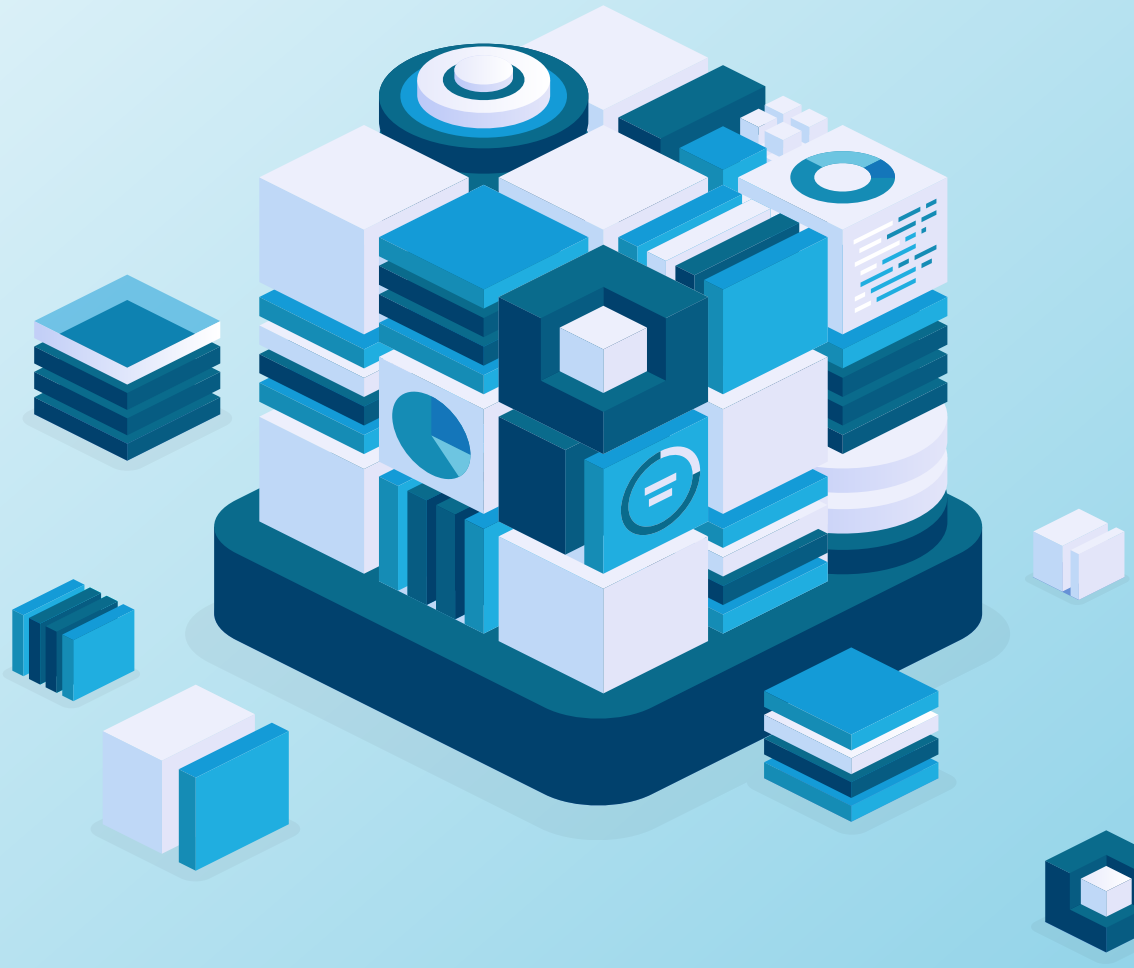
cfc

Case study

Our **Cyber Proactive Response** policy in action

Our cyber policy is built to cover a broad range of cyber threats and risks. See how our policy would respond to each of these situations and help your clients see the true value a cyber policy can provide.

Let's explore how our Cyber Proactive Response policy comes to life through a range of different claims scenarios and see how it can cover your clients.



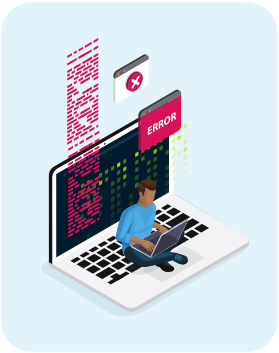
Cyber policy in action

Physical goods fraud

A wholesale supplier of goods is approached by a new customer interested in placing a large order. After initial discussions, the customer pays a deposit and agrees to settle the remaining balance over a given period of time. Trusting the legitimacy of the transaction, the wholesaler ships the goods as agreed.

However, it later transpires the customer was actually a fraudster that disappeared without trace, leaving the remaining amount for the goods unpaid for. With the goods unrecoverable, the supplier is left out of pocket.

With CFC's CPR product in place, the insured is reimbursed for the cost price of the items sent to the fraudster, under the new "Physical Goods Fraud" section of the Cyber Crime insuring clause.

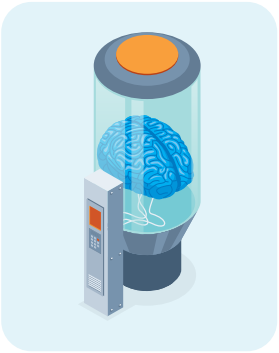


Operator error coverage

A business outsources a key element of its IT infrastructure to a third-party technology provider. During a routine system update, an employee at the technology provider makes an error that results in the business's computer systems going down.

With systems offline, the insured's operations come to a standstill, with customers unable to make new orders. The downtime leads to a significant loss of income and a backlog of unfulfilled purchases.

With CFC's wording in place, however, the business was reimbursed for the lost income caused by this error, as well as the additional costs incurred to mitigate it

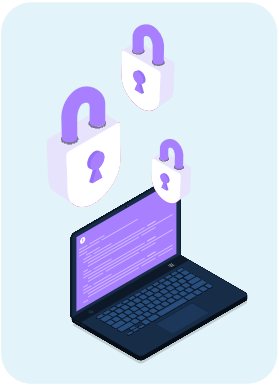


Affirmative AI-attack cover

A hacker uses a sophisticated AI tool to crack a weak password on the insured's remote access solution, allowing them to infiltrate the insured's network.

Once inside, the hacker begins exfiltrating sensitive data, putting confidential client data at risk. The breach results not only in additional costs to remove the hacker from the network, but also notification to individuals whose data has been breached as well as a fine from the regulator.

Fortunately, a CFC cyber policy provides affirmative cover for cyber attacks that utilize AI, ensuring that the business is covered for any of the losses associated with such attacks.



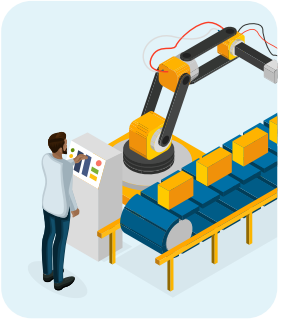
Interim payments for business interruption

An online retailer that relies on continuous system uptime to service customers experiences a distributed denial-of-service (DDoS) attack, taking down its website and making it impossible to operate.

Almost immediately, revenue plummets, and with losses mounting, the business faces serious cash flow issues. While the full extent of the business interruption loss is being assessed, the company needs an immediate financial lifeline to stay afloat.

With CFC's CPR policy, the business doesn't have to wait for the final loss calculation before receiving crucial funds. With cover for interim payments included in the wording as standard, the insured receives payments to cover costs and keep the company running.

Cyber policy in action

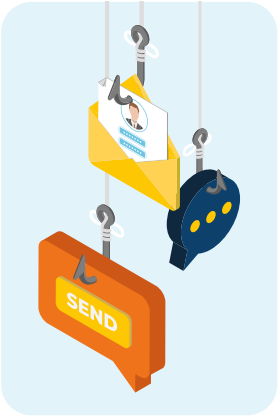


Contingent bodily injury

A manufacturer's operational technology (OT) is infected with malware, causing a serious malfunction in the machinery that results in an employee being seriously injured.

The injured employee subsequently files a lawsuit against the manufacturer, seeking compensation for the harm suffered, but the manufacturer's traditional casualty policy has a cyber exclusion in place.

CFC's policy provides cover for contingent bodily injury claims stemming from a cyber event, paying for any damages issued against the insured as well as defense costs.



Invoice manipulation

A wholesale supplier of goods completes a large order for a customer and sends an invoice over email to facilitate payment. But a hacker has gained access to an employee's email account and intercepts the communication.

Looking to exploit this opportunity, the cybercriminal creates a fake invoice and impersonates the business, falsely stating that the company's bank details have changed. Assuming this is legitimate, the customer wires the payment to a fraudulent account, leaving the business unpaid for the goods they have already delivered.

Fortunately, a CFC cyber policy provides affirmative cover for invoice manipulation losses like this, reimbursing the insured for the funds owed to them, as well as paying for the costs to secure the compromised email account.

Lost or missed bids

An engineering firm in the final stages of securing a lucrative contract with a prospective customer falls victim to a cyber attack that exposes sensitive data.

News of the incident reaches the prospective customer, damaging trust in the firm's ability to deliver secure and reliable services. As a result of the breach, the client rejects the firm's bid, awarding the contract to a competitor instead.

CFC's cyber policy provides affirmative cover for income loss arising from lost or missed bids stemming from a cyber event. This means the business is reimbursed for the income they would have earned from the lost contract, protecting it financially while its seek to rebuild its reputation in the market

Voluntary shutdown

When a professional services firm detects malware spreading, it takes quick action to contain the threat.

As a precaution, the firm voluntarily shuts down its systems to prevent further damage. However, this also disrupts access to critical systems, leading to loss of income.

CFC's cyber policy provides clear coverage for income loss caused by a voluntary system shutdown in response to a cyber event, ensuring the insured can recover financially while taking necessary steps to protect their business.

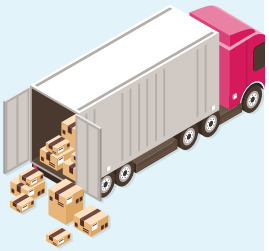
Cyber policy in action

Time franchise

A retail business earning approximately $1,000 per hour from online sales suffers a cyber event which takes the website offline for 16 hours—resulting in income loss of $16,000.

Most cyber policies impose a waiting period to system business interruption losses, requiring systems to be down for a set period of time (typically 8 hours) before cover is triggered. But in many cases this operates like a time retention. In this instance, it could mean only losses incurred after the first 8 hours are covered.

However, with CFC's cyber product, a time franchise is in place as standard. Provided the system is down for more than 8 hours, any losses incurred in the first 8 hours will be covered. As a result, the insured is able to recover the full $16,000 in income loss.

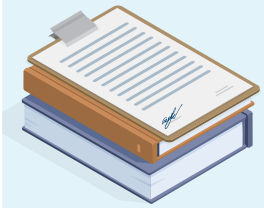


Hardware replacement of operational technology

Following a cyber event, a manufacturer's OT is corrupted, rendering key industrial machinery unusable.

While reinstalling software or firmware is often a viable solution, in this case the extent of the problem meant that doing so would be time-consuming and costly. To minimize downtime and restore operations as quickly as possible, it's deemed most practical and cost-effective to replace the affected hardware with new equipment.

Under CFC's cyber product, the insured is covered for the replacement of hardware (including OT) impacted by a cyber event, where it is more cost effective than reinstalling software or firmware onto the affected items. Instead of facing prolonged disruptions or struggling with partial fixes, the business is able to swiftly invest in new equipment, resume production and avoid the significant financial impact of extended downtime.



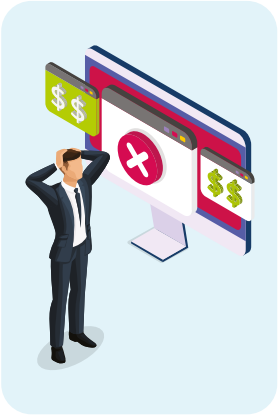
Unlimited reinstatements with nil deductible

A professional services firm with a $1 million policy limit with CFC suffers a ransomware attack, leading to a total loss of $900,000, fully covered by the policy. With nil deductible, the insured wouldn't need to pay anything towards this loss.

A few months later, the company is targeted again—this time in an unrelated social engineering attack that results in an employee transferring $200,000 to a fraudster. Most cyber policies operate with an aggregate limit that erodes with each claim (reducing the limit available), alongside a deductible that applies to each claim. But CFC's cyber wording is different.

With unlimited reinstatements and a nil or single deductible as standard, the firm's $1 million policy limit is reinstated in full after the first claim. This means the insured is reimbursed in full for the $200,000 loss, without paying an any or an additional deductible. This helps the business to remain financially secure despite multiple cyber incidents in the same policy period.

Cyber policy in action

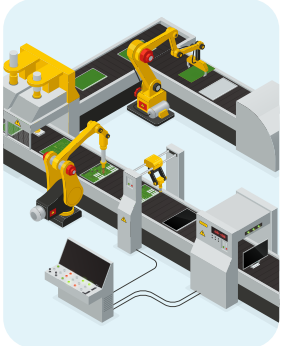


Theft of client funds

A financial advisor with access to its client's bank account is authorized carry out transactions on the client's behalf. When the advisor receives an email from its client requesting a funds transfer to a new payee, it assume the request is legitimate and proceeds with the transfer.

However, it later emerges the email was part of a sophisticated social engineering scam, and the funds were sent to a fraudster. As a result, the advisor took responsibility for the error and reimburses the client for the missing funds.

With CFC's cyber policy, the financial advisor is covered for the cost of reimbursing the client, ensuring the advisor is not left out of pocket for the incident and helping to preserve their relationship with the client.



Emergency and additional operational continuity costs

A manufacturing firm experiences a non-malicious system failure that takes its systems offline, severely impacting the firm's ability to fulfil customer orders.

With an important contract worth $50,000 on the line, the business has to act quickly. To avoid breaching its agreement, the manufacturer incurs an additional $60,000 to outsource the production of the goods to a third party at short notice.

Under CFC's CPR policy, the insured is covered for the additional costs incurred, even though the costs exceed the amount of income loss saved—helping the business protect both its client relationships and bottom line.

Legal disclaimer: These examples are intended for illustrative purposes only and not intended to address the circumstances of any particular insured.

Find out more about CFC's new Cyber Proactive Response product in our webinar

cfc.com

CFC Underwriting Limited is Authorized and Regulated by the Financial Conduct Authority FRN: 312848. Registered in England and Wales RN: 3302887 Registered Office: 85 Gracechurch Street, London EC3V 0AA. VAT Number: 135541330

©2025 CFC Underwriting Limited. All rights reserved.