Cyber security cyber recovery

October 2023

Many organisations have invested heavily in their IT security capability, but few have considered the complexity of recovering from a high-impact cyber incident and how it differs from traditional IT disaster recovery.

We bring together our recovery expertise and experience from dealing with real cyber crises to support organisations in maturing their cyber recovery capability.

> **"90% of UK organisations say they have experienced greater exposure to cyber risk due to increased digitisation in the last two years"**
>
> – PwC Cyber Security Outlook 2023

Common challenges when recovering from a cyber incident include…

Understanding the priority and resilience of services	Organisations without adequate operational resilience preparedness **struggle to prioritise the recovery** of business critical services. It is vital to understand which are your important business services and the other teams and processes on which these services rely, as well as the resilience of any workarounds available.	1
Interdependencies in service technology	Organisations often have not considered **how technology systems will be recovered** in the event of an incident. It is important to understand the interdependencies of the technology on which important business services rely, including third party services.	2
Documentation to support responders	Documented procedures help staff to respond effectively, but **often have gaps** which are discovered during the high stress environment of an incident. This can lead to an inefficient response which does not align with business requirements.	3
Prioritising investigation vs. recovery	Cyber incidents are almost unique because **there is a cyber criminal actively working against you**. Organisations need to be confident they have full control of their systems, whilst carefully balancing technical investigation and business recovery.	4
Lack of subject matter expertise	The majority of individuals **have never responded to a live cyber incident** and therefore may not have the necessary subject matter expertise. Therefore, organisations should consider third party support such as crisis experts, incident responders and external legal counsel.	5

How can PwC support?

Our team can help you to prepare for a high impact or destructive cyber incident. Our services are designed to give you confidence that your organisation will respond effectively in a crisis.

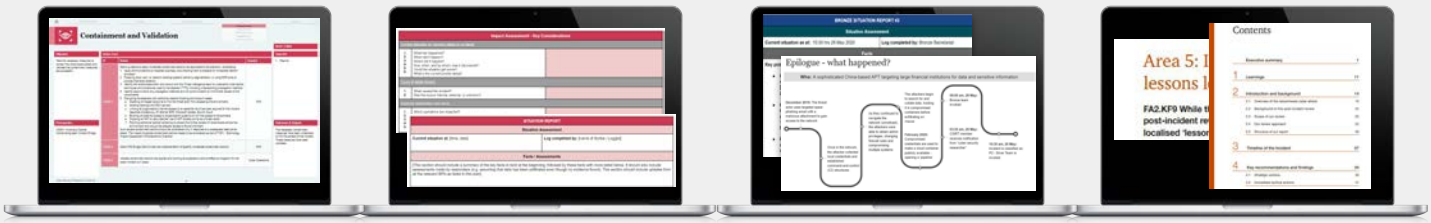
We work with you to understand the technology which supports important business services. We use this information to create robust plans that enable you to plan for effective cyber recovery before an incident occurs. Our team is made up of experts with knowledge of cyber incident response, IT disaster recovery and crisis management.

If you already have plans we can review them, using our knowledge of sophisticated cyber attacks to identify any gaps. We can also help you 'stress test' these plans, by conducting technical testing or crisis exercises.

pwc

Incident response	Disaster recovery	Crisis and resilience
Risk reduction and preparation		
Technical plans, playbooks, and runbooks for cyber security	Disaster Recovery plans and playbooks	Crisis management, communications, and legal plans
Incident response retainers	Disaster Recovery gap analysis	Operational resilience support
	Disaster Recovery end-to-end mapping	Crisis management training and exercising (including cyber security response and recovery)
Cyber recovery playbook*		
Live incident support		
Technical incident response support	Disaster recovery support	Crisis management support
Post incident support		
Post-incident report		

*More details on the Cyber Recovery Playbook can be found here



Cyber recovery playbook | **Cyber incident response guide** | **Training and exercising** | **Post-Incident report**

Why PwC

PwC was named a leader in Global Cybersecurity Consulting Providers and a Leader in Incident Response services providers by Forrester in Q3 2021.

Forrester concluded that PwC surpasses its peers with platforms and board-relevant services. PwC still stands out with its unique intellectual property and the pricing flexibility this creates for clients. While the firm's internal transformation resulted in many successes, PwC relies on optimizing tactical processes for clients as the bulk of its client-facing transformation work. PwC's strategic vision does understand where cybersecurity services will go, helping clients make trust a crucial component of the customer experience and transforming the results of one-off engagements into sustainable outcomes that continue to benefit clients long after the engagement closes.

Contacts for further information

Richard Horne
Partner
Cyber Security
richard.horne@pwc.com

James Cooke
Director
IT Disaster Recovery
james.r.cooke@pwc.com

David Cannings
Director
Cyber Incident Response
david.cannings@pwc.com

RITM13632629