Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

cdbp Complete Data Breach Protection

# Cyber incident response roadmap

## Should your organisation become aware of an actual or potential cyber-incident (i.e. network interruption or data breach), it is important that you respond as soon as possible to minimise the impact to your organisation.

This Cyber Incident Response Roadmap sets out some of the steps that your organisation may wish to take following an incident, and should sit alongside any incident response plan that your organisation has in place.

This document is not intended to be a comprehensive checklist to be followed in every cyber incident nor is it a substitute for your organisation preparing its own incident response plan, which is recommended.

Each incident should be assessed on a case by case basis and in consultation with internal and external advisors, as required.

For more information about preparing for a cyber incident, contact us:

## CDBP Key Australian Contacts


**Tricia Hobson**
**Partner and Chairman, Head of Insurance for Asia Pacific**
Sydney
Tel +61 2 9330 8609
tricia.hobson@nortonrosefulbright.com

**Jacques Jacobs**
**Partner, Insurance**
Sydney
Tel +61 2 9330 8156
jacques.jacobs@nortonrosefulbright.com

**Nick Abrahams**
**Partner, Global Head of Technology & Innovation**
Sydney
Tel +61 2 9330 8312
nick.abrahams@nortonrosefulbright.com

**Matthew Ellis**
**Partner, Insurance**
Melbourne
Tel +61 3 8686 6329
matt.ellis@nortonrosefulbright.com

**Bernard O'Shea**
**Partner, Technology**
Melbourne
Tel +61 3 8686 6573
bernard.oshea@nortonrosefulbright.com

**Jim Lennon**
**Special Counsel, Technology**
Sydney
Tel +61 2 9330 8426
jim.lennon@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

## Detect

Your organisation becomes aware of a potential or actual cyber incident. Notify relevant internal stakeholders. Initial steps may need to be taken to contain incident.

## Notify Insurer / Broker

Notify your insurance broker and insurer of relevant facts and circumstances. Your insurer may facilitate access to a pre-approved panel of external advisors.

## Mobilise response team

Mobilise relevant decision makers in your organisation which may include the IT, legal, PR and risk management functions. To the extent required, engage external advisors who will assist you understand the incident and guide you throughout the incident response process. Advisors include: Legal, IT Security / Forensic, and PR professionals, as well as communications and credit monitoring and ID protection service providers.

## Preliminary assessment

Carry out a preliminary assessment to assess the size, nature and scope of the incident. For example, assess whether the incident is a network interruption or data breach incident, how and when the incident occurred, and impact.

## Contain and investigate

To the extent that this has not already occurred, contain the incident to prevent further loss. External IT/Forensic professionals can assist you contain and investigate the cause and effect of the incident.

## Legal assessment

Consider whether your organisation has any legal or regulatory obligations to disclose the incident to third parties which may include affected individuals, third party contractors, regulators, financial institutions, and law enforcement. Notification may be required for example, where there is a real risk of serious harm as a result of the incident. External Legal professionals can assist you understand your notification obligations and advise on the content of any communications.

## Notification campaign

Should your organisation decide to disclose the incident, take steps to notify relevant third parties as required. External Legal and PR professionals can advise you on a communications strategy to protect your organisation's reputation.

## Credit monitoring and ID protection

To the extent required, engage credit reporting bodies to protect affected individuals against identity theft and other potential financial harm.

## Ongoing Incident Management

Monitor the incident post-notification including responding to regulatory, media and customer relations inquiries. Communications service providers can assist you with engaging with customers post incident.

## Recover from incident

De-brief, identify vulnerabilities that caused the incident, and improve overall cyber security posture to prevent future incidents. Consider recovery actions against third parties responsible for causing or contributing to the incident.