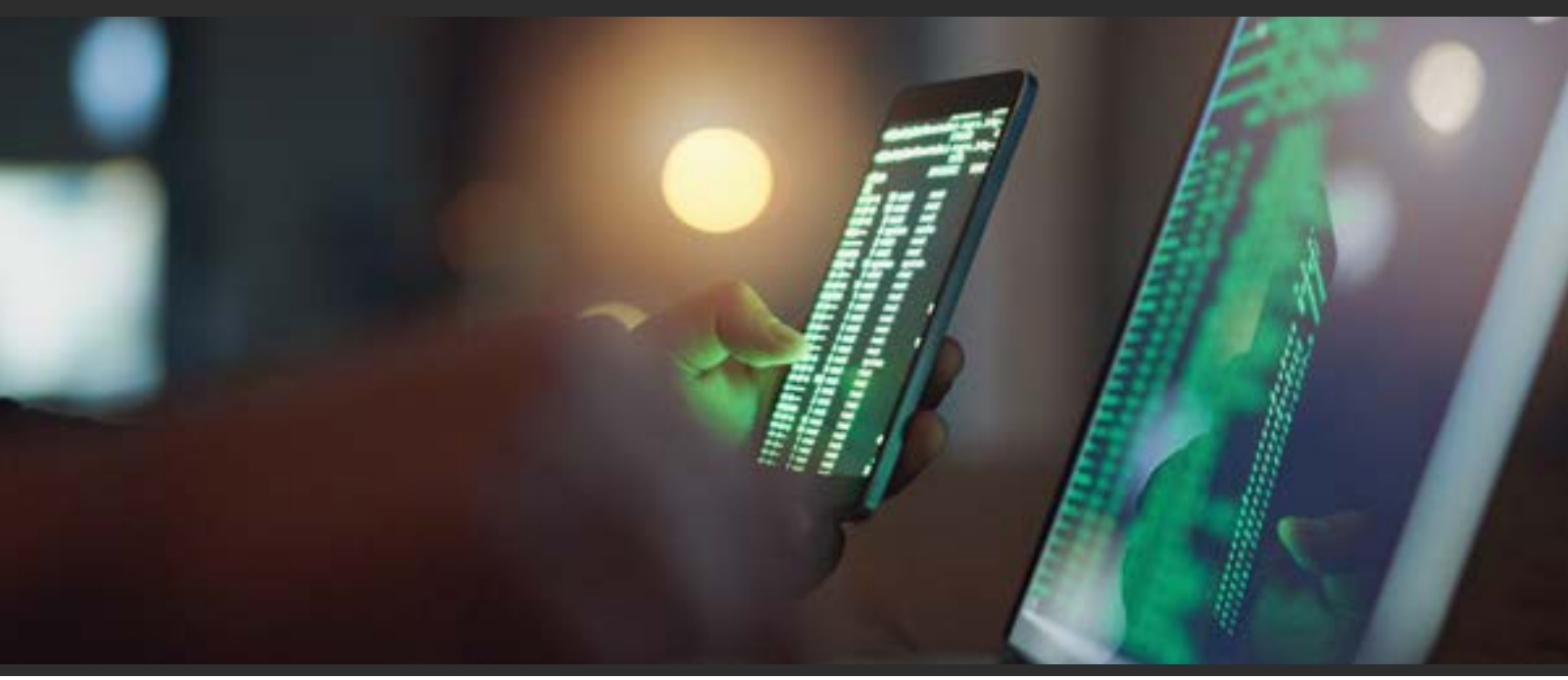
Many organizations are insufficiently prepared for disruptions

According to our Global Digital Trusts Insights 2021 survey, many companies foresee disruptive events in their future and fear a negative impact if these occur. While disruptions can occur from a variety of event types, the predominant source of disruption today stems from cyber threats and the likelihood of a cyberattack is greater than ever before. As digitization increases, so have intrusions, ransomware, and data breaches, along with an increase in phishing attempts.

55% say it's likely or very likely that their **cloud service provider will be threatened** in the next year

57% deem an **attack on cloud services to be likely**

56% rate a **ransomware attack likely** or very likely over the next year



Technology and operational resilience

PwC provides a resilience model that can help companies by prioritizing operational continuity through:

- Developing a broad understanding of current and emerging corporate risk scenarios
- Prioritizing data availability and integrity, during and after a disruptive event, with a focus on maintaining confidentiality
- Evolving prioritizing customers and maintaining continuity of operations through anticipated risks during business continuity planning
- Determining the appropriate levels of recovering in alignment with strategic business imperatives

Key differentiators of our integrated solution include:

1. **An integrated approach to resilience**—We leverage experience across the firm to help provide decision makers with the ability to assess and increase an organization's resilience posture—from business continuity and business impact intelligence, to responding to critical disruptions.

2. **Industry-specific insights and solutions**—We have a unique cross-industry view of the challenges and solutions needed for resilience in various sectors. With an effective combination of technical and industry experience, we tailor our resilience perspective to the company we're working with and the drivers that can influence their business. PwC offers specific resilience solutions for Financial Services, Retail, Healthcare, Technology, Media and Telecom, and Manufacturing.

3. **Resilience framework**—Our approach to resilience focuses on four key stages that are essential in developing and maintaining a resilient enterprise. PwC's custom, industry-agnostic resilience framework addresses each of these components across people, process and technology elements.

4. **Technology enablement**—Our technology enablers leverage the latest and greatest technology to create better outcomes for our clients. We are committed to continuously developing new and innovative solutions for enabling technology and operational resilience, driven by evolving guidance from various regulators.

Some examples of our solutions include:

Dependency mapping—Our dependency mapping platform, Terrain Insights, a PwC product, provides real-time, up-to-date visibility into an organization's enterprise-wide mission critical assets and its related secondary and tertiary dependencies, which is critical for building and maintaining a resilient organization.

Crisis & Event Management—Our purpose-built console Ready Command deploys with speed and provides a trusted, centralized management system in the heat of a fast-paced event. Set up governance, roles and responsibilities, workstream and specific tasks—then monitor and report on progress in near-real time. This suite of technology-enabled services and products is customizable to fit your business needs.

Metrics and dashboard development—Our resilience metrics allow companies to track and manage their resilience risk and understand their recovery capabilities in the event of a significant disruption. Custom metrics and dashboarding provide visibility across functions, enabling strategic alignment across resilience risk management efforts.

Financial institution

Scenario—A **financial institution** experienced a natural disaster that caused a wide scale data center outage. The institution was not able to rapidly restore services, which led to the issuance of a Matter Requiring Attention (MRA) from regulators.

Approach—PwC can help by defining a target state for the institution's Technology and Operational Resilience program. Our team would conduct a gap analysis to identify the gaps between the current and desired state of maturity. The roadmap would consist of a multi-phased approach to achieve target state capabilities for resiliency in alignment with the existing enterprise Business Resilience and Disaster Recovery Program.

Impact:

- The institution is able to implement a strategy for **increasing their resilience capabilities** and **meeting regulatory guidance**.
- The institution can promptly **respond to the regulators** and show the commitment the organization was putting behind **growing their resilience capabilities**.

National gas and convenience retailer

Scenario—A **national gas and convenience retailer** wanted to improve its resilience capabilities to help minimize impacts to its business and operations in the event of a major disruption.

Approach—PwC's Technology & Operational Resilience Framework, coupled with PwC's Disaster Recovery framework, enables PwC to provide a technical perspective for the retailer's wider resilience efforts. PwC can create a resilience strategy and a prioritized roadmap for establishing a formal, holistic resilience program, aligning current and future initiatives, and integrating cross-functional teams/activities throughout the enterprise.

Impact:

- PwC can help the retailer **establish a resilience strategy and prioritized roadmap** to help successfully execute a resilience program.
- A formal approach is developed to **define RPOs/RTOs** for each retailer system and **enhance understanding** of how these recovery objectives are integrated into backup and disaster recovery requirements.

National pharmaceutical retailer

Scenario—A **national pharmaceutical retailer** needs help reviewing the organization's ongoing COVID-19 response as well as assessing the current maturity level of their crisis management program.

Approach—Leveraging PwC's Crisis Preparedness Assessment and Ready Command solutions, PwC can help identify opportunities to improve the maturity level of the retailer's crisis management program and implement those solutions. This opens up opportunities to collaborate with the retailer to further develop our Ready Command solutions, so that we can take them to market as a suite of technology-enabled services and products for crisis and incident management.

Impact:

- PwC can help the retailer achieve **increased maturity** of the crisis management program and an enhanced **ability to react and respond to disruption** through improvement of program governance and development of response plans.
- The PwC Ready Command solution will be leveraged as the **main crisis and incident management suite** for the organization.

Access to thought leadership

PwC's Cyber & Privacy Innovation Institute is your place to access real-time insights on key business priorities around cybersecurity, privacy, and forensics. The Institute brings together the collective experience of cyber professionals and subject matter specialists through executive research and perspectives on trends. From the Institute, you can access the latest thought leadership from industry associations and the academic community, alliances and ecosystems and global research firms.

Check out PwC's latest thought leadership:

- Global Digital Trust Insights Survey 2021
- Global Crisis Survey 2021: US Insights and Actions
- US Digital Trust Insights Snapshot Survey (www.pwc.com/usdti)

Contact us

Gerry Stellatos
Incident Response Leader, PwC US
(202) 420-1982 | gerry.stellatos@pwc.com

Shawn Lonergan
Director, Cybersecurity, Privacy & Forensics
(917) 683-9049 | shawn.lonergan@pwc.com