Cyber coverage highlights:
Nil deductible and separate limit for incident response

At CFC we offer initial cyber incident response at nil deductible, and put the associated costs into a separate limit.* This gives customers immediate incident response services and they don't have to worry about what it will cost.

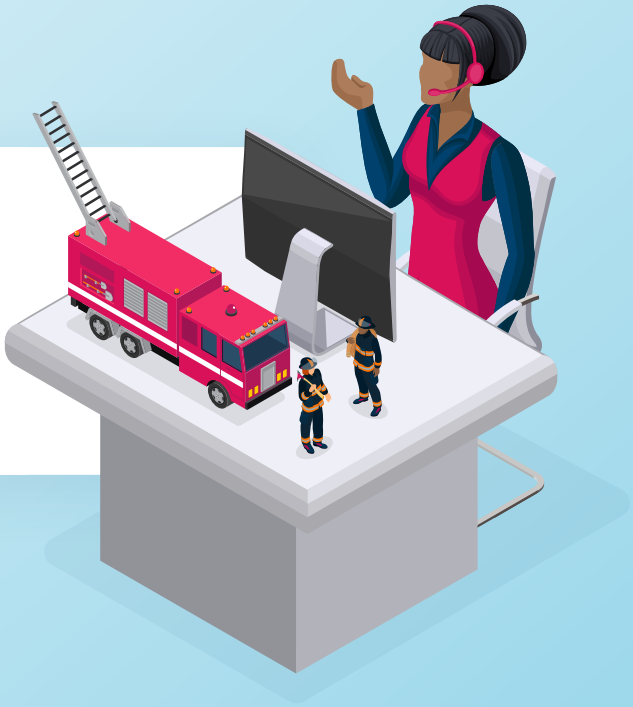
In moving from a promise to pay to a promise to protect, the best cyber insurance policies now come with advanced cyber security and incident response services—essential in preventing cyber attacks and minimizing impact when they do occur. These services are gamechangers in their ability to improve a business's cyber security posture and can make the difference between a business suffering a catastrophic loss or getting back to business as usual. But for many businesses, their positive impact can be hampered by fears over whether engaging with these services will trigger a claim and potentially rise future premiums.

CFC do things a little differently. To encourage policyholders to notify us as soon as they suspect a cyber incident, CFC provides initial support with no upfront payment from the insured, allowing the team to efficiently triage and establish the level of threat without the insured having to worry about what it will cost them. Further, all incident response costs fall into a separate incident response limit, leaving another full limit available for business resumption, business interruption and cybercrime costs.

**Excluding mid-market and large corporate products*

Incident response – definition

When you purchase a cyber insurance policy from CFC, you get access to a suite of technically-led in-house incident responders. Think of them as a fire department for cyber attacks, designed to respond to attacked businesses and help them recover fast and effectively.



What is nil deductible on initial incident response costs?

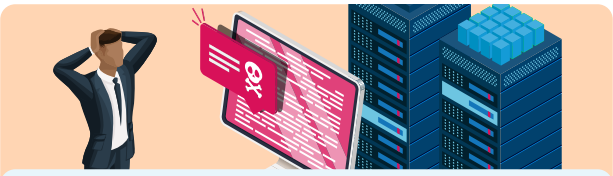
The sooner we know of a potential incident, the faster we can engage our technically-led incident responders to triage, contain and remove the threat. Despite this, some businesses avoid contacting their cyber insurer straight away - some over fears of a hefty upfront cost or that it will trigger a claim and potentially increase future premiums. Rather than engaging the insurer over something that turns out to be nothing, the business may wait and see how the situation develops, only notifying the insurer when things look dire.

This might sound like a sensible plan, but when it comes to cyber attacks every second counts. If you wait and see how the situation develops, by the time you notify your insurer, it can lead to a situation that much worse and more costly than if you'd called right away. That's why we offer initial incident response services at nil deductible. Our policyholders are free to notify us whenever they suspect something is awry, without the burden of having to pay for the initial response and without a claim being automatically triggered. Our expert team is on hand to offer support for any cyber event you experience —from system outage and business email compromise to ransomware and theft of funds.

What is a separate limit for incident response costs?

Most cyber insurance policies have a single aggregate limit which is eroded every time you make a claim. But since responding to a cyber attack can be extremely expensive—taking into account attack forensics, system restoration, data recreation, potential ransom payments, legal fees, regulatory fines, losses from business interruption and so on—it's possible for the total associated costs to exceed the policy limit, leaving the business out of pocket and exposed to another cyber attack in the same policy period.

At CFC we offer two separate towers of cover; one for costs associated with incident response services, another to deal with the business resumption, business interruption and cybercrime costs – essentially giving customers two full limits for the price of one! This way, our policyholders' limits won't fall short. Incident response services will help to mitigate the incident, and if the incident still impacts the business the other policy limit will kick in.



Nil deductible and separate limits in action

For example, let's say a retailer with a $1 million policy limit sustained a ransomware attack when a threat group accessed its systems through a compromised virtual private network (VPN). Using an employee's account they launch malware, encrypt the systems and leave a ransom note.

As a CFC policyholder and unable to access computer systems, the retailer reaches out to CFC via our mobile app, Response. Our in-house team begin a forensic investigation at once (with no initial payment from the insured), discovering the root cause of the attack and taking steps to mitigate. We find up to date data back-ups, and it is decided to not pay the ransom. Our experts guide the business through the necessary steps to reboot its systems, while also engaging a public relations agency to assist with handling messaging for the event.

In this case the incident response costs could easily amount to $100,000, but they'd all be taken care of by the separate IR limit. Meanwhile the retailer would erode its other resumption costs limit, including a significant loss of revenue due to business interruption and third-party action, costing over $1 million. Meaning the retailer would incur a total cost of $1.1 million—fortunately all costs would be covered by its $1 million policy limit due to costs being split between our two towers of cover.

Market-leading cyber cover

At CFC, our cyber insurance is designed to provide comprehensive coverage the lifecycle of the policy. With nil deductible for initial incident response and a separate limit for the associated costs, our policyholders have invaluable peace of mind; if a cyber attack hits, they can rely on CFC to get them back up and running.

Discover the power of unlimited reinstatements, another key cyber coverage highlight, in this article.