canopius

# Cyber Incident Response

## A Global Service


**Contact | Cyber Incident Response Team**

cyber.incident@canopius.com
US (+1) 844 955 5544
UK (+44) 333 305 8045
AU (+61) 1 300 004 880

# Your first call in the event of a cyber attack.

## Cyber security threats are a business reality.

As cyberattacks increase in volume and complexity, the loss of customer data and other sensitive information, as well as damage to data and computer systems, can put your entire organisation at risk.

If your business becomes victim, you need an **instant response**. As your insurer, we offer expertise and services that can instantly assess your situation and begin to mitigate the incident.

# Canopius Global Cyber Response Service.

## A 24/7 service for cyber incidents or data breaches.

Our team is here to guide, co-ordinate and ensure that we are positioned to fully support your business' recovery.

canopius

# Cyber breach response.

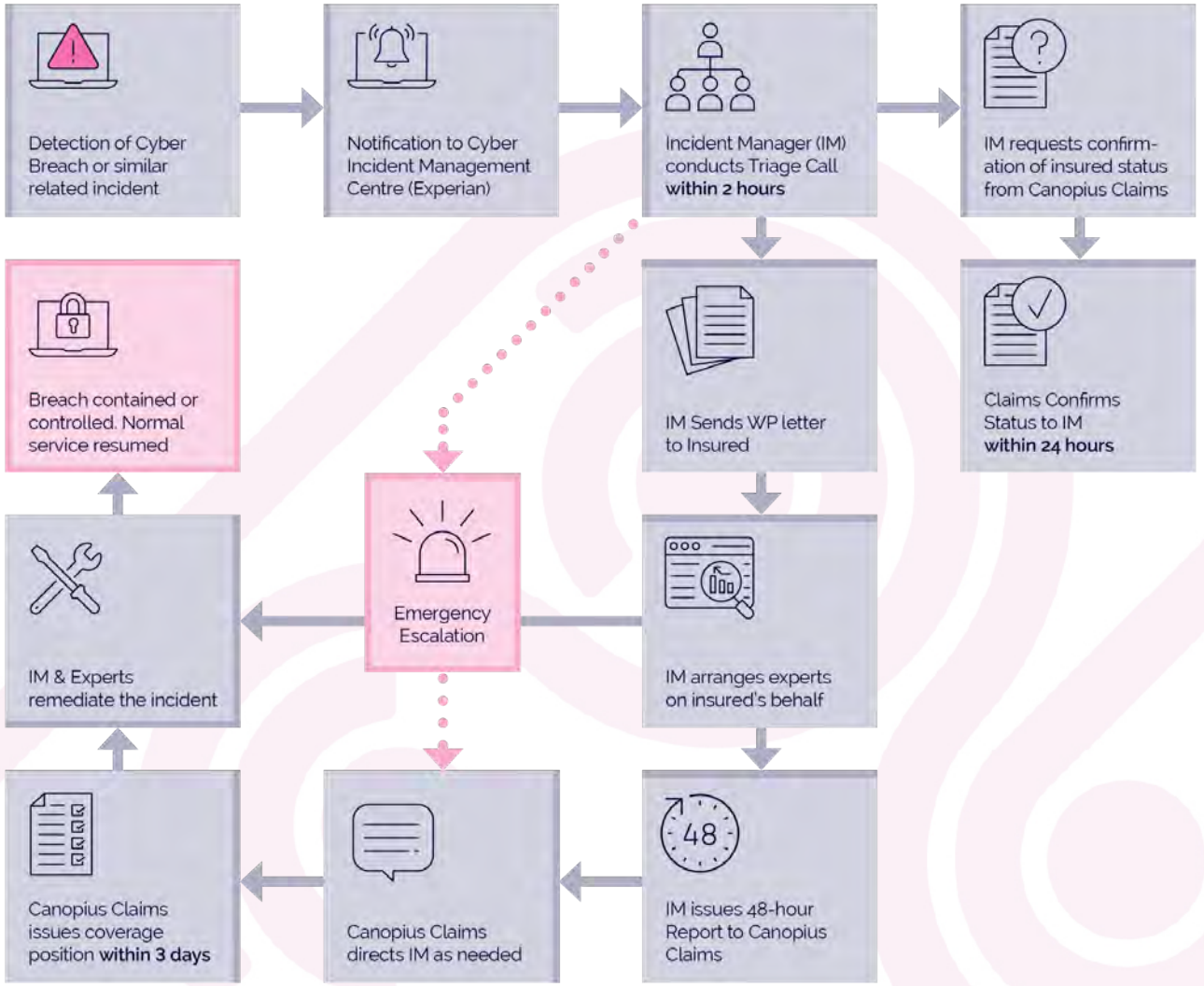
## Instant access to professional, global expertise

Canopius has a Global Cyber Response Service which takes notifications of new incidents through a centralised call centre and inbox:

- **24.7.365 initial triage**
- **Access to incident management experts**
- **Access to our panel of expert service providers – IT forensic, legal, PR, and more**
- **Strictly enforced service levels**
- **Multi-lingual capabilities**

Our global team can provide dedicated underwriting, claims and risk management support.

## The Canopius Global Cyber Response Service




canopius

# Making your claim.

1

## Facts about your claim

Our expert Cyber Claims Team will **liaise with the Incident Manager and service providers** to **obtain the facts** necessary to determine whether your claim is valid.

2

## Working with your broker

Canopius' Cyber Claims Team will **communicate with your broker** to provide a prompt and clear assessment of the coverage available for your incident.

3

## Claims Assessment

We aim to respond to any notification to the Cyber Incident Response Service **within five working days** with an initial claims assessment.

*The Canopius Incident Managers are not empowered to make decisions on whether an incident is covered. Coverage is not part of their role; they are experts in supporting you if a cyber incident occurs.*

## What sets up apart...


We don't default to instructing legal counsel to act as a go between. Instead, we give you direct access to a decision maker and an initial claims assessment within five working days.

Each claim has a dedicated Canopius Claims Adjuster assigned to your incident to work with you to resolution.

Our team is in-house and solely allocated to Cyber, strengthening our knowledge and expertise, ultimately ensuring you have the best resources when you need them the most.

# Less than five

**working days to provide initial claims assessments**

canopius

# Cyber breach response.

## Canopius Cyber Incident Managers – your cyber response within two hours

1

### Two-hour response

Within just two hours of contacting us, an **Incident Manager** will provide a call-back to the insured's nominated point of contact to conduct an **initial incident fact find**.

2

### Action plan

During this call, the Incident Manager will **recommend appropriate steps to respond to the incident**, which may include engaging one or more of our expert service providers from our panel.

3

### Crisis management

Our Incident Managers are seasoned experts in handling cyber incidents and will support the insured throughout the incident with **a carefully managed and co-ordinated response**.

*Where there are specialist systems which require specific service providers to remediate, the Incident Manager is empowered to consider such vendors and can agree to engage. This is subject to a general reservation of rights and on a case-by-case basis.*

### World-class service providers, available to support you

Incident Managers can call upon a range of firms from the Canopius panel, with global expertise covering more than 200 countries and territories around the world.

All firms have pre-agreed discounted rates and Service Level Agreements (SLAs) to benefit Canopius' policyholders. These pre-agreed rates ensure that our policyholders do not have to accept potentially higher 'crisis' rack rates and can instead move immediately to the incident response, rather than negotiating over the contract and rate card.

## Less than two hours

**Provide a call-back upon notification of an incident**

## 24/7

**Response across the globe**

**Discover more about our claims vision here**

canopius

# Cyber Response Service Global Panel.

**Our global panel provides a world-wide capability and our Incident Managers can draw upon additional firms where required to ensure a high-quality vetted service for our policyholders.**

## Digital Forensics & Recovery

- Arete
- KROLL
- Secureworks
- >_Code blue
- FTI CONSULTING
- S-RM
- CYBERCLAN
- Grant Thornton
- Triskele Labs
- GROUP-IB

## Legal Assistance

- CLARK HILL
- Kennedys
- wotton kearney
- CLYDE&CO
- MULLEN COUGHLIN
- CMS law·tax·future
- Pinsent Masons
- DAC BEACHCROFT
- WILSON ELSER

## Public Relations

- FLEISHMANHILLARD
- KEKST CNC
- FTI CONSULTING

## Mass Notification, ID Protection & Credit Monitoring

- experian
- KROLL

## Ransomware Negotiation

- Arete
- CYBERCLAN

## Data Mining

- integreon

canopius

canopius

Smart actions. Practical solutions.

With **unrivalled expertise and inspiration**, ours is a genuine passion to solve business problems and **deliver solutions that work**. By creating smart (re)insurance products, **we help businesses flourish**.

Cyber insurance awards europe

Highly commended

**Cyber Insurance Carrier of the Year**

---

in | insurance insider

HONOURS 2024

Cyber Incident Management Team

**Operational Innovation of the Year**


# Quick thinking and swift action saves the day.

## A key logger attack.

One of our clients noticed some unusual activity on their accounts. **Various funds were being misdirected and had escalated into a five-figure sum** – a huge loss for any small business.

Created to project-manage a crisis like this, our **in-house Cyber Team** was immediately on the case. After listening intently, it was clearly a key logger attack. **Someone had gained unauthorised access to their system and automated small payments were being redirected**. While on the call, we noticed the client was actually under another attack... but **with expert IT forensics this latest attack was rapidly intercepted**.

We isolated the client's systems, securely changed their passwords and removed the malicious software, thereby **providing a practical, innovative response to an urgent security problem**.

The attack could have been catastrophic but **our swift actions minimised the impact on their business, reduced the claims pay out and saved them from costly renewal expenses**. We also helped to futureproof the client from further attacks by outlining improved safety measures and automated software updates.

# Stopping a hacker in their tracks.

Hackers are getting smarter, and determining what's fraudulent is becoming more difficult. Attacks can have a huge impact and escalate rapidly. That's where the expertise of our Cyber Incident Management Team is crucial. T**hey spot the important small details that can often be overlooked**.

Under the pretence of a trusted supplier, a hacker tricked one of our clients into sending them three payments. Another colleague had opened an email giving the hacker free access to their systems.

Our response team recommended a **thorough check by our specialist forensics team**. It quickly identified the hacker had also begun sending phishing spam with numerous fake emails to employees. Five employees had fallen for them already.

The forensics team cleaned up the infected computers, changed all the passwords, and put new tools in place to watch for suspicious activity.

Without our thorough approach to each incident, this case could have had continued repercussions. **New security controls and monitoring tools are now in place, considerably boosting security levels**.

## Thorough checking with expert specialists.

# Experts in crisis management.

## Preventing ransom payment.

Our team responded to a client who logged in and saw any business' worst nightmare – **encrypted files alongside a ransom note**! The note demanded that the client make contact in order to receive the decryption key.

Our team arranged to bring in our **expert panel vendors to assess the situation and get our client's systems fully operational** as soon as possible. For an incident such as this, that means a digital forensics team to investigate how the threat actors breached the system and how to close that security gap so that it cannot be exploited in the future, a ransomware negotiation team to handle communications and a legal team to provide guidance.

Whist ransom negotiations started, the forensics team assessed backups and began to recover files. **Meticulous backups ensured operations could resume quickly and avoided ransom payments.**

**Our team consists of expertly trained crisis managers**. When our clients are faced with incidents like this, our team is on hand to be focussed with a clear action plan, while remaining calm and in control.