British Insurance Brokers' Association

The cyber insurance guide

Helping businesses prevent and survive cyber attacks

cfc

cfc.com

Updated May 2026

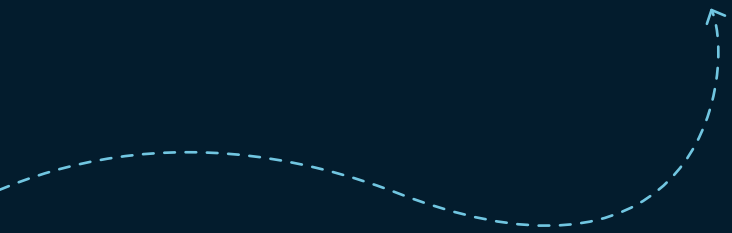
Introduction from **BIBA**

In BIBA's 2026 Manifesto we continued to highlight cyber as one of the most significant and financially disruptive threats to UK businesses. We also committed to help more brokers and their customers engage with cyber insurance. Working together with CFC, we are pleased to update our guide on cyber insurance. This guide is a helpful tool for insurance brokers to support businesses who might not have had the confidence or seen the need to engage with cyber insurance so far.

Without a doubt, CFC is a pioneering cyber insurance provider and scheme partner to BIBA. In the guide, you will learn about a threat landscape that actively targets small businesses and is willing to follow through with threats, but also how cyber insurance as a service makes it straightforward to protect businesses from criminal attacks.

To help brokers help customers understand the importance of cyber insurance.

Graeme Trudgill
Chief Executive Officer, the British Insurance Brokers' Association (BIBA)



Contents

Foreword

The UK cyber market is at a genuine inflection point. Cyber is now consistently cited as the number one risk facing businesses, yet cyber insurance remains one of the most misunderstood products in our industry. Rapidly evolving threats, combined with technical language and complex products, have made it difficult for many to engage with it confidently.

The reality is stark. Businesses are far more likely to suffer a ransomware or social engineering attack than experience a major property loss. As a result, cyber insurance has shifted from a reactive product to a proactive solution that not only responds to financial loss but helps to stop attacks impacting and mitigate that impact when they do occur. Organisations are increasingly targeted not because they are valuable, but because they are vulnerable, making strong cyber risk management essential.

Nowhere is this more evident than in the SME market, which represents the biggest opportunity for growth in UK cyber insurance. Cyber risk is front and centre for SMEs, but this opportunity will only be realised if the industry simplifies products, leads the conversation, and makes cyber insurance easier to understand and access. Brokers, insurers, and security partners all have a role to play, and collaboration has never been more important.

At CFC, we continue to invest heavily in this space, with over 100 cyber underwriters globally and more than 200 cyber security and incident response specialists operating around the clock. With this guide, BIBA and CFC aim to deepen brokers' understanding of cyber risk, from how products work to why cybercrime exists and how we can tackle it together. The moment is now. Let's seize it.

Lindsey Maher
Head of Global Cyber Development, CFC

What is **cyber insurance?**

Cyber insurance is designed to protect businesses from the financial, operational and reputational impact of a cyber event. As more data and systems move online, cyber attacks like ransomware, data breaches and scams are a real risk for businesses of every size, not just large organisations.

Today's cyber insurance cover more than just the costs to recover from an attack. Comprehensive policies may be designed to help protect businesses from attacks in the first place, respond quickly if something does happen, and get businesses back up and running with minimal disruption.

Cyber insurance is an essential part of running a resilient business, helping organisations protect their operations, customers, and growth.

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

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

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, SMEs are targeted nearly 4x more than large organisations*

Here's why:

- **Small businesses are low-hanging fruit:** Cybercriminals look for the easiest and fastest way to be successful. Smaller organisations may have less resources and time to train staff on cyber security 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 cybercriminals 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 target companies who are vulnerable, rather than valuable

*Verizon 2025 Data Breach Investigations Report

Cyber as a **service**

Cyber insurance used to be reactive, stepping in only after a breach occurred. Today, it is a technically led, service-driven solution that helps prevent incidents, responds quickly when something goes wrong, and supports recovery. A good cyber policy works as a complete system, combining prevention, response and recovery.

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

- **Proactive cyber attack prevention services:** These are the preventative services a cyber insurer can provide 24/7 throughout the policy term to try and prevent a cyber attack from happening to a business.

- **Incident response & claims services:** These are technically led response and resumption services that step in when a cyber incident or claim is notified. The incident response team triage, contain and remediate the event at a technical level, while the claims team works in parallel to coordinate any additional technical, legal or PR support required and ensure all services are covered under the policy.

- **Broad coverage:** Cover to reimburse for the financial and operational impact of an attack. This may include cybercrime losses such as extortion, funds transfer fraud and social engineering, as well as the costs of repairing or recreating systems and data. If operations are disrupted, cover can respond to lost income and increased costs while the business recovers.

Cyber policies now work to protect businesses from cybercrime from the very first day they buy cover and throughout the policy period, not only when they make a claim.

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

- A modern-day crime policy designed for digital threats and risks
- Protection for a company's systems and data
- Access to cyber security specialists who help prevent attacks
- A technical response service that gets businesses back up and running following a cyber event

Coverage points to look out for

When comparing policies, it can be hard to tell the difference between an OK policy and a great one – especially when it comes to coverage. These are key points worth questioning.

Incident response

Look for policies that provide immediate access to technical responders to triage and contain the event, and then get systems back up and running. Ideally, incident response costs should sit in a separate limit, be available from day one and come with a nil deductible so recovery can start immediately.

Ask the underwriter: Are incident response costs included as a separate limit and with nil deductible?

Cybercrime cover

A strong cyber policy could reimburse losses from funds transfer fraud and cyber extortion. Check carefully for warranties, call back requirements or minimum security conditions that could restrict cover, and ensure protection extends to common fraud types like push payment scams.

Ask the underwriter: Do you have a warranty statement that requires insureds to have certain cyber security measures in place?

System damage and business interruption

Cyber cover may pay for restoring systems, recovering data and replacing lost income after an attack. It is important to confirm the policy covers data recreation, not just restoration, as rebuilding lost data can be one of the most expensive parts of a claim.

Ask the underwriter: Do you cover costs for data recreation, not just recovery?

Unlimited reinstatements

In a world of repeat attacks, policies should automatically reinstate limits after each claim. This ensures the business remains protected throughout the policy year, even if multiple cyber incidents occur.

Ask the underwriter: Do you offer a new limit for each unrelated claim?

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.

You can think of in built proactive cyber attack prevention as neighbourhood security for a business network.

Rather than waiting for an attack, threats are spotted early through constant monitoring, intelligence gathering and vulnerability scanning. Additionally, through claims data, dark web monitoring and real time alerts, risks are identified and flagged before damage is done, helping businesses prevent incidents, not just recover from them.

- How does proactive cyber attack prevention work?
  A cyber attack preventative service with the aim to identify potential threats and stop them before they occur. This can be done using tools and services like vulnerability scanning, deep & dark web monitoring and threat intelligence feeds, to identify risks and alert businesses to issues that require action. This should be on the minute the policy is bound and active throughout the policy period.
- How does 24×7 cyber incident response work?
  A reactive service of 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.

Benefits of **proactive cyber services**

Proactive cyber services benefit both businesses and brokers

For businesses

- **Protection throughout the policy.** Cyber security and protection that starts working from the day the policy binds, not just when a claim is made.
- **Access to cyber security experts.** Practical, expert guidance with alerts focused only on threats that are likely to turn into an incident.
- **Getting value from your premium.** Cyber security services included as standard that would typically cost thousands if bought separately.

For brokers

- **Greater cyber confidence.** Gives brokers confidence that their clients are well protected, while helping reduce the frequency and impact of cyber events across their portfolio.
- **Stronger client relationships.** Even when a claim is paid, the disruption of a cyber incident can strain client relationships. Proactive protection helps stop attacks before they happen, keeping trust and relationships intact.
- **Streamlined quoting and binding.** Technical insights from threat intelligence and vulnerability scanning support more accurate pricing and faster, simpler application journeys.
- **Proving the value of cyber insurance.** Built in services at no extra cost make the value of cyber insurance tangible, supporting clearer, more positive conversations with clients.

Businesses with cyber insurance are better protected, better supported, and more resilient than those without it.

Did you know?

Each year CFC prevents thousands of cyber attacks by identifying threats, alerting customers and remediating the threat before it can cause harm and turn into a claim. This equates to reduced stress and millions of pounds saved. Here's a look at one of those cases.

A zero-day vulnerability was identified in software provided by a global cyber security vendor, widely used by businesses across multiple sectors. A zero-day vulnerability is a serious weakness found in a system, but is so new, no patch exists yet to patch it. If exploited, attackers could gain unauthorised access to systems, enabling cybercrime such as ransomware or data theft.

Through our exclusive threat intelligence sources, our in-house cyber security team was alerted to the vulnerability as soon as it emerged. The team quickly identified the insureds within our portfolio who were using the affected software and therefore at risk. Acting immediately, we provided clear, step-by-step guidance to those businesses to help them secure their systems and close the vulnerability before threat actors could take advantage.

Using our Response app and direct communications, impacted insureds and brokers were notified the same day the vulnerability was disclosed. This enabled businesses to take prompt action, significantly reducing the risk of compromise while commercial security vendors were still developing detection tools and patches.

By identifying the risk early and acting fast, disruption was avoided for affected insureds. This incident demonstrates how proactive cyber services help prevent attacks before they escalate into claims, reinforcing the value of always-on protection built into a cyber insurance policy.

Why **security controls** are important

It's common for cyber insurers to encourage strong cyber security controls as part of a cyber insurance programme. This is because around 3 in 4 CFC cyber claims are driven by human error, often linked to basic, well understood security weaknesses that can be reduced with the right controls and guidance. The aim is not to burden businesses, but to help them avoid the most common and avoidable incidents.

Brokers are not expected to be cyber security specialists and know what security measures insurers look for. However, having a basic understanding of common cyber security controls helps support better conversations with clients and reinforces the value of cyber insurance as part of wider business resilience.

Cyber security controls generally fall into three categories:

Preventative controls: These are designed to reduce weaknesses in information systems and lower the likelihood of a cyber attack occurring in the first place. Examples include timely patching, firewalls, encryption, physical security controls and multi-factor authentication.

Detective controls: These help identify suspicious activity or attempted intrusions. Controls such as antivirus software, network monitoring and intrusion detection systems which alert businesses to potential threats.

Corrective controls: These are used after an incident to minimise disruption and support recovery. Back-ups are a key example, enabling data and systems to be restored and businesses to resume operations.

While these controls are strongly encouraged as good cyber practice, it's good to know that **CFC does not impose warranties or conditions requiring specific cyber security measures to be in place.**

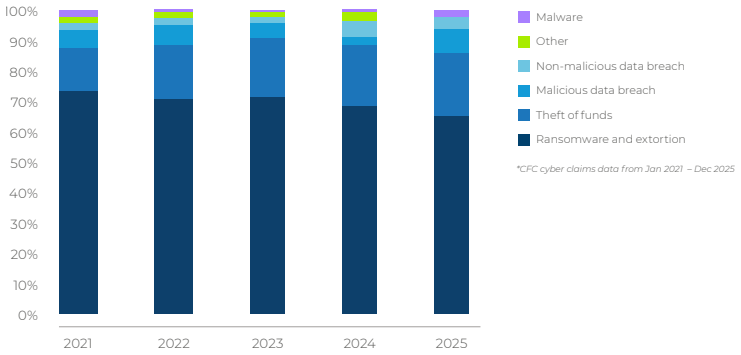
A strong cyber insurer will also have in-house technical expertise, with cyber specialists available to recommend and explain these controls to customers and brokers.

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

Types of **cyber claims**

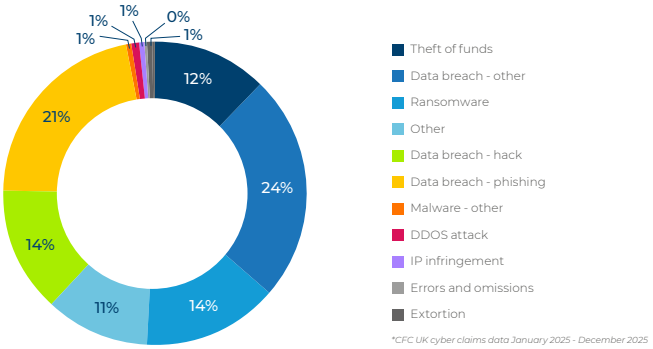
We analyse our claims by looking at both how often they occur, and how costly they are. These graphs highlight severity trends over the past five years, as well as claim frequency in the UK in 2025.

Claims severity over time



CFC cyber claims data from Jan 2021 – Dec 2025

Frequency of claims types in the UK



CFC UK cyber claims data January 2025 - December 2025

When looking at the type of attacks businesses are suffering, we can review our claims data and identify some key trends:

1 Data breaches are most common

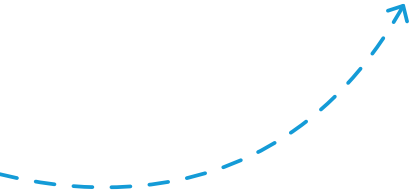
A data breach occurs when valuable information is accessed, stolen or exposed without authorisation. If data holds value to a company, it holds value to the hacker. Personal information like address and bank details are commonly thought of, but data can be manufacturing or building designs, confidential IP or even operational data that keep systems ticking. Breaches commonly arise through hacking, phishing or other accidental or operational failures. While typically less costly than ransomware, data breaches remain highly prevalent and can carry significant regulatory, financial and reputational impact.

2 Ransomware is the most costly

Ransomware is a cyber attack where criminals gain access to a business's systems, encrypt data and demand payment to restore access or prevent data from being leaked. It typically enters through phishing, compromised credentials or unpatched vulnerabilities. While not the most frequent attack, ransomware is CFC's most persistently costly claim type, driven by business interruption, recovery costs and the complexity of restoring operations.

3 Theft of funds is common and costly

Theft of funds refers to criminals tricking a business into transferring money electronically to a fraudulent account. One of our most common claim types, attacks usually rely on social engineering, such as fake supplier emails or impersonation of senior staff, rather than technical system failure. Because payments appear authorised, funds can be hard to recover, making this one of the most common and costly cyber losses businesses face.



Supply chain risk for SMEs

What is cyber supply chain risk?

Cyber supply chain risk is the risk that enters a business not through a direct attack, but through the third parties it relies on. Suppliers, software providers and outsourcing partners often have access to systems, data or day-to-day operations. If one of those third parties is compromised, the impact can quickly flow through to the businesses they serve.

A business's cyber security is only as strong as the weakest link in its supply chain

Why SMEs are exposed

SMEs are not only targeted for cyber attacks because they are vulnerable. They are targeted because they are connected.

Small businesses often act as gateways to larger organisations, providing access to systems, data or trusted relationships. This connectivity also means they can be caught in the fallout of attacks aimed at large technology providers or service vendors.

Due to the size or reputation of these larger suppliers, there is potential for SMEs to have overlooked something in the due diligence of their suppliers' security or just have limited visibility.

For smaller businesses, this disruption up the chain can lead to downtime, lost revenue, reputational damage and contractual consequences. As a result, supply chain cyber risk is now a growing focus for government bodies, including the NCSC.

CFC offer this cover specifically built for SMEs

How cyber insurance addresses supply chain risk

Modern cyber insurance recognises that cyber risk extends beyond a business's own systems and should respond when disruption originates with third parties.

Dependent business interruption
Responds when a supplier or service provider suffers a cyber incident that prevents them from delivering services to the insured, resulting in downtime and loss of income for the insured.

Customer business interruption
Responds when the insured's customer experiences a cyber incident and reduces or stops purchasing goods or services, leading to a direct financial loss for the policyholder. This reflects the reality that cyber events can impact revenue even when the insured has not been directly attacked.

Together, these covers help protect businesses against the financial impact of cyber incidents, no matter where they hit in the supply chain, allowing businesses to grow and partner in confidence.

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.

Theft of funds

How it started

A financial controller at a London law firm received a call from someone claiming to be from the firm's bank, saying suspicious wire transfers had been flagged. The caller insisted funds had been stolen and requested a password and pin code to freeze the account.

What went wrong

The financial controller shared the pin code and password and was told the account had been frozen. The next day, the bank confirmed it had not been in contact and that £100,000 had already been wired out and could not be recalled.

How we supported

As the transaction appeared authorised, the bank refused reimbursement. However, the law firm had cyber insurance with social engineering cover and was reimbursed for the full loss.

Business interruption

How it started

A haulage company in Glasgow suffered a ransomware attack that encrypted all critical data, including routes, logistics, key contacts, stock quantities and payment processing systems. The attackers demanded a ransom of £9,920 for the decryption key.

What went wrong

The business refused to pay and instead rebuilt data using paper records and employee knowledge, resulting in significant overtime costs. More damaging was the loss of income caused by the prolonged system outage and operational disruption.

How we supported

Following the attack, the business lost around 80,000 sales in the next month, equating to nearly £1 million in lost revenue. Thanks to the comprehensive cover within their cyber policy, almost all financial losses were recovered under the policy.

Data breach

How it started

A private healthcare clinic became the victim of a cyber attack in which patient information was stolen from its systems. The attackers threatened to publish the data on a public website unless the clinic paid a ransom of £13,220 in Bitcoin.

What went wrong

The clinic immediately contacted CFC, who deployed our in-house incident response team to assess the situation. An external IT forensics firm was engaged to validate the attacker's claims. Following the investigation, it was confirmed that data relating to approximately 3,000 patients had been compromised, although no sensitive medical records had been accessed.

How we supported

The clinic decided not to pay the ransom. Instead, the CFC engaged a crisis communications consultancy to support patient notification and help protect the clinic's reputation. The clinic's cyber policy covered the costs of forensic investigation and crisis communications, helping the business manage the incident and its wider impact.

Ransomware

How it started

A hacker gained access to a Cambridge school's computer network through a weak remote desktop protocol (RDP) connection. Using a brute force attack, the hacker tested multiple password combinations until they were able to gain unauthorised access to the system.

What went wrong

Once inside the network, the attacker deployed ransomware across the school's systems. Multiple servers and back-up systems were encrypted, leaving the school unable to operate and access critical data. The hacker then demanded a ransom payment of 2 bitcoin in exchange for the decryption key.

How we supported

CFC's incident response team moved quickly to support system restoration and investigate the root cause of the attack. The investigation confirmed that the attacker's primary motive was financial gain rather than the theft of sensitive data. The school's cyber policy responded to cover the costs associated with the ransomware event, including forensic investigation, root cause analysis, security assessments and legal support.

Choosing a **cyber insurance provider**

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

Proactive cyber attack prevention: While it's imperative to have coverage that reimburses losses and access to an expert team to remediate incidents, a good cyber insurer should also be **working to help prevent cyber attacks from happening in the first place.** Look for a provider that uses a range of advanced cyber security tools and methods, including vulnerability scanning, threat hunting, external threat intelligence and proprietary claims data.

In-house cyber security and incident response: What makes a cyber insurance offering comprehensive is being 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. Businesses may want to look for incident response that is led by a technical cyber experts, rather than a non-expert legal team, to ensure the incident can be contained and remediated, before moving into recovery and coverage.

Meaningful claims experience and data to back it up: When businesses are considering insurance providers, you may want to look for one that not only has dedicated and specialised cyber claims adjusters. But also a team that uses their claims data 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 terms 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

When a business puts locks on their doors to reduce the chance of theft or installs sprinkler systems to mitigate the risk of fire, they will usually purchase property damage insurance in case the precautionary measures fail. The same point holds true when it comes to cyber security. **Investing in IT security is a great precautionary measure, but hackers can often bypass security measures** and exploit human error. Cyber insurance is there to act as a valuable safety net if these measures fail to prevent an attack.

Theft of funds, ransomware, extortion and non-malicious **data breaches are often caused by 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 ever-changing and 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 outage caused by a cyber event or 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.

Most cyber insurance policies will extend cover data and systems hosted by third parties, as well as business interruption losses caused by system outages at third-party IT providers.

Debunking cyber **misconceptions**

✕ 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 computer systems to operate, whether for business critical activities or simply electronic banking has 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, while **ransomware can cripple an 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 insurance is too expensive

Cyber attacks can be catastrophic for businesses. The financial impact often goes far beyond a single ransom demand and can include prolonged business interruption, forensic investigation, legal and regulatory costs, remediation, recovery and reputational damage. For many organisations, these combined losses can run into the hundreds of thousands and, in some cases, **are enough to force a business to close.**

While the cost of cyber insurance reflects the rising severity of cyber claims, it also includes access to specialist security and incident response **services that would otherwise be inaccessible by smaller companies or cost thousands to purchase independently.** These services add value to businesses as they work to spot vulnerabilities early, respond faster when an incident occurs and limit damage when every minute matters.

Seen in this light, the cost of a premium is small compared to the financial, operational and reputational losses of a serious cyber event.

cfc Masterclass

Keen to level up your cyber knowledge? Join Cyber Masterclass

Our award-winning video learning series, built to give brokers the knowledge and confidence to sell cyber with ease.

You will:

- Gain 5 hours of CPD accredited learning, for **free** at a pace that suits you
- Over +25 videos learn about a range cyber topics - from cyber economics & coverage to security & landscape
- Gain insights that you can apply to your client conversations
- Become your clients go-to for cyber risk and grow your cyber book

Accredited by the Chartered Institute of Insurance (CII) and Irish Insurance Institute (III)

★★★★★

Marketing Campaign of the Year

Insurance Times Awards 2025

★★★★★

Cyber Awareness Initiative of the Year

Intelligent Insurer's Cyber Awards, Europe 2026

★★★★★

Cyber Awareness Campaign of the Year

Intelligent Insurer's Cyber Awards, USA 2026

Visit cfc.com/cfc-cyber-masterclass

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.

Attack surface
The total number of systems, devices, software and internet facing points that could potentially be targeted or exploited by a threat actor.

Back-ups
Secure and frequently taken copies of data and systems that allow a business to restore operations quickly after a cyber incident.

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

Business email compromise (BEC)
A type of cybercrime where attackers impersonate a trusted contact via email to trick employees into making payments or sharing sensitive information.

Business interruption (cyber)
Loss of income and increased operating costs caused by a cyber event that disrupts a business's ability to operate normally, such as system outages, network failures or ransomware attacks.

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 behavioural 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.

Funds transfer fraud
A cybercrime where criminals trick a business into electronically transferring money to a fraudulent account.

Incident containment
The actions taken to stop a cyber attack from spreading, limit damage and secure systems once a threat or breach has been identified.

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.

Lateral movement
The technique used by attackers to move through a network after gaining initial access, allowing them to reach more systems, sensitive data or backups.

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.

Push payment scam
A type of fraud where criminals manipulate someone into voluntarily sending money to a fraudulent account, often through impersonation of a trusted organisation or contact.

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 cyber security 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 hunting
A proactive cyber security activity where specialists actively search networks, systems and external sources for signs of malicious activity that may not yet have triggered alerts.

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.

British Insurance Brokers' Association

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 across Europe, North America, Australia and Asia, CFC has over 1,000 employees and is trusted by more than 200,000 businesses in 100 countries. Learn more at cfc.com and LinkedIn.

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

About BIBA

The British Insurance Brokers' Association is the UK's leading general insurance intermediary organisation and represents the interest of insurance brokers, intermediaries and their customers.

Member Helpline: 0370 7700 266
Email: enquiries@biba.org.uk
Website: www.biba.org.uk
Twitter & Instagram: @BIBABroker
LinkedIn: BIBA

The information in this document is of a general nature and is not intended to address the circumstances of any particular individual or entity. BIBA or CFC cannot accept any responsibility for any loss occasioned to any person or entity as a result of action or refraining from action as a result of any item herein.

First published in 2019, this guide was last updated in May 2026. It is reviewed annually to ensure the data and commentary remain relevant, although some details may change before the next review.

cfc.com

cfc