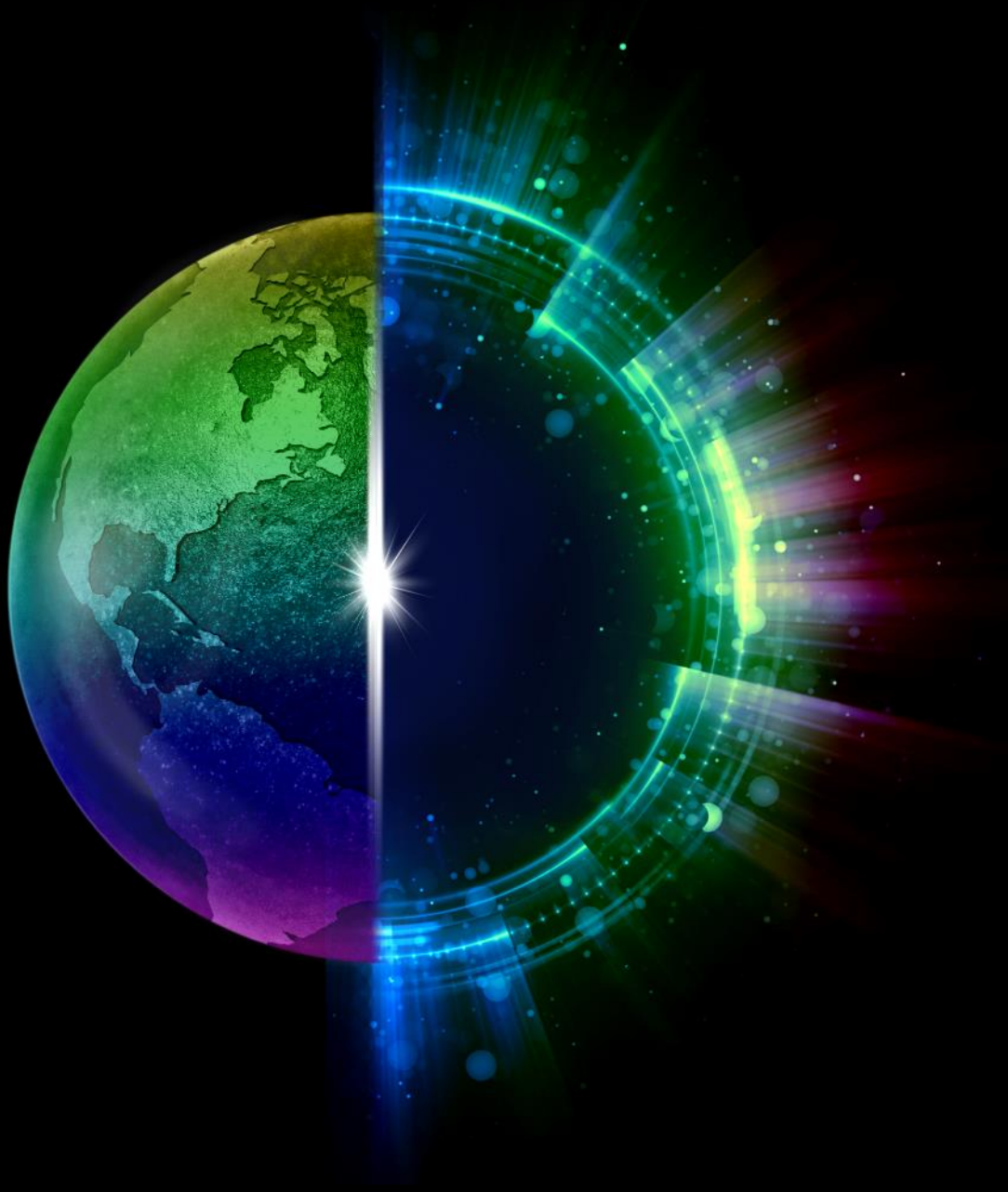
Deloitte.



Digital Resilience and Enterprise Recovery:
Would your business survive a catastrophic cyber attack?

2023

Against a backdrop of increasingly common and impactful cyber incidents, a frequently asked question by the board, regulators, shareholders and customers is "could our business recover from a catastrophic cyber attack?".

In many organisations, resilience capabilities remain siloed. Elevating resilience to a strategic, enterprise-wide issue will foster the attention and funding that it now warrants.

This whitepaper will analyse why digital resilience is so important and will demonstrate what a cyber attack looks like and how it feels in real time. We will explore the common weaknesses that consistently exacerbate these incidents and the challenges that organisations face during recovery, enabling you to better understand, and increase, your ability to recover your business if the worst was to happen.

What is Digital Resilience and Enterprise Recovery?

Organisational Resilience is the capability of an organisation to be prepared for disruption and to adapt in a changing environment.

Digital Resilience is a key element of Organisation Resilience. It is building the capacity for **agility, adaptation and restoration** in order to deal with complex and severe cyber events[1].

Enterprise Recovery refers to an organisation's **ability to respond to**, and **recover from, catastrophic cyber attacks.**

What is a catastrophic cyber attack?

A **catastrophic cyber attack** is one that impacts an entire enterprise and can be a **near extinction-level** event.

These attacks will present significant and wide-spreading impacts, including **financial, operational, reputational and legal**.

Catastrophic cyber attacks are extremely severe but plausible cyber events and are often caused by **ransomware**.

[1] Deloitte's Global Resilience Report Key findings from Deloitte's 2022 Global Resilience Survey

Why is this important?

Common drivers and trends are putting Digital Resilience and Enterprise Recovery on the agenda.

External Developments — The threat landscape continues to evolve. Attackers are becoming more organised and networked, and attacks are becoming increasingly indiscriminate.

- **Networks of attackers:** these are highly skilled and well resourced groups; no longer standalone, isolated individuals.
- **Attackers motives have changed:** there is a focus on gaining profit from extensive, long-lasting disruption, with all industries now a potential target.
- **Targeting immature industries:** money can be made from traditionally untargeted industries with lower cyber maturity.
- **Collateral damage:** the rise in indiscriminate attacks through supply chains has meant organisations do not need to be specifically targeted to be a victim of a cyber incident.
- **Ransomware:** to maximise profits and disruption, attackers are frequently using ransomware as the means to attack organisations.

+

Organisational Changes — There is a demand from businesses to adopt and embrace new technologies, but this increased reliance on technology has inadvertently created vulnerabilities.

Drivers	Vulnerabilities
Building connections as a business to facilitate **data sharing** and availability.	Data is nearly always 'on network', leaving it **susceptible to attack.**
Demand to adopt **new technologies** to generate advantages and insights.	Security and protection is an after thought, creating **new vulnerabilities.**
Shifts in the way we work.	**Increased attack surface** available for attackers to exploit.

Every industry is now a potential target for catastrophic attacks

Attackers becoming more sophisticated, coupled with growing digitalisation of businesses, have increased the likelihood that any industry could be targeted, or be an unintended victim.

Ransomware trends and statistics:

$40 million

Largest publicly reported ransomware payment to date[2].

66%

Percentage of organisations that were hit by ransomware[3].

90%

Percentage of ransomware hit organisations whose ability to operate was impacted[3].

$265 billion

Expected global cost of ransomware by 2031[4].

[2] Bloomberg CNA Financial Paid $40 Million in Ransom
[3] Sophos State of Ransomware 2022
[4] Cybercrime Magazine Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031

What does a catastrophic cyber attack feel like?

A catastrophic cyber attack will impact the entire enterprise, causing disruption that puts the business into survival mode.

Organisations experience the impacts and consequences[5] of catastrophic cyber incidents in multiple areas:

- Operational and Production
- Financial and Contractual
- Regulatory and Compliance
- Data and Intellectual Property
- Communication and Reputation

Immediate Impacts

Through our **Cyber Incident Response (CIR) experiences,** we have witnessed organisations suffer the **following impacts in the immediate aftermath of an incident.**

These were observed through Deloitte's experiences when responding to incidents between 2017-2022

- Critical business processes halted.
- Financial systems unavailable.
- Critical business systems offline.
- Intellectual Property (IP) leaked.
- Immediate legal and regulatory reporting required.
- Critical data compromised or destroyed.
- Public confidence and brand equity impacted.
- Critical infrastructure services impacted.
- Internal communication platforms down.

Lasting Consequences

The consequences of an incident will exist beyond the immediate impacts, affecting the organisation across their **entire value chain.**

These were observed through Deloitte's experiences when responding to incidents between 2017-2022

- Interruptions to supply chains.
- Critical equipment irreparably damaged.
- Regulatory action and fines.
- Key licences and permits to operate revoked.
- Extensive financial costs to recover.
- Failure to meet demand and contracts.
- Unable to contact employees, clients or stakeholders.
- Damage to client trust and reputation.
- Critical data destroyed and needs to be reconstituted.

[5] Deloitte Global Future of Cyber Survey 2023 Consequences resulting from cyber incidents and wider business impacts

What are the common weaknesses in these incidents?

There are common weaknesses that consistently exacerbate these incidents and cause them to be so impactful.

Inadequate controls and insecure networks enable access, movement, persistence and eventually catastrophic impacts. There are several weaknesses that **mean organisations cannot contain these attacks**, causing them to be catastrophic incidents in nature.

A "flat network"

A **flat network** can allow an attacker to **move freely across the network**. An attack from anywhere on the network can put the entire network at risk.

Weak authentication factors

Not enabling the right authentication factors where necessary makes it easier for an attacker to **compromise your network.**

Insufficient privileged access controls

Attackers frequently **exploit weaknesses in privileged access security**, giving them a high level of control within the network.

Vulnerable Active Directory (AD) architecture

Failure to deploy the **right controls and principles** within your AD setup can leave **AD artefacts open** to a range of attack techniques.

Weak endpoint protection

Not deploying and maintaining the right technology solutions to **protect endpoints** can create **vulnerable entry points to your network**.

Misconfigured endpoint detection

Misconfigured, or an overreliance on, **Endpoint Detection & Response (EDR)** tools can lead to attacks going unnoticed.

Vulnerable backups

Vulnerable setup of backup networks can lead to **compromised backup services** during an incident, requiring a rebuild from scratch.

Insufficient monitoring

Security logs not being gathered or being **monitored ineffectively**, reduces the opportunities to detect and prevent incidents before occurrence.

Legacy Operating Systems (OS)

Legacy Operating Systems and/or **vulnerable protocols** in use, expands the attack surface and leaves well-known vulnerabilities existing.

Poorly protected low privileged accounts

Insufficient Identity protections on low privileged accounts enables easier exploitation, providing an attacker access.

Proactively securing and addressing these vulnerabilities can help to reduce the impact and blast zone of a potential catastrophic attack.

What challenges make recovery so difficult?

Organisations consistently struggle in the same areas during a catastrophic attack, making recovery longer and more challenging.

The **challenges** which organisations face during recovery consistently **delay a return to Business as Usual** (BAU). The impacts that have been witnessed from catastrophic cyber attacks add additional layers of complexity to these challenges.

Crisis Organisation

Organisations do not have processes and procedures that are suitable for an enterprise-wide response that a major cyber crisis demands.

Third Parties

The complexity of today's ecosystems and supply chains demands an integrated approach to recovery; this is often overlooked in recovery planning.

Prioritised Recovery

There can be a mismatch between what is recovered by technology and what is actually needed by the business, delaying recovery even further.

Data Backups and Storage

Traditional recovery practices are vulnerable to catastrophic data destruction events; all backups can be infected and unavailable.

Recovery Components

Organisations lack the documents, plans and tools to aid recovery from a severe but plausible cyber event where entire estates are impacted.

Financial Decision Making

The pressure that organisations feel during a catastrophic cyber attack leads to decisions which prioritise recovery speed and cost over security.

Human & Physical Availability

There can be an overreliance on a few key resources; physical infrastructure being impacted and overstretched by these events creates further delays.

Communication Channels

Communications, internally and externally, is restricted due to today's reliance on network-enabled channels which would be unavailable.

Proactively addressing these challenges in the context of a cyber attack will enable a more efficient return to BAU following a catastrophic incident.

What should you do now?

The journey to building and sustaining digital resilience is different for every organisation and is shaped by your business drivers and priorities.

Understand your main drivers

Understanding your key drivers for embarking on a Digital Resilience journey will help to shape the path taken and the activities that you prioritise. Is this move being driven by:

- An increasing reliance on data and technology?
- A "near miss" incident?
- Protecting your organisation's core DNA?
- Or other key business drivers?

Take the first step

There are several starting points that can lay the foundations for your journey. This will look different for every organisation and does not always mean starting afresh. Starting points could be:

Ransomware Readiness Assessment
Identify where you are vulnerable to ransomware and design your future state roadmap.

Business Prioritisation
Identify priority processes and their related systems, according to business criticality.

Cyber Simulation Exercising
Exercise your executive team to increase awareness and obtain senior buy-in.

Vaulting Solution
Implement a vault to identify, assess and protect your organisation's core DNA.

Taking the first step enables you to proactively shape your Enterprise Recovery journey before an incident.

Increase and maintain business confidence

Continue your Enterprise Recovery journey and build Digital Resilience to ultimately give confidence that the business could recover from a catastrophic cyber attack. What might this journey look like?

Initial recovery capabilities implemented in pockets, but not catering for a major cyber event.

Repeatable capabilities in some areas but not formally defined or documented.

Defined recovery capabilities maintained with processes formalised and documented.

Adaptive and embedded cyber recovery capabilities, integrated across the organisation's ecosystem.

How can we support you?

Enterprise Recovery focuses on being prepared for an incident, and responding and recovering efficiently after it.

Recovering the business after a catastrophic cyber attack requires a breadth of capabilities

In the aftermath of an incident technical expertise is key. However, it is not the only area in demand. Capabilities across a multitude of areas is vital. Legal, people leadership, communications, and forensics are examples of the skills required. Deloitte has the breadth and depth of experiences supporting organisations across the phases of an incident:

Respond

- **24/7 Incident Response:** incident triage, analysis, containment
- **Incident Leadership:** strategic level guidance; a trusted partner
- **Recovery Strategy:** strategy and journey to recovery

Recover

- **Business Driven:** identifying what is critical to the business
- **Recover Securely:** recover technology to a secured state
- **Future Planning:** reduce the likelihood of a further breach

Transform

- **Risk Identification:** focus on the key risks to the organisation
- **Build Foundations:** foundations for a more resilient, future state
- **Transformation:** a business wide strategy to continue uplift

The response and recovery from catastrophic cyber incidents can be quick, efficient and less financially damaging if organisations invest in recoverability, as opposed to waiting to react.

Through extensive experience in Cyber Incident Response (CIR), Deloitte has developed a comprehensive set of services which build Digital Resilience and improve Enterprise Recovery preparedness.

Preparing for a catastrophic cyber attack is an all-encompassing journey

Before an incident, organisations can increase preparedness for a catastrophic cyber attack. Deloitte's approach to achieve this looks across five key pillars that should all be considered to increase overall readiness. These services look to enable organisations to reduce the impact of an incident and enable a quicker return to business as usual.

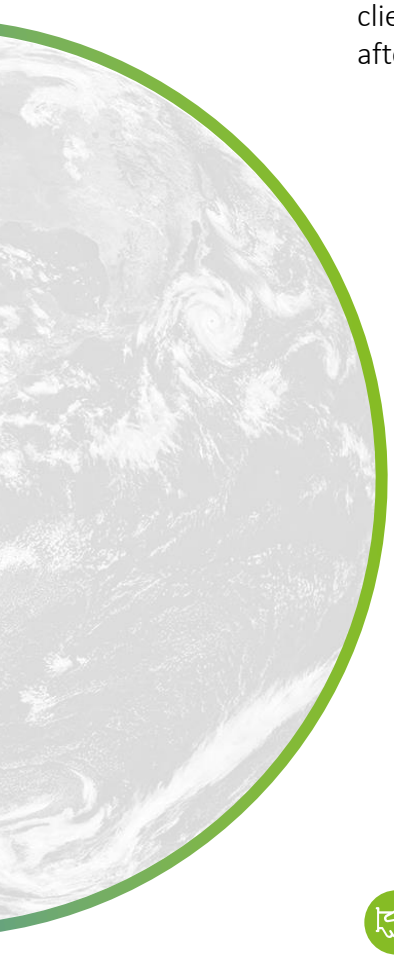
	Description	*Example Services*
Prioritised Recovery Planning	Plans for recovery that are prioritised and based on business criticality	• Process & technology mapping • Recovery Playbooks
Building Blocks of Recovery	Actual recovery tools and materials in place to rebuild the organisation	• Data Vaulting solutions • Backup architecture
Burst Capacity	Ability to scale up/down resources where they are scarce/excessive	• Review of choke points • Third Party assessments
Organisational Readiness & Alignment	Crisis team, procedures and processes enabling an enterprise-wide recovery	• Crisis Exercising • Business Continuity
Minimise Blast Radius	Security and architectural thinking to reduce the reach of an incident	• Active Directory hardening • Vulnerability & Patch Management

Deloitte's Cyber Resilience and Recovery practice

Experience, insight, innovation and leadership.

Deep technical experience

Our cyber practice has managed resilience and recovery on the most complex, technical projects across industries. We are experts in this field, focused on empowering our clients to be prepared for incidents and to get back on their feet as quickly as possible after an incident.



We see the bigger picture

At Deloitte, we understand the scale of the organisational change that is required. Our services span all areas of resilience, response and recovery and can be tailored to your specific needs based on your capabilities and business drivers.

Access to our network of experts

Deloitte brings more than just technical responders. We have a global network of skilled experts across technology (IT and OT) and business consulting, human capital, privacy, legal, forensics and people leadership. We design and manage programmes to empower our clients to succeed.

Leverage our leadership

Deloitte has taken the lead on many high-profile critical incidents. Acting as CIOs, CISOs and Incident Managers for our clients we have gained valuable insight, expertise and know-how to consolidate our ability to lead organisations out of a crisis.

Our Accreditations

Ranked #1 globally in Security Consulting; 10 Consecutive Years based on revenue by Gartner[6].

Named a global leader in Incident Readiness Services based on strategy and capabilities by IDC[7].

Named a leader in Cyber-security Incident Response Services based on strategy and current offering by Forrester[8].

Named a global leader in Cybersecurity Consulting Services by Forrester[9].

[6]Gartner, Market Share Analysis, Security Consulting Services, 2020
[7]IDC MarketScape: Incident Readiness Services 2021 Vendor Assessment
[8]TheForrester Wave™: Cybersecurity Incident Response Services, Q1 2019
[9]Forrester's Wave™: Global Cybersecurity Consulting Providers, Q2 2019

Contact us

Drop us a note to get the conversation started and to discuss your Digital Resilience and Enterprise Recovery journey.

Ivelina Koleva
ivelinakoleva@deloitte.co.uk
Director, Cyber

Sydney Grenzebach
sgrenzebach@deloitte.co.uk
Partner, Cyber

Bia Bedri
biabedri@deloitte.co.uk
Partner, Cyber

Nick O'Kelly
niokelly@deloitte.co.uk
Partner, Cyber

Deloitte.