



Does cyber insurance coverage cost too much?

These days, the cost of cyber insurance is a hot topic. Here are three reasons it represents great value—and a vital service—for any modern business.

[Cyber insurance](#) plays a vital role in enabling and protecting modern businesses. But without a full understanding of how it works and why it's essential, it's easy to look at the price and deem it an unnecessary purchase, particularly for smaller businesses completely new to cyber.

Customers often remark the cost of cyber cover is comparable to more traditional insurance lines—and it's true. Like insurance for fire damage or crime, cyber events have huge potential to disrupt business operations. In fact, as cyber incidents become more frequent and costly to manage, and cyber services more innovative and effective, purchasing cyber insurance isn't just great value for money, it's one of the best investments any business can make.

Here are three things that influence the cost of good cyber cover.



1 Cyber is today's biggest exposure

Cyber incidents have been reported as the top business risk for the fifth year running, according to the [ICAEW's 2023 report](#), with cybercrime also named a [top cause of economic](#) crime for most businesses. Driven by a perfect storm of increasingly sophisticated and frequent cyber attacks, businesses today are simply much likelier to face dealing with a cyber event than a traditional risk like fire damage. As insurance for fire damage is seen as standard practice, shouldn't cyber be viewed with the same lens?

Cyber insurance works by empowering businesses to transfer their cyber risk to the insurer. As this risk grows rapidly, the insurer takes on a heavier burden. Of course, different industries do come with different levels of cyber risk. [Use our cyber risk heat map](#) to see how they compare.

2 The average cost of cyber claims is huge

Imagine your business is one of [the 72% worldwide impacted by ransomware in 2023](#). Like this [law firm](#), you may have failed to spot a malicious email attachment, leading to an attack which results in business downtime. Here, the cost of legal assistance, a forensic team and the ransom demand would have run into the hundreds of thousands. That's a huge burden for any business working alone to handle.

Cyber event costs include:

1. Loss from operational disruption
2. Remediation and recovery expenses
3. Legal fees
4. Hiring of expert teams
5. Regulatory fines
6. Ransom payment, if you choose to pay it
7. Reputational harm
8. Loss of customer loyalty

The same is true for other cyber incidents. Say one of your employees falls victim to a social engineering tactic. [This recruitment firm](#) unwittingly welcomed a fraudster into its ranks, resulting in a significant payment being misdirected. The funds were deemed unrecoverable, with the actual bill still to be paid.

Fortunately, both these firms had taken out a policy with CFC. They had access to a team which specializes in dealing with such events and received cover for financial loss—an amount far exceeding the premium paid—and expert advice on getting back up and running. More than anything, as they'd taken out a broad policy, they could focus on returning to business as usual instead of worrying about what they were covered for. That's why cyber insurance is so vital.

3 Good cyber insurance offers both proactive and reactive services

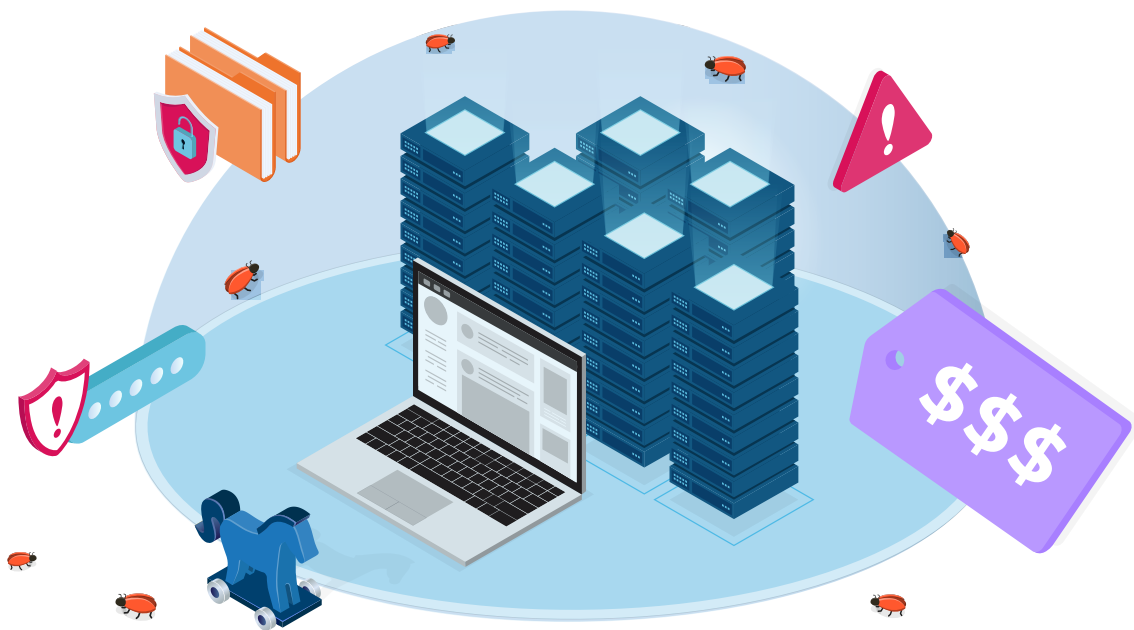
With cyber attacks, it's a case of who acts fastest wins. [Cybercriminals need around 9.5 hours](#) to access a target's network, so for the defender every minute counts. But what small business has the resources spare to build a dedicated cyber security team, one with the experience and skill required to match escalating cyber threats?

Cyber insurance is filling this gap. CFC has built the single largest in-house team of cyber experts in market, working around the clock from the moment a policy binds to detect and alert our customers to cyber threats targeting their business. Our global team has built a vast third-party threat intelligence network they use alongside vulnerability scanning tools, threat hunting and our own claims data to gather in-depth insights on whether our customers are at risk. When our team finds a cyber security issue, they notify the impacted business through our [Response app](#), offering instant support and eliminating the threat before it develops.

And if a cyber attack does happen, our expert cyber incident response team is on-hand 24/7—with a technical responder available in under 15 minutes—to triage incidents, contain threats and get businesses back online.

The best part? While these types of proactive and reactive services can cost businesses tens of thousands every year, they come as part of a standalone CFC cyber policy. That's instant peace of mind and constant protection for our policyholders, at no extra charge.

With the cost of global cybercrime set to reach [\\$10.5 trillion by 2025](#), comprehensive cyber insurance is just as inexpensive as it is invaluable. At CFC, we're continuing to innovate and expand our cover. We're not just here if the worst happens, our proactive service is designed to get businesses ahead of cyber risk, so they can operate with confidence and thrive.



Learn all about comprehensive cyber cover in our [cyber insurance guide](#).
Reach out to our expert team with any questions at cyber@cfc.com.