What is cyber insurance?

Cyber insurance can help protect your business against the financial loss resulting from a range of cyber threats and exposures, including cybercrime, data breaches and system interruption.

Cyber insurance is important because as businesses increasingly use technology to operate, the digital assets they hold, like important business data, corporate information and client records, are becoming more valuable and more vulnerable.

A typical cyber insurance policy covers both first party and third party liability exposures such as:

Cybercrime including attacks like phishing scams that allow hackers system access or malicious emails that trick employees or customers into wiring money to fraudulent accounts

Business interruption caused by a cyber event, such as a ransomware attack or extortion, or prolonged system downtime that means your company cannot fully operate

Privacy breaches and the costs associated with them, like notifying affected customers, providing credit monitoring and identity restoration services, and paying for legal advice and services

Reputational damage inflicted by a cyber event that leads to cancelled contracts or customers choosing to find goods or services elsewhere

Cyber insurance is not just a product. It's a service.
When you buy a cyber insurance policy, you are ultimately buying access to technical resources in case the worst happens. A good cyber policy reacts immediately to a cyber event, providing instant access to IT security experts, forensic investigators, lawyers and crisis communications specialists who will help you manage the situation and get back online as quickly as possible. Most policies will also provide free risk management tools, like employee training and dark web monitoring, that can help keep your business secure and prevent events from happening.

For a more information about cyber insurance, visit www.cfcunderwriting.com/cyber

*(Claims Sept 18 – Aug 19)

Cyber for professional services

Whether you're an accountant or a designer, your greatest assets are your people and your ideas. Technology has made it easier to create, collaborate and deliver your services to customers both around the corner and around the world. But as your employees and your business move online, you also become a target for cybercrime.

Cyber insurance can help...

Recover and re-create important files and data

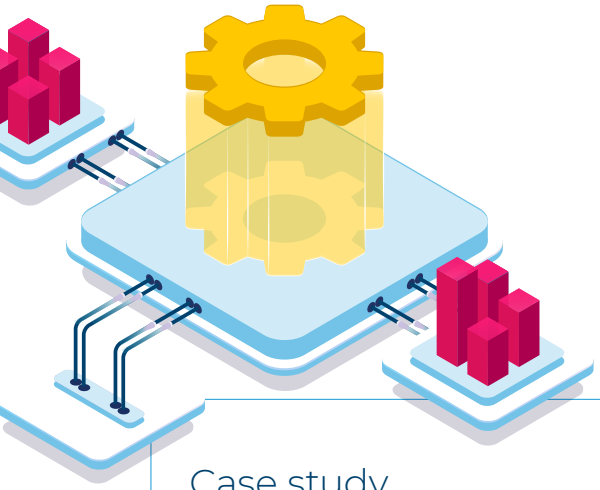
Nowadays, hackers are increasingly targeting businesses with cyber attacks and social engineering scams to lock down systems and hold important assets for ransom. Whether it's customer invoices, design files, project plans or your next big pitch, losing access to business-critical files and data can be disastrous to a professional service firm. Cyber insurance can protect you against the financial loss associated with these kinds of events, paying for the recovery and even re-creation of important data and minimizing any long-term impact to your business.

Guard you against fraudulent payments

Many professional service firms deal with wire transfers, whether you are requesting payments from clients or trying to pay suppliers. Unfortunately, this leaves you exposed to a growing problem – funds transfer fraud. Often initiated with a simple phishing email, fraudsters increasingly dupe employees into transferring what they believe are legitimate payments to fraudulent bank accounts. Cyber insurance can protect your business, as well as your customers, from the financial loss incurred in such scams.

Limit the fallout of a data breach or other cyber event

Reputation is everything. So when a cyber attack or data breach damages your clients' trust, it can threaten your ability to generate new customers and retain old ones, even if you do everything by the book. Cyber insurance can limit the reputational fallout of cyber events by giving you access to specialist PR firms that can help you through the process of notifying customers and by covering the future loss of profits caused by lost contracts and customers who choose to go elsewhere.



Case study

In 2017, an engineering firm was hit by the global outbreak of the ransomware known as WannaCry, which encrypted all the data files on their server. This included a catalogue of technical drawings, prints and complex design specifications for the various projects and bids they had worked on over the years.

Not only was this valuable intellectual property and the very foundation of their business, but they also often used modified versions of these previous drawings and specifications to help with marketing, preparing for bids and undertaking new projects.

> It soon transpired that the contingency plan – a cloud backup – had been failing for three years.

The company thought that they had a contingency plan in place for data recovery in the form of a remote cloud backup. However, it soon transpired that the policyholder's cloud backup had been failing for three years. This meant that the only option was for the data to be re-created from scratch at a cost of over $270,000. The loss was covered in full under our cyber insurance policy.

Ransomware is a disproportionately expensive type of cyber event. Although it makes up 13% of cyber claims by volume, it accounts for 27% of the total financial losses suffered due to cyber events.

Want a quote? Contact your broker today

Our cyber insurance policy covers

Cyber incident response costs

Giving you instant access to our cyber incident response partner network including IT forensics and security, legal and PR specialists, all available 24/7 through our hotline and mobile app.

Comprehensive cybercrime

Covering the financial loss for a broad range of cybercrime events including social engineering scams, invoice fraud, ransomware and targeted extortion.

System damage & system business interruption

Covering the costs associated with prolonged system downtime, restoring data, and getting your business back up and running after a cyber event.

Privacy liability & breach notification costs

Helping you manage the fallout if you lose confidential information.

Risk management services

Manage your cyber risk ahead of time using our range of free risk management tools.

Choosing your limit

76% of businesses in your peer group choose coverage limits of **between 500k and 2m ($/£/€)**

About CFC

With 20 years' experience, CFC was one of the first companies to offer cyber insurance and has one of the largest cyber underwriting and claims teams in the world. Our award-winning cyber insurance products and incident response services protect over 40,000 businesses in more than 60 countries.

Learn more at cfcunderwriting.com/cyber

Proactive →

Cyber exposure:

Client conversation starters

Before talking about cyber insurance premiums and the coverage available, it's important that clients first recognize some of the basic cyber risks faced by their business as many may not know where their major exposures lie or that insurance exists to cover them.

To help you get the conversation started, we've put together a handful of questions you can ask along with key talking points for each.

Do you send or receive wire transfer payments?

1

- **Cybercriminals are increasingly intercepting wire transfers**, often by hacking into email accounts, pretending to be someone else, and sending fraudulent instructions.
- **These scams are hard to spot** because cybercriminals are taking the time to study how their victims send and receive payment requests, and they often come from real email addresses.
- **Payments are rarely retrievable** as they are siphoned off into other accounts quickly. Banks rarely refund the losses.
- **Cyber insurance can refund the often significant financial losses** that come from scams like these. In fact, funds transfer fraud makes up about a quarter of CFC's cyber claims globally.

Do you collect or store personally identifiable information (PII) like credit card numbers or health information?

2

- If sensitive information that you are responsible for is lost or stolen, you will most likely **have to notify affected individuals** of the breach and provide credit monitoring services.
- When it comes to PII, there are a number of **rules and regulations** about how you collect, use and store that information. If you do not adhere to them, you could face regulatory fines and penalties.
- A malicious third party isn't always to blame. Often times, it's as simple as an employee **losing a company laptop**.
- **Cyber insurance covers the range of costs associated with data breaches**, like notifying affected individuals and your responsibilities under different regulations.
- **Even if you don't store PII, you probably store other business-critical information** on your systems. **See Question 3** to find out why this could pose a risk.

Do you store business-critical information on your computer systems, such as client contracts, designs and plans, stock levels and other corporate information?

3

- Even if you don't store a lot of customer records or credit card information, **you still likely have important information that you need regular access to**, from appointment bookings to intellectual property.
- What's more, if business-critical data becomes unavailable, it can have a serious impact on your ability to operate and ultimately your bottom line. **See Question 4 for more information** on business interruption.

Proactive →

How long can your business operate without access to computer systems and the data they hold?

4

- **You are probably more dependent on computer systems than you realize.**
- Understanding that modern businesses are partly or entirely reliant on technology in order to operate, cybercriminals increasingly see **ransomware attacks and targeted extortion attacks** as an easy way to make money. They do this by encrypting key data and demanding large sums of money in exchange for the decryption key.
- **Most small businesses lack to the technical resources** to deal with attacks like these in-house and may not have anyone experienced enough to turn to in the event that their systems are brought down.
- Our incident response team notes that the **average downtime is two to three days**, but that's with the assistance of technical experts. In worst case scenarios, businesses aren't fully operable for weeks or even months after a cyber event.
- **Backups are are frequently targeted and disabled in these attacks**, leaving businesses with little recourse when it comes to reinstating their data.
- **Cyber insurance not only gives you access to a range of technical experts** to help get you back online fast, but it covers the financial losses incurred as a result of your business being interrupted and the costs of re-creating any corrupted data. It can even cover the reputational impact of cancelled contracts and customers choosing to go elsewhere.

Do any of your employees work remotely?

5

- Whether good practice or not, **people reuse their passwords** across multiple platforms, so if a username/password combination is breached in one cyber attack, hackers most likely have combinations for future attacks.
- With login credentials already to hand, **cybercriminals can easily gain access to business email accounts** or even log into a company's remote desktop service (RDS).
- In addition, there's always the risk that work **devices taken outside of the office can be lost or stolen.**
- **Cyber insurance can cover the fallout from hackers gaining access to your emails** or systems, whether stolen funds, business interruption, or a privacy breach.

Are you confident that you or your employees will never make a mistake?

6

- Humans are the weakest link in the cybersecurity chain. In fact, **the vast majority of cyber incidents – for CFC, it's about 75% - involve some kind of human error** or oversight.
- This includes everything from being **tricked into giving over your username and password**, reusing passwords which makes account compromise easier, not following up wire transfer requests with a phone call, or losing devices containing sensitive information.
- Cyber insurance covers the financial losses that can result from these types of events as well as giving you **instant access to the right specialists** if someone makes a mistake. It also often comes with a range of **free risk security tools and employee training.**

← Reactive

Cyber exposure:

Client objection handling

By now, you may have spoken to your clients about their cyber exposures and perhaps even presented a quote for coverage. But they still aren't convinced.

To help you explain their cyber exposure and the value of cyber insurance as a form of protection, we've put together some of the most common client objections along with key talking points to help you respond.in handling each.

"We don't need cyber insurance. We invest in IT security..."

1

- **You're still likely exposed**. Not only are cyber threats continually evolving to bypass the latest security measures, but even large corporates who spend vast amounts on cybersecurity still routinely get hit.
- **People are still the weakest link in an organisation's IT security chain**. Approximately three quarters of the cyber claims we deal with involve some kind of easily-preventable human error.
- Theft of funds, ransomware, extortion and non-malicious data breaches **usually start with a human error** or oversight such as leaving a laptop on a train or clicking on a phishing link, which then allows cybercriminals to access your systems from the inside.
- Cyber insurance is a cost-effective way to not only get access to risk management tools like phishing-focused employee training programs, but also to **cover the financial loss if someone makes a mistake.**

"We outsource all of our IT, so we don't have an exposure..."

2

- Unfortunately, **using a third party for IT doesn't eliminate your exposure.**
- If you outsource your data storage to a third party and that third party is breached, you will still likely be **responsible for notifying affected individuals** and dealing with subsequent regulatory actions.
- What's more, many businesses rely on third parties for business-critical operations, and should those providers experience a system failure, **it could have a catastrophic effect on your ability to trade**, resulting in a business interruption loss.
- Most third-party technology service providers have **standard terms of service that limit their liability** in the event that a breach or system outage causes financial harm to one of their clients.

"We don't collect any sensitive data, so we don't need cyber insurance..."

3

- Two of the most common sources of cyber claims **aren't related to privacy at all – funds transfer fraud** is often carried out by criminals using fraudulent emails to divert the transfer of funds from a legitimate account to their own, while **ransomware** can cripple any organization by freezing or damaging business-critical computer systems.
- Neither of these types of incidents would be considered a data breach, but **both can lead to severe financial damage** and are insurable under a cyber policy.
- **Any business that uses technology to operate will have a range of other cyber exposures which a cyber policy can address.**

← Reactive

Cyber attacks only affect big business. We're too small to be a target...

4

- Although cyber attacks affecting large organizations are most often in the news, **over half of all cyber attacks are aimed at small businesses.**
- This trend is continuing to rise. In 2018, **attacks on small and medium-sized businesses rose by a staggering 424%.**
- Cybercriminals see smaller organisations as **low-hanging fruit** because they often lack the resources necessary to invest in IT security or provide cyber security training.
- Cyber insurance is a great solution for smaller organizations because not only does it cover the growing number of cyber attacks on these businesses, but it gives you **instant access to a number of technical and legal experts** needed following a cyber event, but who you might not have in-house.

Cyber is already covered by other lines of insurance...

5

- Cyber cover in traditional lines of insurance often **falls very short of the cover found in a standalone cyber policy**. While there may be elements of cyber cover existing within traditional insurance policies, it tends to be only partial cover at best.
- Property policies were designed to cover your bricks and mortar, not your digital assets; crime policies rarely cover social engineering scams - a huge source of financial losses for businesses of all sizes - without onerous terms and conditions; and professional liability policies generally don't cover the first party costs associated with responding to a cyber event.
- A standalone cyber policy is designed to **cover the gaps left by traditional insurance** policies, and importantly, comes with **access to expert cyber claims handlers** who are trained to get your business back on track with minimum disruption and financial impact.

Cyber insurance is too expensive...

6

- **Cybercrime rates are quickly overtaking traditional crime rates**, making cyber risk one of the most pressing business issues of today.
- For the **sizeable losses** you could be faced with – often in the hundreds of thousands – from stolen funds, lost revenue or considerable clean up costs, it is worth the extra insurance spend.
- **Cyber insurance gives you instant access to a wide range of technical specialists** who are experts at helping businesses quickly recover from cyber events. Policies also come with a range of **free cybersecurity tools** that you might spend hundreds or thousands on implementing yourself.