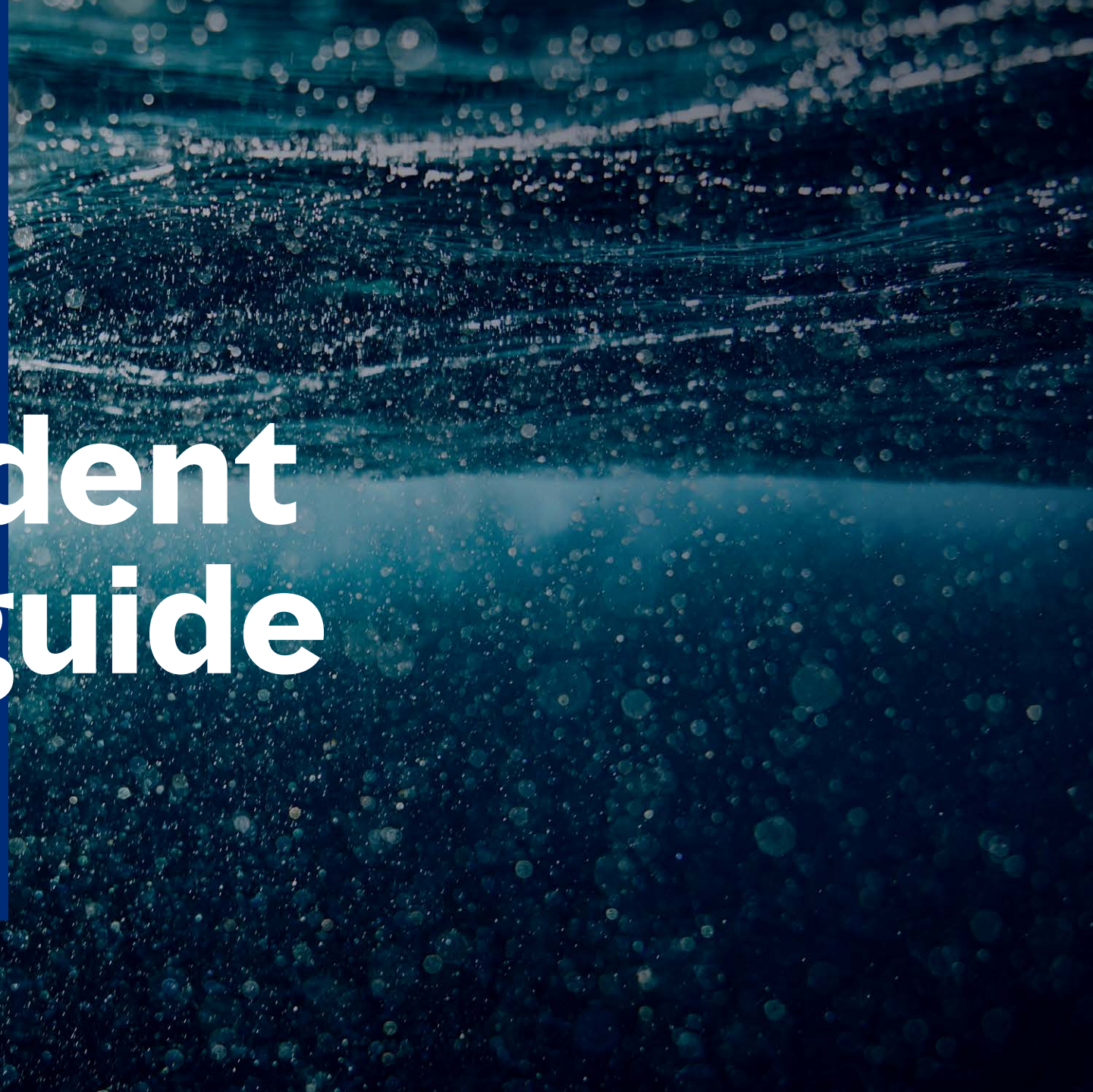
Marsh

Marsh Specialty

Cyber incident response guide



June 2022

Contents

Cyber threats remain one of the top concerns for business leaders, according to the World Economic Forum's Global Risks Report. This practical guide is intended to help organisations respond effectively to cyber incidents, including ransomware attacks.

As cybercrime and recovery costs continue to climb, organisations need to be prepared to take the necessary steps following an incident that could disrupt their operations. A successful response involves a number of critical steps, starting with prompt coordination of resources.

BEST PRACTICE STEPS FOR DAY ONE OF A CYBER INCIDENT

1 Gather the facts.

- Establish what happened and the nature of the incident.
- Determine when the incident occurred and when it was discovered.
- Find out which systems and devices have been affected.
- Determine what kind of data has potentially been impacted.

2 Contact Marsh immediately, even if you don't yet know all the facts.

- The Marsh Cyber Incident Management (CIM) team will provide you with initial guidance and support.
- Your Marsh broker will obtain a copy of your cyber insurance policy.
- A Marsh claims advocate will be assigned to your case.

3 Contact your cyber insurer immediately, while you're still gathering facts.

- Use your insurer's 24/7 monitored email and hotline to report the incident; this alerts your insurer that you are likely going to need covered services. The Marsh CIM team can assist you with this.
- Most cyber insurance policies cover certain incident response services, which often require prior consent. Many insurers have panel vendor requirements, so it's important to check this list before appointing third parties to assist with your crisis response.
- Marsh will typically follow up with an official notification to your insurer/excess insurer in accordance with policy terms as well as review panel vendor requirements in your policy. Your Marsh claims advocate will facilitate an internal call with your insurer.

4 Be mindful of electronic communications.

- If you suspect your systems have been compromised, consider keeping communications outside of your organisation's network, either by phone or through a contingency email platform that is not connected to your network.
- Do not send copies of your cyber insurance policy via your organisation's email system, whether you're communicating internally or externally.
- Marsh can help you establish an off-network collaboration channel, if needed, through the creation of cyber incident preparation and management rooms hosted by Cygnys.

5 Reach out to the necessary external expertise.

Some policies allow you to choose your external vendors, but many require you to seek prior consent from your insurer or choose an expert from the insurer's vendor panel. You should communicate the appointment of vendors to your insurer as soon as possible and keep your insurer updated with statements of work as they are produced.

Marsh can assist you with selecting from and activating the support of your insurer's vendor panel or help you identify appropriate vendors from Marsh's network.

- **Privacy counsel/"breach coach"**
  - Retain experienced privacy lawyers in order to guide the investigation, provide legal advice on regulatory notifications and ransom payments, and maximise potential legal privilege.
- **Digital forensics and incident response (DFIR) vendors**
  - External technical DFIR expertise may be necessary to support your IT team's internal investigation.
  - It can be beneficial for the DFIR firm to be retained by the outside law firm in order to maximise potential privilege.
- **Other incident response vendors**
  - Depending on the specific incident, you may need the services of other categories of incident response vendors, for example, crisis communications support or notification and call centre vendors in the event of a data breach requiring you to notify affected individuals.

Marsh will support you throughout the cyber incident response and claims process.

- The Marsh CIM team will continue to provide support and guidance as your cyber incident response progresses.
- Your claims advocate will ensure that your claim has been formally notified to the market and will:
  - Facilitate ongoing communication with your insurer(s) and its assigned claims adjuster or monitoring counsel.
  - Review whether any other policies may apply to the incident.
  - Confirm the extent of the coverage available, advise on insurer requirements, and assist with obtaining any necessary insurer approvals.

KEY CONSIDERATIONS FOR RANSOMWARE ATTACKS

Ransomware attacks are intensifying in both frequency and severity. They typically involve the encryption of files, data, or systems, and often involve a secondary extortion tactic involving a threat to disclose information.

These guidelines are designed to help you navigate this challenging situation. Note that this guide does not cover all possible fact scenarios and you should always seek expert advice.

1 Do not contact the threat actors directly.

We recommend that you seek external advice prior to making any contact with a threat actor.

2 Retain legal counsel and extortion consulting services.

Extortion consulting services are provided either by forensics firms or by standalone ransom negotiation firms. An extortion consultant can:

- Give information about the threat actors.
- Negotiate with the threat actors.
- Obtain proof of the information the threat attacker purports to possess.
- Verify that the decryption code will work if a ransom is paid.
- Obtain cryptocurrency for the transaction.
- Working with counsel, perform due diligence in accordance with the requirements of the Office of Foreign Assets Control (OFAC) and other regulators worldwide.

3 Notify law enforcement.

Through legal counsel, notify the UK National Cyber Security Centre (NCSC), Action Fraud, and other relevant organisations depending on the territories impacted by the ransomware. This may be a requirement of the relevant insurer.

4 Investigate back-ups.

Your IT team should investigate the availability of back-ups and, if back-ups are available, assess the time and resources needed to restore the data.

5 Decide whether to pay the ransom/extortion demand.

Such a decision involves a multi-faceted series of considerations, including assessing the effect on your business and the time to recover data/files and systems. Your organisation will need to do a dual-track analysis of its ability to restore data and systems from back-ups versus the potential for successful restoration if a ransom is paid. These fact-specific decisions are best guided by counsel and other experts.

6 Adhere to legal and regulatory requirements.

The payment of a ransom is not in itself illegal in the UK. However, depending on who the money is paid to, payment could trigger a variety of anti-money laundering, terrorism, or sanctions offences. It's also illegal to make ransom/extortion payments to entities on OFAC's Specially Designated Nationals and Blocked Persons (SDN) list. OFAC has extra-territorial reach. Prior to paying any ransom/extortion, check the list and document your due diligence. Extortion consultants can provide sanctions-checking services and the related due diligence documentation.

7 Keep insurers updated.

Some policies require that insurers provide prior consent for ransom/extortion payments, even in situations where the payment will not exceed the applicable retention.

Insurers expect to be kept informed of all aspects of negotiations with the threat actor and will require documentation, including screenshots of the extortion demand, proofs of payment and cryptocurrency costs, and due diligence documentation.

Insurers may perform their own sanctions due diligence and that process is often ongoing when the extortion payment is made.

Cyber extortion payments are usually made on a reimbursement basis, meaning you will need to be prepared to pay the extortion amount to the extortion consultant upfront.

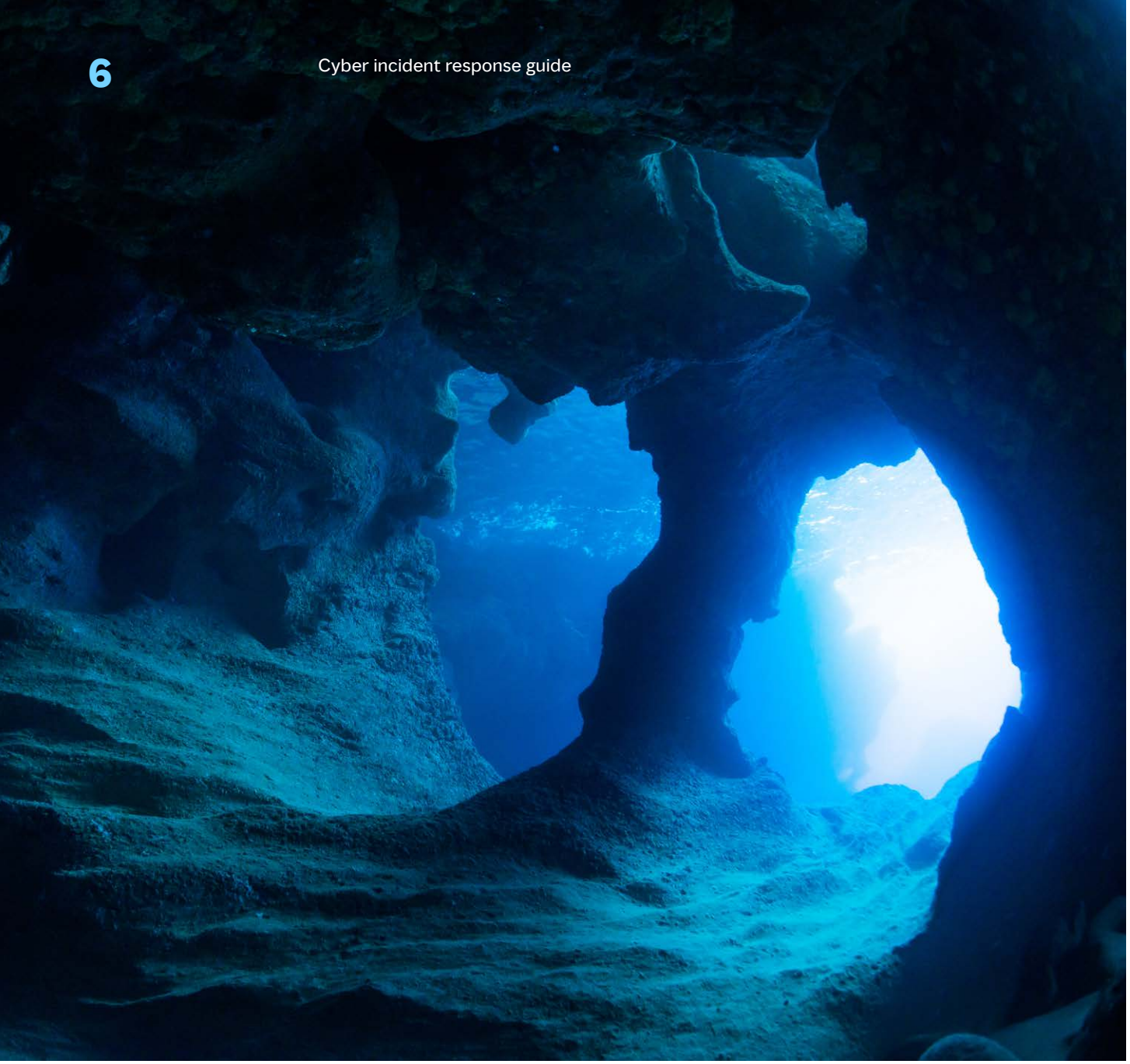
8 Document and track costs.

It's important to keep track of costs and retain documentation, whether or not systems are restored following a ransom/extortion payment. It's also important to track business impacts, such as loss or reduction of revenue, slow-down or interference with operations, and extra expenses to minimise impacts such as employee overtime.

Marsh Claims Solutions can assist with cost and reimbursement tracking and business interruption evaluation and quantification.

9 Determine relevance of other coverage.

You may have other insurance policies that will respond to a ransomware attack, such as a kidnap and ransom policy. Your Marsh broker or claims advocate will assist in determining if additional insurers should be notified.



This guide provides a high-level summary of the key initial steps typically required to respond to most cyber incidents.

For more detail and/or information on how to integrate these steps into your organisation's incident response plan, please email us at ***cim.uk@marsh.com***, reach out to your Marsh representative, or contact our cyber incident and claims specialists.

Helen Nuttall
Cyber Incident Management Leader, UK

+44 (7385) 482553
helen.nuttall@marsh.com

Patrick Cannon
Cyber Claims Advocacy Leader, UK

+44 (7385) 517241
patrick.cannon@marsh.com

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 45,000 colleagues operating in 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue nearly $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit marsh.com, follow us on LinkedIn and Twitter or subscribe to BRINK.