Building resilience for severe but plausible scenarios

August 2024

pwc

The recent IT outage that sent shockwaves through global enterprises underscores a fundamental truth: the digital age, while transformative, is fraught with risks that can disrupt even the most well-prepared organisations. July's incident, which reverberated across various sectors, highlighted the imperative for robust resilience strategies and transparency in communication.

The Inevitable Adversity

In an interconnected world, where cybersecurity measures like Endpoint Detection and Response (EDR) systems have become a staple, the paradox of protection is evident: a system, designed to fortify defences, inadvertently triggered widespread outages. This incident is a stark reminder that resilience must go beyond individual solutions and encompass an enterprise-wide approach to safeguard critical assets. What is needed is a truly enterprise-wide approach to resilience to protect what matters most.

As organisations complete their recovery and undertake post-incident reviews, we share our view and recommended actions for any organisation seeking to enhance its resilience.

Post-Incident Reflections: A Technology Perspective

Across all sectors, technical changes—from simple maintenance to major implementations—are the primary cause of IT incidents, often disabling resilience measures such as redundancies and failover capabilities.

Organisations' increasingly complex and integrated technology environments, which rely on numerous third-party services, make understanding service interactions challenging and consequently require rigorous control to avoid outages. If change management is not sufficiently rigorous, this leads to increased outage risks. Recent IT incidents show that even minor changes can cause major disruptions.

From a wider resilience and recovery preparedness perspective organisations need to prepare and test for major incidents that inflict more damage to their technical environment without which recovery is not certain. A successful Cyber ransomware attack presents responders with far a more severe challenge as it often destroys the host environment, making the road of recovery from a compromised backup slower and more complicated. Lessons from Cyber Recovery have a key role to play in guiding secure recovery from accidental IT disruption.

Actions for CIOs and CISOs

1. Understand critical business service interactions, dependencies on enabling services and identify those that can disable the organisation if they fail. Place specific change guardrails on enabling services, particularly central Cyber tools.
2. Review and uplift change management processes, associated tooling and testing regimes.
3. Review and update incident management and cyber recovery processes alongside your security function.

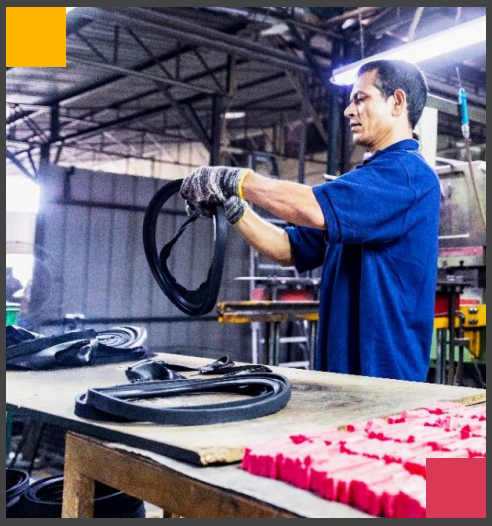
Operational Resilience: A Holistic View

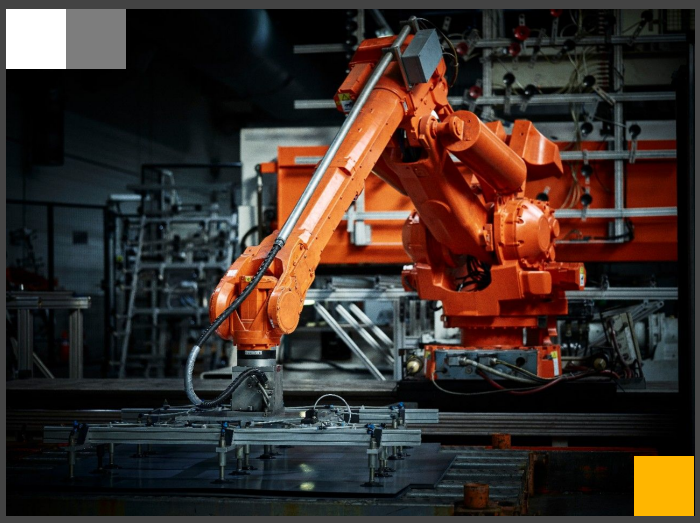
Preventative controls are essential, but organisations must also prepare for inevitable disruption by planning for severe yet plausible scenarios. The complexity of modern enterprises, with their myriad dependencies and 'black box' technologies, often hinders effective business continuity planning. True resilience necessitates an end-to-end understanding of service delivery, beyond functional silos.

Understanding the end-to-end delivery of critical business services is challenging but essential. Organisations that have done this planning would have been able to quickly absorb the disruption from the IT outage switching to tested workarounds resulting in minimal impact.

Tracking in real-time requires technology. Tech-powered dashboards enable executives to visualise different interdependent operations—and prioritise actions when faced with disruption.

Those with resilience technology platforms are more able to identify the outage and invoke recovery strategies that minimise its impact based on tolerances set by management.





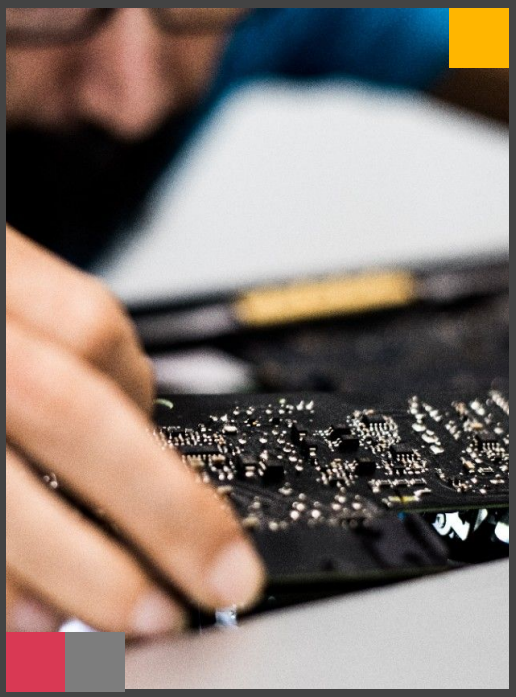
Actions for CEOs and COOs

1. Consider your resilience maturity and how this is reported to the Board.
2. Develop a cross-functional resilience program aligned with organisational strategy and priorities.
3. Implement technology-driven dashboards for real-time monitoring and response prioritisation.
4. Define how your organisation determines whether a service is critical, map those critical business services, their dependencies (third parties, tech, assets, sites, people), agree impact tolerances through a stakeholder lens and workarounds to minimise impact.
5. Set Key Resilience Indicators (KRIs) and exercise plausible, severe scenarios and bring third parties together to ensure response efforts all focus on critical business services.
6. Identify and stress test contingency plans for loss of critical business services in various scenarios.

Digital Supply Chain Vulnerabilities

The outage underscores the critical need for enhanced collaboration between Third Party Risk Management (TPRM), IT, and service owners. TPRM professionals need to work closely with IT to better understand digitisation, product development, and the technology architecture that underpins critical business services - an EDR provider needs to be listed as a critical resource.

The digital supply chain, with its inherent complexity and opacity, poses significant resilience challenges. Organisations must adopt a ‘resilience by design’ approach, emphasising comprehensive understanding and proactive management of third-party dependencies.



Actions for COO

1. Map supply chains to show service delivery and third-party interactions.
2. Conduct rigorous risk assessments and collaborative exercises with critical suppliers.
3. Stress-test contingency plans to ensure robust response capabilities.
4. Conduct joint exercises, war games and / or scenario tests with critical third parties to embed and rehearse a joined up response capability, and identify vulnerabilities which may impact critical service provision in the event of future outages.

Effective Crisis Response

A well-coordinated response to IT disruptions extends beyond IT teams, requiring organisational alignment and strategic decision-making. In this outage, the Blue Screen of Death forced some crisis teams to stand up their ‘out of band’ communication tools to help them assess and respond to the situation. An effective crisis response would have required planning and the rehearsal of defined roles, responsibilities, and communication strategies. Those who responded well recognised that this crisis presented an opportunity to demonstrate resilience and accountability.

Effective crisis-management skills are developed through frequent exposure to the characteristics, pressures, and demands faced when disruption occurs. Leaders need to continue developing relevant skills, mindsets, and behaviours though tech-based microsimulations or simple scenario-planning discussions.

Finally, it is vital that there is a clear understanding of the contractual frameworks that an organisation operates under and, critically, where they are protected when things do go wrong. Organisations need to ensure they are assimilating the precise data and information from the start of a response and through to recovery to support a credible and evidenced claim for any compensation—whether that is under service level commitments or under business insurance policies. Whilst businesses can’t just rely on insurance as their only mitigation, many organisations won’t have tested the breadth and limits of coverage they have against scenarios like this.

Actions for Heads of Resilience

1. Review and refine response structures based on recent outages.
2. Conduct comprehensive crisis exercises to validate and enhance response frameworks.
3. Review and ensure you understand how your insurance will respond to situations like the recent outage.

Critical Questions for the Executive Team

1. Do we know how resilient our organisation is to unforeseen disruptions, including IT system failures and third-party dependencies?
2. Have we considered global best practices on sound operational resilience?
3. Are our change management procedures sufficiently robust?
4. Have we tested our response capabilities for severe but plausible scenarios?
5. Are we investing in making the most critical parts of our business resilient?
6. How are we using technology to identify and monitor our vulnerabilities?
7. Do we have a clear understanding of our contractual protections, including the role of insurance?

Conclusion

This IT outage event only reaffirms that evolving risk landscapes necessitate a transformative approach to enterprise resilience. By addressing vulnerabilities, leveraging opportunities and preparing for severe but plausible events, enterprises can not only withstand disruptions but thrive despite them.

Contact us:

Kumar Tulsi
Partner, Third Party Risk Management & Resilience
+27 (0) 83 452 5763
kumar.tulsi@pwc.com

Veeran Laloo
Partner, Transformation Confidence & Resilience
+27 (0) 72 086 7291
veeran.laloo@pwc.com

Jacques Muller
Partner, Africa Risk & Regulation Leader
+27 (0) 72 900 0161
jacques.muller@pwc.com

Hamil Boora
Partner, PwC Africa Cybersecurity Leader
+27 (0) 72 388 4444
hamil.bhoora@pwc.com

Hennie Jansen van Rensburg
Partner, IT & Data Risk
+27 (0) 83 269 6525
hendrik.jansen.van.rensburg@pwc.com

Gerhard Rossouw
Partner, IT Risk & Third Party Assurance
+27 (0) 79 883 6573
gerhard.rossouw@pwc.com

Kerin Wood
Partner, Crisis Response & Compliance
+27 (0) 84 42 00009
kerin.wood@pwc.com

Trevor Hills
Partner, PwC Southern Africa Forensics Leader & Cyber Incident Response Management
+27 (0) 79 599 4677
trevor.hills@pwc.com