cfc

Cyber insurance guide

cfcunderwriting.com

As we become increasingly reliant on technology, the potential impact of cyber-related incidents continues to grow. Yet the cyber insurance market is relatively new in comparison with other lines of cover.

This straightforward guide explains how cyber risk and insurance has evolved and how a good cyber policy addresses these modern exposures.

Contents

Welcome to the cyber insurance guide

Foreword

Cyber is often cited as the number one risk modern businesses face today. But many Australian businesses have yet to come to terms with transferring their biggest risk to insurance – their intangible assets. Perhaps there is the belief that a cyber attack won't happen to them. Many say they're too small to be a target. Or, in more recent times, it's not worth investing in a policy that potentially won't respond – the cost-of-living crisis deterring an additional insurance spend.

Subsequently, we estimate that less than five percent of Australian businesses purchase a dedicated cyber insurance product to cover what is now their largest exposure, and with the exception of large, risk-managed corporations, that figure drops even further. An alarmingly low figure despite the major headlines, validated by financial reports and broker penetration rates across their portfolios.

And yet the Australian cyber landscape in the last few years has gone through an unprecedented amount of change. Gone are the days where cyber exposure was understood to only be a privacy risk or a 'big company' issue only affecting the retail and healthcare industries. Manufacturing, a vital industry to the Australian economy has been one of, if not the most impacted by cyber attacks despite holding little to no sensitive information.

Cyber threat actors have shifted from small scale social engineering scams to large scale extortion, targeting any business that is potentially vulnerable. These attacks can be costly, resulting in extraordinary amounts spent on everything from forensic analysis to data restoration, and in some cases the extortion demands themselves.

But with change, comes innovation. And never in the history of the market has an insurance product evolved so quickly to meet the needs of its customers. The product has evolved from a reactive to a proactive solution that works to prevent attacks, rather than just respond to them.

The 2023 year brings much more stability for insurance products, and capacity once again grows through both new entrants exploring the market for the first time, and traditional insurers expanding their appetite for business. Insurers are collaborating with government, the private sector – and even with each other – to combat cyber crime. As a market we must acknowledge that cybercrime isn't going away, but collectively we can equip businesses to manage and mitigate it.

At CFC, we're proud to say that our team has grown to more than 100 cyber underwriters around the world. Our cyber security and response division now includes almost 150 threat analysts, forensic specialists and security engineers spanning three continents, with a 'boots on the ground' presence in Australia that is unrivaled in size and expertise. These are the experts Australian businesses are buying access to through insurance, and the core of a good cyber proposition. Providing around the clock assistance to detect, prevent and respond to cyber security incidents for our Australian customers.

We hope this guide serves to take your understanding of cyber to the next level. Throughout this guide you'll find everything from how to articulate how cyber products work, case studies of real life cyber attack in action, and how to have more informed discussions about why cyber insurance is the most important coverage businesses will invest in today.

Our unwavering commitment to the Australian cyber market remains stronger than ever. We look forward to the years ahead as we continue to support and protect Australian businesses.

- Lindsey Nelson, Cyber Development Leader

**Anything highlighted in red throughout this guide will be defined in our easy to read cyber glossary at the end.*

What is cyber insurance?

Technology has revolutionised the world for businesses and individuals alike bringing monumental shifts in human behavior directly linked to technological advancements. From the way we shop, to the way we bank, to the way we work, our everyday life is anchored by technology.

For businesses, this technology revolution has brought unparalleled opportunities for efficiency, innovation and scale. It has also created new exposures and introduced the risk of cybercrime.

Cyber insurance exists to help protect businesses against the threat of cybercrime.

The risk to small businesses

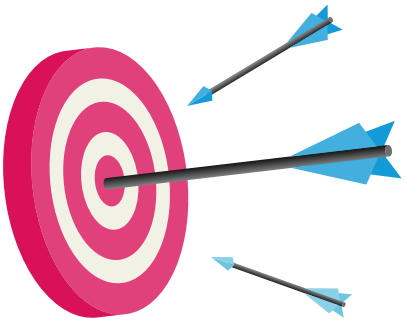
There's a common misconception that cyber attacks are only a "big business" problem, and it's easy to see why. Cyber attacks on larger businesses tend to grab the attention of the press because they involve familiar brand names and involve substantial amounts of customer data.

But thousands of smaller businesses suffer cyber incidents each year.

In fact, 96% of all cyber attacks are directed at small and medium-sized businesses.

Here's why:

- **Small businesses are low-hanging fruit:** Cyber criminals look for the easiest and fastest way to be successful. Smaller organisations may have less resources and time to train staff on cybersecurity risks, which makes them more susceptible to attacks like social engineering. They're also more likely to pay ransom demands when they feel like they don't have anyone to turn to for help.



- **Small businesses can be the gateway to larger organisations:** Many small and medium sized companies are connected to the IT systems of larger partner organisations. So, when cyber criminals want to infiltrate larger and more secure organisations they often target their suppliers. What's more, many of these IT relationships are identifiable through publicly available data.

- **Small businesses can be collateral damage:** If a cyber attack is launched against a large partner or technology provider, the smaller businesses that rely on those organisations can also be adversely affected. This could involve disruption to their business, breached data, or even reputational harm.

Threat actors are looking to target companies who are vulnerable, rather than valuable.

The role cyber insurance plays in tackling ransomware

> Ransomware is an increasingly serious threat to businesses and is one of the primary drivers for businesses to transfer what is now one of their top business risks to insurance.

Over the years, these attacks have become more frequent and more severe. Since 2020, the average ransom demand has increased by 100%. (Coveware report, 2022)

There are many reasons why this crime continues to develop:

- Some companies have yet to implement adequate cyber security controls or invest sufficiently in IT security. This makes them lucrative, easy targets with a high reward for the criminal.

Drug traffickers in 1992 were 625x more likely to get arrested than a ransomware threat actor in the last year! (Coveware, 2022)

- The media may sometimes demonise businesses that fall victim to ransomware, making them fear negative publicity and fueling their desire to pay rather than be “outed”.
- Tough privacy regulations and the accompanying fines have made extortion even more lucrative for criminals.

The cyber insurance industry is playing a critical role in tackling ransomware. Many prominent cyber insurance companies actively collaborate with global law enforcement as well as other public and private cyber security organisations to share threat intelligence, identify active ransomware groups and standardise how to respond to ransom demands.

Are businesses with cyber insurance more likely to pay ransom?

The opposite is more often true. Businesses supported by a cyber insurance policy have access to experts who can guide them through the incident and will attempt to recover their systems or data so that paying a ransom becomes the last resort. On the other hand, many small businesses without these resources assume that they have no other option but to pay.

Cyber as a service

The evolution of cyber insurance

> A decade ago, cyber insurance was all about policy wording and reactive solutions. A data breach would happen and the policy would work to step in and respond with a team of experts.

But in the last few years, the cyber insurance market has shifted to a more technically-led and service-oriented solution, one that aims **to prevent cyber incidents from happening and respond quickly in the event they do.**

What are the core components of a good cyber insurance policy?

- **Proactive services:** These are the preventative services a cyber insurer can provide 24/7 throughout the policy term to prevent a cyber-attack from happening to a business.
- **First party sections (your company's own losses):** These cover the insured's own financial loss arising from a cyber event, CFC defines this as any actual or suspected unauthorised system access, electronic attack or privacy breach, or system downtime.
- **Third party sections (your liabilities to others):** These cover the business for liability actions against them arising out of a cyber event.
- **Incident response services:** These are technically-led response and resumption services that step in when a cyber claim or incident is notified. For businesses; these are the insurer teams that help the computers back on and get you up and running asap.

Cyber policies now work to protect businesses from cybercrime from the very first day they buy cover with their insurer, not only when they make a claim.

In simple turns, you can think of a cyber insurance policy as:

- A modern-day crime policy
- Coverage for a company's intangible assets
- Access to a team of experts who work to prevent cyberattacks and provide security advice
- A service of technical experts working to get businesses back up and running following a cyber event

Proactive protection and response

> Insurers' cyber security, technical expertise and real-world experience can make the difference between suffering a catastrophic loss or keeping a business trading.

Recognising this, the cyber insurance market has moved towards providing technical cyber security resources as part of their policy, to help protect customers from cyber threats and reduce the impact (and cost) should one occur.

There are two critical cyber security services, businesses and brokers may want to consider when looking for a comprehensive cyber insurance policy. These would ideally be in-house and in addition to the policy coverage:

- **Proactive monitoring and remediation:** A preventative service with the aim to identify potential threats – through device scanning, dark web monitoring and threat intelligence feeds – and remove them before they can harm the business. Ideally this would be provided throughout the policy period.

- **24x7 cyber incident response:** A reactive service offering immediate, technical response to a real or suspected cyber event. This usually includes a team of forensic analysts, cyber security engineers, ransom negotiators and business resumption specialists that triage the incident, contain the threat and repair systems to get the business back online.

Why an in-house cyber-security team is vital

It keeps the insurer and business interests in line with ensuring they are motivated by getting businesses back operationally. Cyber incidents are almost always technical incidents, and require technical expertise by a team who sit with the same intentions as claims and underwriting. In-house expertise also means they understand the principle of indemnity, and can provide clear guidance on services that are covered by their insurance policy rather than costs for services in addition to that will surprise clients.

Threat intelligence vs. vulnerability scanning

Simply put, cyber **threat intelligence** is the data that companies receive about potential cyber attacks and the threat actors operating at any given time. This insight is then analysed and used to determine whether a company is at risk and how to prepare for and ideally prevent an attack from happening.

In the cyber insurance market, threat intelligence is often confused with vulnerability scanning, another valuable but entirely different technology, and it is important to understand the difference.

Vulnerability scanning is the process of identifying a company's internet-facing assets and looking for weaknesses, like unpatched software or open ports. **It's the equivalent of inspecting a house to see if there are unlocked doors or open windows.** Vulnerability scanning is often used to underpin cyber risk reports.

Threat intelligence, on the other hand, combines insights from the dark web, government and other third-party cyber security sources, as well as cyber claims data to identify the types of attacks most likely to take place, the threat actors carrying out those attacks and the potential victims.

Vulnerability scanning is purely internal-facing, while threat intelligence looks outward to understand what threats are on the horizon.

By combining threat intelligence with vulnerability scanning, you can more effectively predict cyber attacks and prioritise the vulnerabilities to remediate, ultimately preventing losses and disruption to the business.

Proactive cyber services benefit both businesses and brokers:

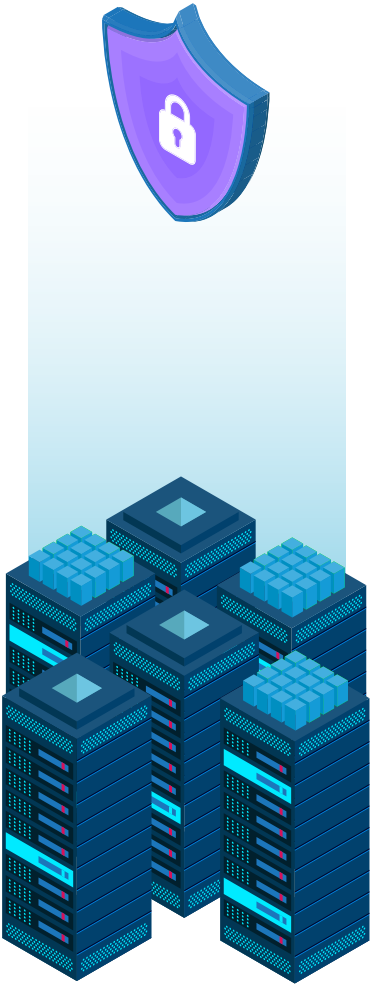
For businesses

- Cyber security and protection from the day the policy begins
- Cyber security guidance improves your position and prevents criminal threats occurring
- Inclusive cyber security services means businesses get value from their insurance policy even when they don't make a claim

For brokers

- **Market sustainability.** Reducing cyber attacks for businesses not only means good value for your customer, but sustainable loss ratios mean product coverage stays broad
- **Streamlined underwriting.** Technical services like threat intelligence and scanning can increasingly reduce the need for long application forms
- **Greater cyber expertise.** Explaining how cyber products work in real-life improves your cyber knowledge and helps demonstrate value to clients.

Our hypothesis is that businesses are safer with a cyber policy than without one.



Did you know?

Each year CFC prevents hundreds of cyber attacks by identifying threats and remediating client vulnerabilities before they turn into claims. This equates to tens of millions of pounds saved in potential losses. Here's a look at one of those cases:

Cobalt Strike is a penetration testing toolkit originally created for ethical hackers but is now used by cyber criminals. The toolkit allows the attackers to place an agent, called a beacon, on a target network. From there, the attacker can perform a variety of exploitations and attacks including the execution of malware.

Through our bespoke network of threat intelligence sources we were alerted that a new Cobalt Strike beacon had been activated on a target network. Our in-house cyber security team identified where the beacon was located and discovered that it belonged to our insured, a childrens hospital.

The activity we then witnessed indicated that the attacker had created administrative accounts and was using unauthorised access to exfiltrate data and prepare for a ransomware attack.

With the insured's permission, our team worked tirelessly to remove the foothold that the attacker had in the environment. Based on our ransomware claims data, a hospital of this size could have faced a ransom demand of up to $4,000,000, had the attack been successful.

In our final correspondence with the insured they said, *"it is apparent that the quick actions yesterday based on the intel received may have very well have prevented this from being much worse."*

Why security controls are important

It's becoming increasingly common for cyber insurers to require potential customers to adopt basic cyber security controls in order to obtain the best terms for their business. This is because the majority of successful cyber attacks, and therefore cyber claims, can be traced back to the exploitation of common security weaknesses for which there are widely available solutions. Cyber insurers want to ensure that their clients can avoid the very basic and most common incidents.

Brokers aren't expected to be both insurance and cyber security experts, and businesses have multiple facets of their operations to be responsible for. But, it is important to have a basic understanding of the common security controls that a business may be required to deploy.

Cyber security controls fall into three groups:

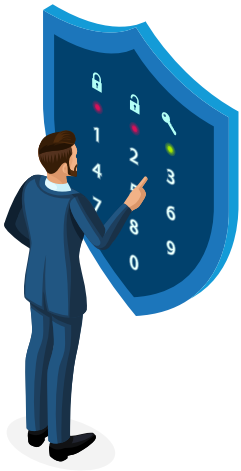
Preventative controls – improve weaknesses in information systems to prevent you from experiencing a cyberattack in the first place, for example, patch updates, firewalls, encryption, physical barriers and multi-factor authentication.

Detective controls – alert businesses to attempts to infiltrate their networks and can warn when a cyberattack occurs, for example antivirus and intrusion detection software.

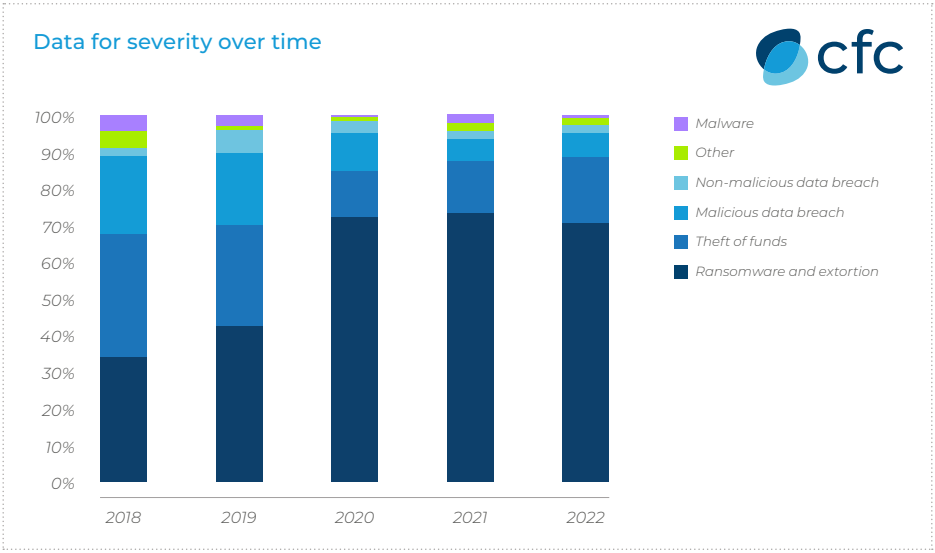
Corrective controls – are used after a cyber incident to minimise the impact and help restore as quickly as possible, for example, back-ups.

A good cyber insurer will have the technical capabilities in-house, with experts who make themselves available to explain key concepts and provide support to customers.

More information on common cyber security terms can be found in the glossary at the end of this guide.



Types of cyber claims



More than 95% of cyber claims are for losses for your own business, and they fall into three broad categories:

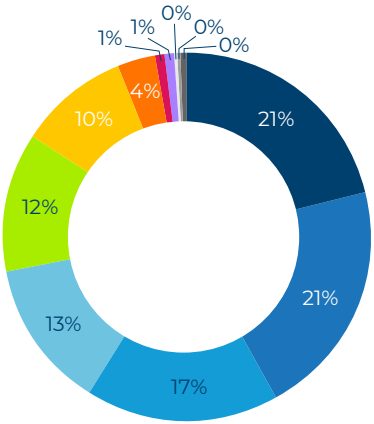
Theft of funds

This is straight-forward theft of money from a company's bank account. The fact that nearly every business can now move its money around electronically and remotely means that it is much easier to steal. Instead of stealing physical funds, criminals are increasingly stealing electronic funds through social engineering scams. And if a business has somehow been negligent in allowing this to happen, their bank may not reimburse them.

Theft of data

Data is valuable, and if something has value, it is worth stealing. Identity theft has reached record levels around the world and in order to commit identity theft, criminals need data. Seemingly innocuous information such as names and addresses stored on a computer network can be worth more money than you think.

Occurrences in past 5 years



- *Theft of funds*
- *Data breach other*
- *Ransomware*
- *Other*
- *Data breach - hack*
- *Data breach - phishing*
- *Malware - other*
- *DDOS attack*
- *IP infringement*
- *Copyright infringement*
- *Errors and omissions*
- *Extortion*

Damage to digital assets

In order to operate, businesses now have an incredibly high dependency on their systems, and criminals know that. By either damaging or threatening to damage a firm's digital assets, attackers know that they can extort money from their victims who might prefer to pay a ransom rather than see their business grind to a halt. And even after paying up, the victim is often left with systems that are unusable and costly to fix.

Cyber policies in action

CFC handles thousands of cyber claims each year. While ransomware has dominated the headlines in the last few years, there are a variety of cyber-attacks that can impact a business.

Social engineering

A financial controller in a law firm in Melbourne received a call from someone purporting to be from the firm's bank, explaining that some suspicious wire transfers had been flagged on the business account. The caller insisted the funds had been stolen, and to prevent further losses a password and pin code would be required to freeze the account.

The financial controller confirmed the pin code and password, and the caller confirmed that the freeze had been applied and that they would be in contact once the situation was resolved. However, upon calling the bank the next day, the financial controller was told that the bank had not in fact been in contact and that $170,000 had been wired out of the account and was too late to recall.

Because the transactions had seemingly been authorised, no reimbursement was offered by the bank. Fortunately, the law firm had purchased a cyber insurance policy containing cybercrime cover with social engineering and was able to recover the full amount from insurers less their policy deductible.

Business interruption

A haulage company based in Perth suffered a ransomware attack where cyber criminals encrypted all of their data files including their routes, logistical information, key contacts, and stock quantities – as well as their payment processing capabilities. The hackers then requested a ransom of over $17,000 in exchange for the decryption key.

The business refused to pay the demand and instead, set about reconstituting data from a collection of paper records and their employees' knowledge of operations, though this resulted in a large amount of overtime costs. What was worse, however, was the loss of business income that resulted from the extended outage of their systems and the consequential impact on operations.

Due to the attack, the business was down 80,000 sales in the month following, this amounting to nearly $1.7 million in revenue lost. Fortunately, after adjustment by their cyber insurance provider, the business was able to recover nearly all of the financial loss suffered under their policy.

Data breach

A private healthcare clinic was the victim of a cyberattack where patient information had been stolen. Hackers were threatening to post the data on a public website unless they received a ransom payment of $23,000 in Bitcoin.

They called their cyber insurers and immediately the insurer's in-house incident response team was able to step in. They advised the clinic's IT team on what to do in order to fix the immediate vulnerability and also pulled in an IT forensics company to verify the legitimacy of the attackers' claim. After an investigation, it was determined that data relating to 3,000 patients had been compromised, but luckily no sensitive medical data had been accessed.

Consequently, the decision was made not to pay the ransom demand. Instead, the insurer connected the company with a crisis communications consultant. They recommended to still notify affected patients to prevent any adverse reputational impact and assisted with the construction of a notification notice.

They have heard nothing further from the hackers to date. The clinic's cyber insurance policy covered costs of the IT forensics company, and the crisis communications company for a total claim of $34,500 less the small policy deductible.

Ransomware

A hacker accessed a Brisbane school's computer system via a weak remote desktop protocol (RDP). These ports, allow remote users to connect to the desktop of another computer through a network connection, and when unsecure they can allow hackers to gain unauthorised access. With initial access gained they then proceeded to launch a brute force attack, using a computer program, which attempted numerous possible password combinations in rapid succession to crack the password for further systems.

Once in, the hacker unleashed ransomware across the school's computer systems. The malware encrypted multiple servers and locked the school out of its systems and back-up servers, rendering the school inoperable. The hacker then demanded a payment of 2 bitcoin for the decryption key.

Fortunately, CFC's incident response team swiftly stepped in to help the school regain access to their systems. They were also able to determine the hacker's main motive, which appeared to be financial gain rather than the theft of sensitive data.

Based on this information, the school's CFC cyber policy was able to cover all incurred damages from the ransomware attack, including root cause analysis, network security assessment, forensic investigation and legal counsel.

Choosing a cyber insurance provider

> Today's cyber insurance products go beyond words on paper... or at least, they should. Here are a few things – in addition to policy language - that brokers and businesses might look for when choosing a cyber insurance provider.

In-house cyber security and incident response: Comprehensive cyber insurance policies are backed by a technical team that is actively helping to prevent cyber claims from happening as well as prepared to remediate an attack and limit the impact. Proactive, preventative services are available to you throughout the lifecycle of the policy, not just at the outset. Businesses are encouraged to look for incident response that is led by a technical team.

A documented process for handling ransom demands and sanctions: Ransomware is top of mind and one of the leading sources of claims. It's important to consider whether your cyber insurance provider has a clear process regarding ransom payments and sanctions checks before they advise your clients making a payment. This is a quick way to gauge whether the provider has been involved in many ransomware claims.

Meaningful claims experience and data to back it up: When businesses are considering insurance providers, look for one that not only has substantial claims handling and incident response experience, but data that they're willing to use to identify potential trends, threats and targets to help prevent future claims.

Debunking cyber misconceptions

In the past there have been some misconceptions around what cyber insurance is and what it can offer in way of protecting a business. As cyber is now one of, if not the largest exposure for any business, it's important to overcome these misconceptions and shed some light on the true value of the cyber offering.

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

Similar to when a business installs security cameras and sprinkler systems, they still purchase property insurance in case those precautionary measures fail. Cyber insurance works the same. IT security is a great precautionary measure, but hackers can still gain access and cause damage regardless.

Cyber threats continually evolve to the latest security measures, and even large corporates who spend vast amounts on cyber security still routinely get hit.

Theft of funds, ransomware, extortion and non-malicious data breaches usually start with a human error or an oversight like losing a laptop or clicking on a phishing link, which then allows cybercriminals to access your systems.

Ultimately, the cyber landscape is everchanging; no matter how much a company invests in IT security, they will never be 100% secure. Cyber insurance is there to add another layer of protection and respond in the event that the worst happens.

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

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...

You don't need to be collecting sensitive data to have cyber exposure. In fact, any business that relies on a computer system to operate, whether for business-critical activities or simply electronic banking has a very real cyber exposure.

Two of the most common and costly sources of cyber claims are ransomware and funds transfer fraud. Funds transfer fraud is often carried out by criminals using fraudulent emails to divert legitimate fund transfers to their own accounts, whilst ransomware can cripple any organisation by encrypting or damaging business-critical computer systems.

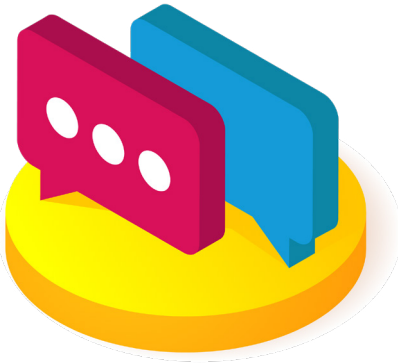
Neither of these types of incidents needs to involve a data breach, but both can lead to severe financial losses which are insurable under a cyber policy.

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

Cyber cover in traditional lines of insurance often falls very short of the cover found in a standalone cyber policy. Moreover, in many commercial policies there are 'total' cyber exclusion clauses.

Property policies were designed to cover your bricks and mortar, not your digital assets - and more recently, go as far to specifically exclude cyber events through affirmative exclusions. Equally 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 for intangible risks, 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.



Glossary of terms

Application whitelisting
A security solution that allows organisations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

Antivirus
A product that can detect and prevent malicious software on computers, laptops and other tech devices.

Asset inventory
A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Brute force attack
A method whereby threat actors submit multiple password attempts in rapid succession until they successfully gain entry into business networks.

Cloud
A virtual space on the internet used for storing digital resources instead of on local computer networks. Clouds can be public, private or hybrid, each with pros and cons. Examples include Google Drive, Apple iCloud, Netflix, Amazon Web Services (AWS), Dropbox and Microsoft OneDrive.

Custom threat intelligence
The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organisations with intelligence on cyber threats and cyber threat actors pertinent to them.

Cyber
Relates to or characteristic of the culture of computers, information technology, and virtual reality.

Cyber attack
An unauthorised attempt by hackers to damage, destroy, alter or exploit a computer network, system, or employees.

Cybercrime
Extortion by phishing, ransom attacks, social engineering or losses caused by malware or DDOS.

Cyber event
Actual or suspected unauthorised system access, electronic attack or privacy breach.

Cyber insurance
Cyber insurance exists to help protect businesses against the threat of cybercrime.

Cyber security
The technologies, processes and controls used to protect and support information technology (IT).

Cyber threat analysis
The dedicated team typically provided by a cyber insurer to help detect, prevent and stop cyber attacks from affecting businesses before they fall victim.

Database encryption
Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss prevention
Software that can identify if sensitive data is being exfiltrated from a network or computer system.

DDoS mitigation
Hardware or cloud based solutions used to filter out malicious traffic associated with a Distributed Denial of Service (DDoS) attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC
An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering
A specific technique to block access to known bad IP addresses by users on your network.

Email filtering
Software used to scan an organisation's inbound and outbound email messages and place them into different categories, with the aim of filtering out spam and other malicious content.

Employee awareness
Training programmes designed to increase employees' security awareness. For example, programmes can focus on how to identify potential phishing emails.

End user device
Any computer or mobile device used by the end customer.

Endpoint protection
Software installed on individual computers (endpoints) that uses behavioral and signature based analysis to identify and stop malware infections.

Extortion
A crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack.

Firewall
Hardware solutions used to control and monitor network traffic between two points using predefined parameters.

Incident response
An organized approach involving technical, legal and claims expertise to address and remediate a cyber incident. These are typically offered by a cyber insurer as the full suite claims service.

Incident response plan
Action plans for dealing with cyber incidents to help guide an organisation's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system
A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Malware
Includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals.

Managed service provider
A third party organisation that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

Mobile device encryption
Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Multi-factor authentication (MFA/2FA)
Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Network
Two or more computers linked to share electronic communications, resources and file exchanges.

Network monitoring
A system, utilising software, hardware or a combination of the two, that constantly monitors an organisation's network for performance and security issues.

Next-generation firewalls
Software or hardware solutions that combines traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems and anti-virus.

Patching
Applying updates to software to improve security and/or enhance functionality.

Penetration test (pen test)
Authorised simulated attacks against an organisation to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls
Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Phishing
Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Ransom attacks
The act of using malicious software to freeze or encrypt a victims data until they pay the requested demand.

Ransomware
Malicious software that freezes data so the attacker can threaten to publish it on a public domain. Or render systems and data unusable until the victim makes a payment.

Response app
A proprietary app offered by cyber insurers (CFC) to allow for threat intelligence alerts notifying policyholders of a potential vulnerability or compromise.

Remote desktop protocol (RDP)
RDP is a proprietary Microsoft protocol that allows a user to access their desktop and computing resources remotely from another computer. It is also sometimes referred to as Terminal Services.

Security info and event management (SIEM)
System used to aggregate, correlate and analyse network security information – including messages, logs and alerts – generated by different security solutions across a network.

Security operations centre (SOC)
A facility that houses an information security team responsible for monitoring and analysing an organisation's security posture on an ongoing basis. The SOC team's goal is to detect, analyse and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. SOC's can be internal and run by the organisation themselves or outsourced to a third party.

Social engineering
Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Supply chain partner
A third party who businesses depend on to operate, with services including but not limited to hosting, platforms, software or file storage.

System failure
Sudden, unexpected and continuous downtime of computer systems which renders them incapable of supporting normal business functions.

Threat actor
An individual, or group of individuals, intending to maliciously cause harm to a company's intangible assets and digital operations.

Threat intelligence
The collection and analysis of data from open source intelligence and dark web sources to provide organisations with intelligence on cyber threats pertinent to them.

Trojan
A type of malware or virus disguised as legitimate software that is used to hack into the victim's computer.

Virtual private network (VPN)
A VPN is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. Most commonly used to provide a secure remote connection to an organisation's network.

Vulnerability
A weakness or flaw in software, systems or processes. A threat actor may seek to exploit a vulnerability to gain unauthorised access to a system.

Vulnerability scans
Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall
Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering
The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organisation. For example, known malicious websites are typically blocked through some form of web content filtering.

Zero-day
Vulnerabilities that are discovered by threat actors before vendors become aware of it. These can then be exploited before patch updates are made available to businesses.

About CFC

CFC is a specialist insurance provider, pioneer in emerging risk and market leader in cyber. Our global insurance platform uses cutting-edge technology and data science to deliver smarter, faster underwriting and protect customers from today's most critical business risks.

Headquartered in London with offices in New York, Austin, Brussels and Brisbane, CFC has over 500 staff and is trusted by more than 100,000 businesses in 90 countries. Learn more at cfcunderwriting.com and LinkedIn.

To contact us, please email inbox@cfcunderwriting.com or dial 0207 220 8500. Our cyber team can be reached via email on cyber@cfcunderwriting.com.

All information in this booklet is correct as of 01 January 2023. We take great pride in our professional expertise on cyber insurance and as such would like to state that certain content within this guide is liable to become outdated due to the fast-paced nature of the cyber security and insurance market.