



canopius

Smart actions. Practical solutions.

Cyber Incident Response

Americas Service

Contact | Cyber Incident Response Team

cyber.incident@canopius.com

Canada: (+1) 613 699 2267 (French Canadian / English)

United States: (+1) 844 955 5544

International: (+1) 646 652 0749

canopius.com



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's recovery.

Cyber Breach Response.

Instant access to professional, global expertise

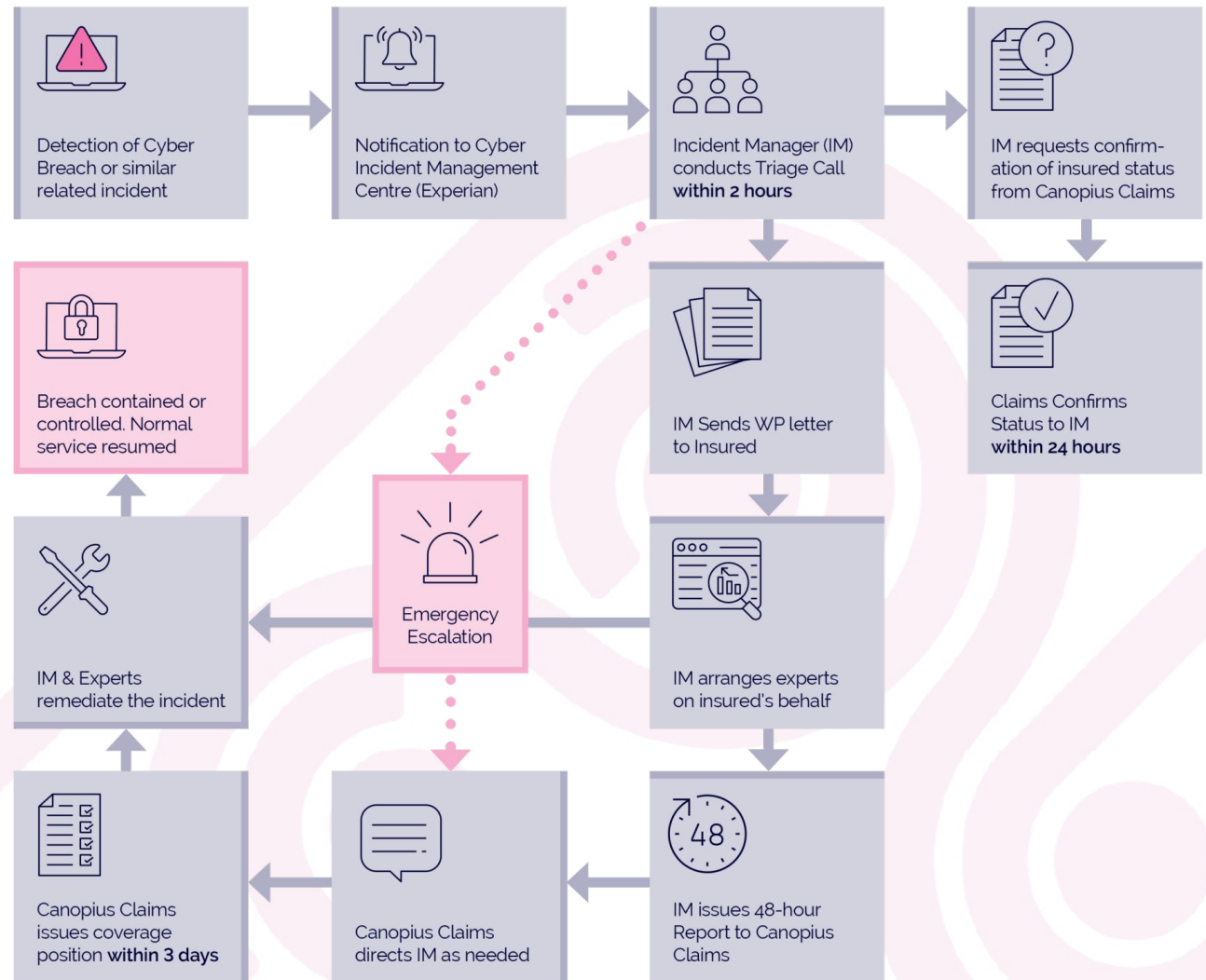
Canopus has a Global Cyber Response Service which takes notifications of new incidents through a centralised call centre and inbox:

- **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 Canopus Global Cyber Response Service



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.

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.

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.

What sets up apart...



We don't default to instructing legal counsel to act as a go between, giving you direct access to a decision maker and a faster initial claims assessments is within 5 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 insuring you have the best resources when you need them the most.

< 5

working days to provide initial claims assessments

Cyber Breach Response.

Canopius Cyber Incident Managers – your cyber response within two hours

1

2 hour response

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

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.

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 its incident with a **carefully managed and coordinated response**.

< 2 Hours

Provide a call-back upon notification of an Incident

24/7

Response across the globe



Discover more about our vision here

Cyber Response Service Americas Panel.

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

Digital Forensics & Recovery



Additional Approved Vendors

- Charles River Associates • Navigant Consulting • Pondurance
- Surefire Cyber • Unit 42 / Palo Alto

Legal Assistance



Additional Approved Firms

- McDonald Hopkins • Polsinelli

Affiliate

- Baker Hostetler • Dolden Wallace Folick • Fasken
- McCarthy Tetrault LLP • Other smaller firms

Public Relations



Additional Approved Firms

- Edelman

Data Mining

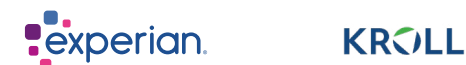


Provided by most of our Digital Forensic Firms and Legal Assistance

Ransomware Negotiation



Mass Notification, ID Protection & Credit Monitoring





Cyber
insurance
awards europe

Highly commended
**Cyber Insurance Carrier
of the Year**

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.

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** were 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. **They spot the important small details that can often be overlooked.**

Under the pretence of a trusted supplier, a hacker tricked our client 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 their specialist**

forensics team. They quickly identified the hacker had also begun a phishing spam, sending 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.

With a thorough approach to each incident, this case could have had continued repercussions. **New security controls and monitoring tools are place, 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's 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 clients 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.

Whilst 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 are 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.