Anatomy of a **cyber policy**

We've dissected our cyber policy to show you how it ticks

Cyber insurance policies tend to be modular in nature, meaning that they consist of a variety of different coverage areas. For many, that has led to confusion around how exactly this cover fits together to create a uniform whole.

To help explain this further, we've dissected our cyber policy section by section to show how each part of this body of coverage functions.

Key – parts of the policy

To make things simple, our CFC cyber policy is broken down into the following three areas:

Proactive cyber attack prevention
From the moment a CFC cyber policy is bound, we work round the clock to help prevent cyber attacks for our insureds.

Incident response and cyber claims
Triage incidents, contain threats and repair networks to minimize the impact and get businesses back online.

Comprehensive cyber cover
Covers the costs of a cyber attack, and helps get your businesses back to where it was before the incident.

Brain: Cybercrime cover

Not thinking about cybercrime? We don't think that's very clever. Within the context of a cyber insurance policy, cybercrime usually refers to the loss of electronic funds as a result of a cyber attack. This usually happens in one of three ways:

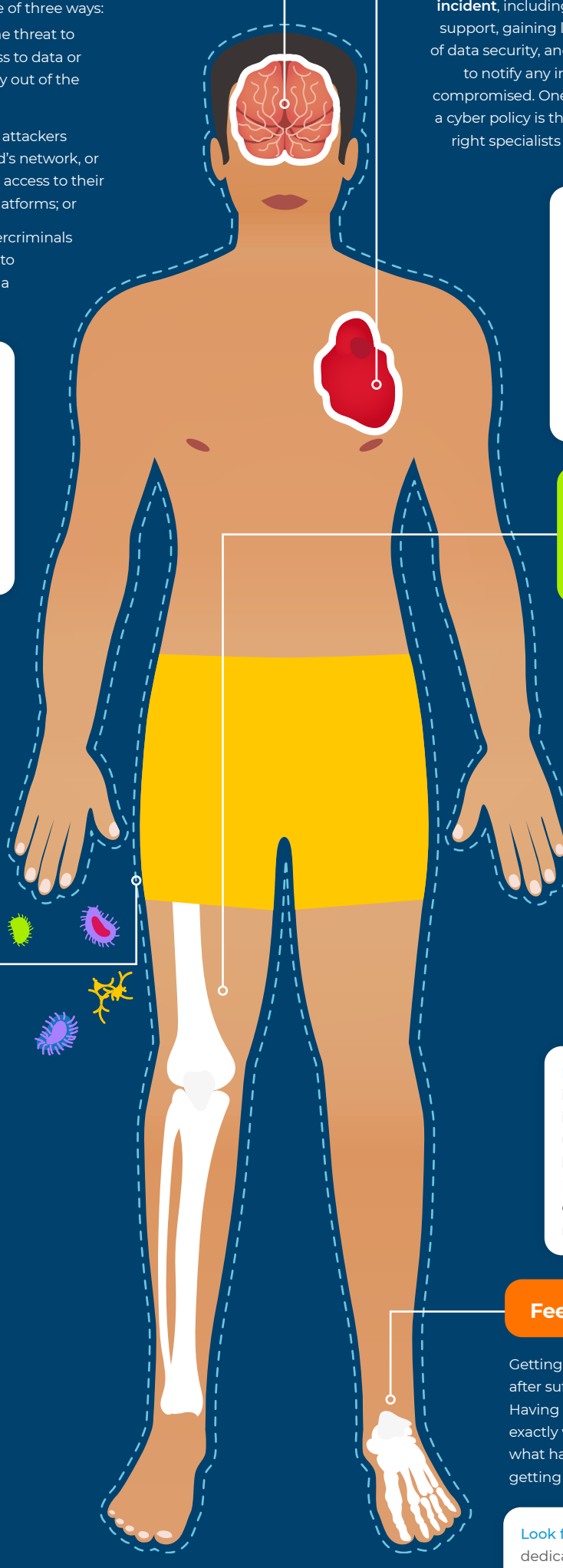
- **Extortion:** where hackers use the threat to expose, destroy or prevent access to data or systems in order to extort money out of the victim organization;
- **Electronic compromise:** where attackers manage to hack into the insured's network, or a third party's network and gain access to their online accounting or banking platforms; or
- **Social engineering:** where cybercriminals trick employees or customers into voluntarily transferring funds to a fraudulent account.

Look for ▶ policies that cover the full range of cybercrime losses, from funds transfer fraud and ransomware to targeted extortion and the unauthorized use of computer resources. Even if you have multiple attacks during your policy, having unlimited reinstatement means you'll be covered.

Heart: Incident response

A quick resuscitation from a cyber event is key, which is why incident response is at the heart of any good cyber policy. This section of cover will generally pick up all of **the costs involved in responding to a cyber incident**, including IT security and forensic specialist support, gaining legal advice in relation to breaches of data security, and the costs associated with having to notify any individuals that have had their data compromised. One of the most important aspects of a cyber policy is that it provides speedy access to the right specialists as well as paying for their services.

Look for ▶ insurance providers that have technically-led 24/7 inhouse expertise. At CFC our <15min response time helps streamline the response considerably and reduce downtime and costs. Costs for incident response should sit separately to the policy and at nil deductible.



Legs: System damage and business interruption

What really gives a cyber policy legs is a strong system damage and business interruption section. Helping to keep your business up and running, this crucial section covers the costs for an insured's data and applications to be repaired, restored or recreated in the event that their computer systems are damaged as a result of a cyber event. It also reimburses the loss of profits and increased cost of working as a result of an interruption to a business's operations caused by a cyber event or a non-malicious system failure.

Look for ▶ business interruption cover that includes a indemnity period of up to 12 months, which gives a business more time to recover. Ensure it covers the costs of data recreation, not just recovery.

Immune system: Proactive cyber attack prevention

As much as having a healthy and comprehensive policy is essential, with a robust immune system your policy might not even need to be triggered. And like a good immune system, it should identify potential threats, alert vulnerable clients and mitigate the risk before it even becomes an issue.

Look for ▶ a provider that uses a range of cyber security tools to monitor and prevent attacks 24/7. At CFC we provide vulnerability scanning, threat monitoring and real-time cyber attack prevention throughout the lifecycle of the policy.

Feet: Cyber claims

Getting your business back on it's feet after suffering a cyber incident is vital. Having cyber specialists who understand exactly what has been triggered and what hasn't allows you to focus on getting back on track.

Look for ▶ a provider that has a dedicated in-house cyber claims team that specialize in cyber attacks and has regional experience.

Online doctor: Response, mobile app

Sometimes you need some expert advice about your health. Our mobile app for cyber, Response delivers real-time critical threat alerts about your business. It's the quickest and most secure line of communication with our cyber security team, available 24/7 to respond to incidents and prevent cyber attacks.

Want to learn more about our award-winning cyber policy? Visit cfc.com/cyber