

Cyber Incident Management (CIM) service





Cyber incidents can have a huge impact on organisations, damaging reputation, incurring significant costs, and preventing critical operations. Being able to quickly respond to incidents, mobilise internal stakeholders, and obtain expert support helps to limit the impact of an incident and to prevent further financial and reputational damage to your organisation.

Professional guidance and access to specialists are key in enabling you to make the correct decisions under the pressure of a real cyber incident.

Our Marsh Cyber Incident Management (CIM) service offers you a complete solution to assist you in preparing for, responding to, and recovering from cyber incidents. With Marsh CIM, you are better prepared to deal with a crisis and have experts by your side from the very first moment you identify a cyber incident.

WHAT DOES MARSH CIM OFFER?

Leveraging Marsh’s cyber expertise and connections, CIM provides active support and professional guidance in navigating cyber incidents, from preparation to incident triage and support, through to post-incident.

CIM can provide assistance with a wide range of services dependent on the level of coverage you select. The support we provide can include:



Pre-incident Services

Preparatory work to establish your organisation with the service, connect with relevant vendors, and improve your cyber resilience.

- We can work with you to embed the CIM service into your existing incident response plans and procedures.
- We can review your existing vendor relationships and provide recommendations on the key categories of incident response vendors, such as IT forensic, legal counsel, extortion specialists, and crisis communications.
- In addition to the CIM service, you can choose from a selection of bolt-on consultancy modules, designed to help you to manage cyber risk and improve resilience, including incident response plan reviews, best practice incident response workshops, executive training, and more.



Active Incident Response Coordination (AIR)

Incident triage and support when you encounter an issue.

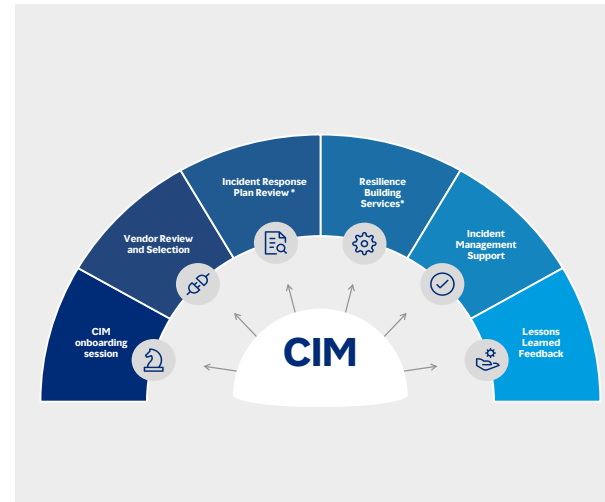
- Access to an expert cyber incident manager to stand by your side throughout a cyber-incident, provide best practice guidance, and support your internal stakeholders.
- The CIM service includes access to our specialist vendor network, ensuring that you connect with the right external experts at the right time.



Post-incident Support

To help you recover effectively.

- We can provide post-incident assessments and advice on how to incorporate “lessons learned” into your incident response plan, to prevent future incidents, and avoid pitfalls.
- If you have cyber insurance placed through Marsh, you can also receive support from the Marsh Cyber Claims Team who can assist you to prepare and submit your insurance claim.



* additional fees apply

Case study

Ransomware incident – Manufacturing company

A major manufacturing company was subject to a ransomware attack that encrypted key systems, led to significant operational impact, and compromised sensitive data.



The challenge

The company was subject to a ransomware attack that encrypted key systems, which led to a significant impact on business operations. The cyber criminals exfiltrated sensitive data from the network.

Senior leadership found themselves running the response alongside mobilising a “plan B” to keep various entities of the business running.

The attackers were demanding a ransom in cryptocurrency, equivalent to millions of euros, in exchange for the decryption key and a promise to delete the exfiltrated data. Failure to pay would result in the data being disclosed online within a matter of days.



Our approach

The company needed urgent support to identify the relevant response measures, and mobilise the right external vendors to support them. Once engaged, Marsh quickly connected the company with IT incident response & forensic support to investigate the incident and explore options for a fast and secure recovery.

Extortion experts were retained to support the threat actor engagement. Legal counsel were involved in various jurisdictions to advise on regulatory notifications and the impact on individuals’ data. Additionally, crisis communications specialists were involved in order to develop the communication strategy towards employees, business partners, as well as the public and the press.



Result

The impact on the business was significantly reduced through the rapid response and the advice and support of expert advisors. The Marsh CIM alleviated pressure from senior management by providing best practice guidance, coordinating the response, predicting hurdles, and smoothing the path to resolution.

Thanks to the professional response to the incident and the transparent communication, the company’s business partner relationships became stronger than prior to the event.

WHY ORGANISATIONS NEED CIM?



Cyber incidents are **fast-paced** and involve multiple internal and external stakeholders, burning senior leader time and resources



Brand and reputation can be at stake. Shareholders, customers and the media expect a quick and effective response



Organisations need to get back to business as **quickly** as possible, **limiting downtime** and losses



May be unable to access insurance and requires incident management **expertise** as a fall-back

MARSH DIGITAL CYBER MANAGEMENT TOOLS:



Cyber Incident Preparation and Management Platform

A safe and secure platform that centralises communication through an off-network workflow tool, with finegrained access control and the ability to collaborate securely internally and externally in order to prepare for and manage cyber incidents (via CYGNVS*).



Risk Intelligence:

Threat intelligence, risk based economic modeling, and quantification tools to inform data-driven decision making.



Cybersecurity:

Advisory expertise to enhance resilience, uplift cyber risk management and governance and support decision-making.



Insurance:

Proprietary insurance programmes, products, and tools to inform and improve cyber risk transfer.

*Marsh has partnered with CYGNVS to provide our clients with a secure incident management platform. The Marsh CYGNVS Cyber Incident Management tool is a secure collaboration platform that helps you to plan for, manage and respond to cyber incidents. Importantly, the platform helps you bring together the right internal and external teams, documents, workflows, and vendors to practice and prepare for a cyber incident before it occurs.

What is included in Marsh CIM?

The team can help align your incident management approach and resources before, during, and/or after an incident:

Solutions	Lite	Corporate	Elite
Onboarding call - 1 hour	✓	✓	✓
Access to 24/7 hotline	✓	✓	✓
Access to CYGNVS (demo link and QR code available)	✓	✓	✓
Vendor onboarding discussion	✓	✓	✓
Active Incident Response - \$500 per hour thereafter	✓	✓	✓
5 hours triage included (additional hours available)	✗	✓	✗
10 hours triage included (additional hours available)	✗	✗	✓
*Review/uplift/implementation of Incident Response plan	✗	✗	✓
*Board level workshop - 1 hour	✗	✗	✓
*Additional advisory services can be built in as requested	✓	✓	✓

* = services subject to additional fees



Meet the team

For more information
contact:



Steve Thompson
Cyber Business Development
Manager – Australia

 +61 467 958 546
steve.thompson@marsh.com



Gill Collins
Head of Cyber, Marsh McLennan Pacific | Head, Cyber
Incident Management and Cyber Advisory, Marsh Pacific

 +61 414 486 188
gill.collins@marsh.com

WHY MARSH

Our core capabilities span four areas of
cyber risk:

- ✓ Risk intelligence
- ✓ Insurance
- ✓ Incident management
- ✓ Cybersecurity

Whether you need help to build an
insurance programme from the ground
up or to identify a cybersecurity
vendor, our cyber risk advisors are your
objective, insightful guides throughout
the process.



About Marsh

[Marsh](#) is the world's leading insurance broker and risk advisor. With more than 45,000 colleagues advising clients in over 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 of \$23 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](#), and follow us on [LinkedIn](#) and [X](#).

Disclaimer: Marsh Pty Ltd (ABN 86 004 651 512 AFS Licence No. 238983) arrange this insurance and are not the insurer. The information contained in this publication provides only a general overview of subjects covered, is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Insureds should consult their insurance and legal advisors regarding specific coverage issues. All insurance coverage is subject to the terms, conditions, and exclusions of the applicable individual policies. Marsh cannot provide any assurance that insurance can be obtained for any particular client or for any particular risk.

If this communication contains personal information we expect you to treat that information in accordance with the Australian Privacy Act 1988 (Cth) or equivalent. You must advise us if you cannot comply.

© Copyright 2024 Marsh Pty Ltd. All rights reserved. LCPA 24/195. S24-279109