# Cyber Security

## Cyber Recovery Playbook

A Cyber Recovery Playbook gives you confidence that you could respond to an attack that has a widespread impact on IT systems. It is a pragmatic playbook, that balances trade-offs between risk reduction and the rapid recovery of business services whilst also integrating with existing cyber response plans and playbooks.

We have designed and driven programmes in numerous organisations to enable them to recover from catastrophic ransomware attacks. While recovery planning is different for every organisation, the structured approach for secure recovery server by server, application by application and service by service enables a clear view for prioritisation and time calculations. The Cyber Recovery Playbook brings together step-by-step action cards to structure and guide the strategic and operational response to a cyber incident.

### Why do you need a Cyber Recovery Playbook?

**Decreased Response Time**

The Cyber Recovery Playbook sets out the initial containment actions and decision making authority. This allows responders to take these actions swiftly to limit propagation methods and thereby further spread of ransomware/malware
.

**Consistency and Visibility**

The Cyber Recovery Playbook can link action cards for the different response teams. This supports greater visibility and consistency of actions, ensuring the correct interactions take place between teams and actions are undertaken in the correct order and are not missed.

**Investigation**

The Playbook supports cyber security investigation and evidence preservation, ensuring that known details about the attacker are taken into account during the response. This supports post incident learnings and also insurance claims.

**Regulatory Compliance**

The Playbook provides action cards for Legal and Compliance teams, ensuring that regulators are informed at the correct time and that regulatory compliance considerations for your organisation have been taken into account.

**Change and Strategy**

Crises can cause great harm to organisations but they can also provide opportunity for change. The Playbook will decrease the mental load on responders and leaders, providing more space to set future strategy and make the most of opportunities that present themselves during a crisis.

### Key sections of the Cyber Recovery Playbook

Each section is tailored to your organisation

**01**
Scope and Governance

**Providing the underlying response structure and scope of the Playbook.**

**02**
Invocation and Recovery Process Overview

**Details invocation and escalation actions in the case of a high-impact cyber incident.**

The Playbook orchestrates Action Cards in five - colour coded - phases

When to invoke this playbook - operational mobilisation

Detect Escalate Mobilise Establish

**03**
Action Cards

**The quantity and level of detail of the response action cards can be tailored.**

CMT Time Critical Actions

Recovery Communications

**04**
Appendices

**Appendices include tools and templates and a summary of the response process.**

Crisis Communications Checklist Cards

Template Checklist Card

**Actions cards are grouped by phase and are tailored to be bespoke to your organisation. You can choose the level of detail for the action cards, the teams for whom action cards are created, the number of action cards per phase, and the terminology used.**

### Invoke and Contain

The initial phase contains action cards detailing how you invoke the correct individuals and teams to respond to the incident and the initial containment actions that need to occur (including decision making authority). Potential action cards for this phase include:

- Escalation to the crisis management team.
- Initial containment actions.
- Invoking an Incident Response Retainer.
- Initiate business continuity plans.

### Notify and Assess

The second phase focuses on assessment and establishing situational awareness. This phase can include action cards such as:

- Impact assessments.
- Assess regulatory notification requirements.
- Proactive communications to third parties.

### Foundational Recovery

Foundational Recovery details the actions required by teams to recover core infrastructure impacted by the incident. Examples of action cards include:

- Recover core infrastructure.
- Threat Hunting.
- Recovery Communications.

### Scalable Recovery

Scalable Recovery covers the recovery of applications in a prioritised manner for the business and the related data (referencing documentation on recovery from backups as appropriate).
Actions cards can include:

- Desktop Recovery and Vaccination.
- Eradication Event Planning.
- Tactical Security Improvement.

### Post-Incident Activities

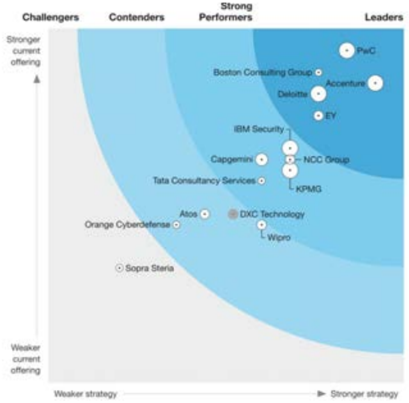
- Post-Incident Activities contains action cards of the activities required once the incident is deemed closed. This phase may include action cards such as:
- Post Incident Review.
- Planning for litigation.
- Ongoing recovery activities which have been channelled into business-as-usual.

### Our cyber security credentials

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

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.

The Forrester Wave™: European Cybersecurity Consulting Providers, Q3 2021



### Contacts for further information

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

**Nick Morgan**
Senior Manager
Cyber Crisis and Resilience
Nick.x.morgan@pwc.com

**Will Oram**
Director
Cyber Incident Response
will.oram@pwc.com

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