Building resilience for severe but plausible scenarios

July 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. Last week'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. It underscores the need for 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 Technological Perspective

Technical disruptions, whether from routine maintenance or significant upgrades, remain a predominant cause of IT incidents. The complexity of modern technology environments, compounded by a lack of comprehensive end-to-end oversight, often exacerbates these issues. Redundancies and failover mechanisms, while crucial, can be rendered ineffective if not properly integrated and understood.

The intricate web of dependencies within an organisation's digital ecosystem—spanning third-party services, integrated systems, and critical interdependencies—demands rigorous change management and resilient planning. The recent outage, while disruptive, demonstrated the efficacy of coordinated recovery efforts. However, the spectre of cyber threats, such as ransomware attack, still looms large, necessitating robust cyber recovery planning.

Cyber threats, such as a successful ransomware attack, present responders with far a more severe - but not dissimilar challenge. An attack which corrupts data, compromises accounts and the infrastructure they administer, disrupts communication channels, and triggers distrust over integrity of 'safe' backups is deliberately challenging to resolve. Lessons from Cyber Recovery have a key role to play in guiding secure recovery from accidental IT disruption.

Actions for CIOs and CISOs

1. Maintain a dynamic understanding of critical business service interactions and dependencies.
2. Fortify change management processes with stringent testing and risk assessment protocols.
3. Enhance incident and cyber recovery processes to ensure a seamless coordination and effective response.

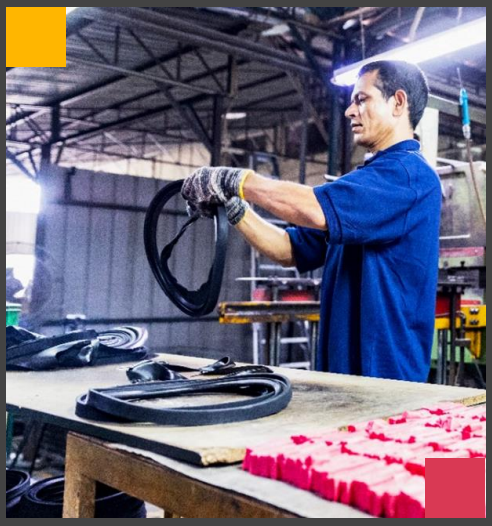
Operational Resilience: A Holistic View

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 would have been able to easily establish the impact, invoking recovery strategies in order that the impact of the outage remained in the tolerances set by management.



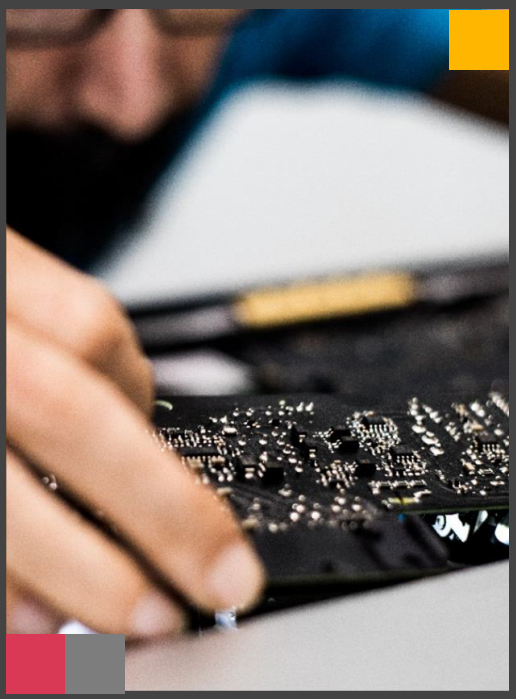
Actions for CEOs and COOs

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.

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 this.

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.

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. Are our change management procedures sufficiently robust?
3. Have we tested our response capabilities for severe but plausible scenarios?
4. Are we investing in making the most critical parts of our business resilient?
5. How are we using technology to identify and monitor our vulnerabilities?
6. Do we have a clear understanding of our contractual protections, including the role of insurance?

Conclusion

This IT outage event only reconfirms 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 amidst them.

Contact us:

Uthman Mayanja
Country Senior Partner
PwC Uganda
uthman.mayanja@pwc.com

Peter Ojekunle
Senior Manager
Consulting & Risk Services
PwC Uganda
peter.s.ojekunle@pwc.com

Patrick Matu
Associate Director - Deals
PwC Uganda
patrick.k.matu@pwc.com

Hilda Kamugisha
Manager
Legal Business Solutions
PwC Uganda
hilda.Kamugisha@pwc.com