

Cyber Recovery

Bridging the recovery gap

PwC Risk
December 2023



Contents

The Cyber Recovery gap

The ransomware risk continues to grow	4
.....	
C-Suite lack confidence in their current cyber recovery capabilities	5
.....	
Organisations are unable to fully recover	6
.....	
Timeline of a ransomware attack	7

Building a Cyber Recovery capability

How can you self-assess your ransomware readiness?	9
.....	
How to prioritise your cyber recovery initiatives	10
.....	
How can PwC help?	11

1

The Cyber Recovery gap



90%

of UK organisations say they expect greater exposure to cyber risk due to increased digitisation in the last two years¹.

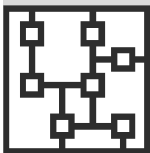
As the frequency and severity of ransomware attacks continues to increase, cyber resilience has become a top priority for leaders in every geography, industry, and size of organisation.

Building resilience to such attacks means building a robust cyber recovery capability.



Cyber attacks have been commercialized, and the frequency of destructive attacks continues to increase

Cyber attack services are more effective, integrated and accessible than ever before - as a result the proportion of destructive attacks has risen. As malicious groups and nation states continue to refine capabilities the scope and frequency of attacks increases.



Supply chains are amplifying the impact of attacks

As modern organisations increasingly rely on third parties, their exposure to cyber attacks grows. Attacks don't just harm their immediate targets - the impacts are felt up and down the victim's supply chain as the attack spreads through integrated services and infrastructure. Similarly, zero-day vulnerabilities expose broad groups of organisations and users.



No organisation is fully defensible

Without full control of the service chain it's impossible to guarantee security. Preventative measures and perimeter security offer a critical first line of defence, but achieving meaningful resilience requires an effective capability to recover IT from a cyber attack.

¹ - Cyber Security Outlook 2023, Cyber Threats 2022: A Year in Retrospect, PwC

Despite increased investment in cyber resilience, C-Suites are not confident in their recovery capabilities

The pace of technology innovation, transformation and change continues to accelerate.

More than two-thirds of organisations are investing in digital and/or technical transformation¹. This presents new challenges and risks. IT environments are becoming more complex, harder to govern and increasingly difficult to secure and gain visibility over. To support the more complex IT landscape, organisations are relying on third parties which expose organisations to vulnerabilities outside of their direct control - these range from major Cloud service providers to parties further down the technology supply chain.

The risk of this has not gone unnoticed - 39% of UK senior executives say they expect cloud-based threat vectors to significantly affect their organisation in 2023 compared to 2022¹.

In response, organisations continue to increase spending on cyber security.

The market for cyber security products and services has grown dramatically to meet growing concern for cyber security in light of these challenges. Half of CEOs say they are increasing investments in cyber security in the next 12 months to reduce and mitigate cyber risks¹.

More than 70% of business executives responsible for technology and security say they have seen improvements in cyber security in the past year following increased investments and C-Suite collaboration².

Based on our experience, whilst many organisations have implemented prevention and detection measures, few have the capability to fully recover their data and services following a ransomware incident.

Having supported organisations across multiple domains: incident response; post-incident investigations, and recovery implementations, we have identified 3 common themes which impair organisations' ability to recover from a cyber attack:

- 1. Incomplete understanding of ransomware and other cyber disaster scenarios;**
- 2. The assumption that vaulting solutions alone will enable rapid cyber recovery; and,**
- 3. Lack of an environment for forensics, and a trusted environment for recovery.**

Resulting ad-hoc recovery is likely to be long, complicated and costly. In a worst case scenario, organisations will be unable to recover all critical services and or forced to pay the ransom.

1 - Cyber Security Outlook 2023, PwC

2 - A C-suite united on cyber-ready futures: Findings from the 2023 Global Digital Trust Insights, PwC

Why are organisations unable to recover from ransomware?

A disaster event can take many forms - each with different impacts on IT and operations. To be effective, an IT disaster recovery (ITDR) programme must define what disaster scenarios the recovery capability is going to cater for, and those it is not. The solutions and procedures for disaster recovery need to be designed around the requirements specific to each scenario.

Many organisations rely on their responses to existing disaster scenarios, such as physical loss of systems - in doing so, they ignore key characteristics of a destructive cyber attack scenario:

Production data and storage will be corrupted

Cyber incidents are logical failures which lead to data corruption across connected storage. As a result, consideration should be made in how to minimise the 'blast' radius:

- Immutable backups
- Environment segregation

Data will need to be inspected before recovery

This step will occur pre-data recovery to ensure all recovered backups are clean. In order to speed up this step, the following should be considered:

- Specialised tooling
- Dedicated forensic environment
- Dedicated forensic team

Hosting environments and infrastructure services will be compromised

Recovery process must ensure that trustworthiness is verified - not just of data, but also of hosting and infrastructure services:

- Recovering active directory and other core services
- Dedicated recovery environments
- Environment segregation

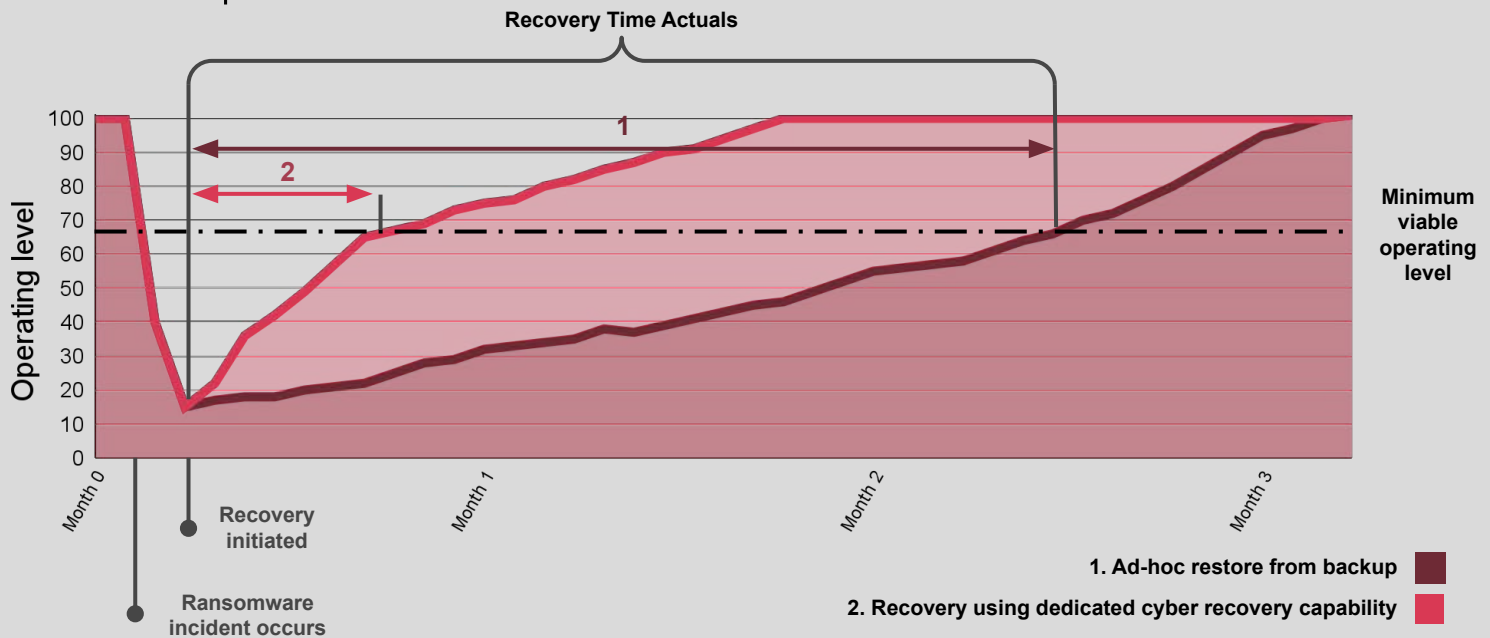
Mass data loss will extend restoration times

To minimise data loss, and meet recovery requirements, the following should be considered for both system level and mass recovery:

- Aggressive recovery point objective (RPO)
- Aggressive recovery time objective (RTO)

Lack of preparedness will prolong impact in the event of a major cyber disaster

Illustrative response timeline



1. Ad-hoc restore from backup

- Assuming existing backups are not encrypted these can be used for recovery, though this will still present challenges. If they are affected, organisations will need to consider alternative options; paying the ransom or attempting to use their services without historical data.
- Extended recovery times are a result of manual identification of clean backups and building new, trusted hosting environments, infrastructure and supporting services system-by-system leading to prolonged business impact over several months.
- A lack of tooling to identify non-encrypted backups for recovery can lead to inconsistent points of recovery across the recovered estate.
- Long term, some data may be permanently lost. Cost of recovery will be high with full business capacity only reached after several months.

2. Recovery using dedicated cyber recovery capability

- If the organisation has prepared to recover from this scenario then the relevant recovery teams are aware of their roles and responsibilities and the recovery has been tested resulting in a seamless response and recovery with services being brought back within the Service Level Agreements (SLAs).
- Ransomware detection and recovery tooling ensure all backups are free of encryption, ensuring no data is lost.
- Full delivery capacity is achieved within SLAs as a result of successful recovery where the remediation actions were predictable and managed.

2

Building a Cyber Recovery capability



How can you self-assess your current readiness?

Recovery Sequence

Is there a defined disaster scenario and recovery sequence for ransomware?



A pre-defined recovery sequence will enable a quick and efficient response to a cyber failure scenario, which delivers a shorter recovery time.

Is the recovery sequence tested on a regular basis?



Regular testing ensures the process is fit for purpose and enables people, processes and technology to build a strong ‘muscle memory’ that can be quickly triggered when a cyber attack occurs.

Isolation and Immutability

Is there a separate recovery environment to recover to?



Affected production environments are quarantined on detection of ransomware to limit propagation. Maintaining a recovery environment alongside production dramatically reduces the recovery time of the organisation.

Has immutable storage been implemented for backups?



Immutable storage prevents data from being erased or modified. In parallel with an air-gapped environment this protects important data from cyber attacks.

Detection and Monitoring

Is there adequate visibility of the IT estate?



A clear, visible IT estate with comprehensive asset management tools enables organisation to prioritise their applications, maximise their chances of early detection, and scope their cyber recovery initiative.

Do you have the capability to quickly identify the last “good” backup?



Backup monitoring tools enable quick and efficient ‘good’ backup detection in real-time, allowing for a shorter recovery time.

Security

Are backups and recovery tooling in an air-gapped environment?



Air-gapped environments provide secure storing of data and ransomware tools from ransomware attacks: effectively storing it ‘offline’ and preventing direct access.

Is there robust security in place for infrastructure services?




Robust security architecture and access controls are required to ensure infrastructure services, including backup and recovery tooling, are not compromised during a cyber incident, but still easily accessible by relevant teams.

How should organisations prepare to recover from a ransomware attack?

Depending on level of IT cyber recovery maturity, different concerns are relevant to organisations. Below are the commonly experienced ‘pain points’ and how we can leverage our people, technology and experience to address them:

“
I don’t know what the impact of ransomware will be, how much I can recover, and how long it will take.


Assess exposure and evaluate capability



Establish a current state baseline and perform gap analysis of existing IT cyber recovery / disaster recovery capability to surface risks and provide recommendations for improvement.

“
Will I be able to recover from ransomware with my current recovery capabilities?

Stress test cyber recovery



Develop and deliver tabletop exercises to identify gaps and improve response. This can be extended to performing live recovery testing with internally developed ransomware to test response capabilities with a representative scenario.

“
How do I design and build an ITCR capability from the ground up?


Design and build cyber recovery capability



End-to-end support in the design, implementation and operation of Cyber Recovery programs, or support to a sub-set of the programme lifecycle.

“
I’ve been hit by ransomware - what should I do now?

Investigate and report



In the wake of a significant incident or disaster we can provide impartial post-incident review, root cause identification and support remediation activities.

How can PwC help?

Our multi-disciplinary team of experts and practitioners have real-world experience helping organisations assess, improve and test their cyber recovery capabilities - we can work alongside you to improve your cyber recovery position.



Karen Penman

karen.penman@pwc.com
+44 7899 797331



Richard Horne

angelina.marie.murphy@pwc.com
+44 7483 935105



Mo Meskarian

m.meskarian@pwc.com
+44 7561 788971



James Bristow

james.bristow@pwc.com
+44 7483 434589



Angelina Murphy

angelina.marie.murphy@pwc.com
+44 7483 935105



James Cooke

james.r.cooke@pwc.com
+44 7718 864896

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2023 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.