Cyber playbook

a **broker guide** to **cyber insurance**

2023

AVIVA

Spotlight on cyber crime

As businesses and industries embrace digitalisation to drive operational efficiencies and meet customer expectations, new opportunities for cyber attacks open up. Consequently, there's a growing need for businesses to ensure they're protected against such threats.

Taking on an ever-evolving threat

Businesses are increasingly aware of the importance of cyber security, with a significant number seeking information and protection. But the threat is evolving, and there remains room for improvement.

All statistics sourced from the Cyber Security Breaches Survey, 2023, DCMS

32%

of businesses experienced a breach or cyber attack in the last 12 months

34%

of those businesses ended up being victims of cyber crime

£15,300

is the approximate average annual cost of cyber crime per victim for UK businesses

49%

of businesses sought outside cyber security guidance or information in the past year

Increasing need for cyber insurance

Click each heading for more information

Growing risk +

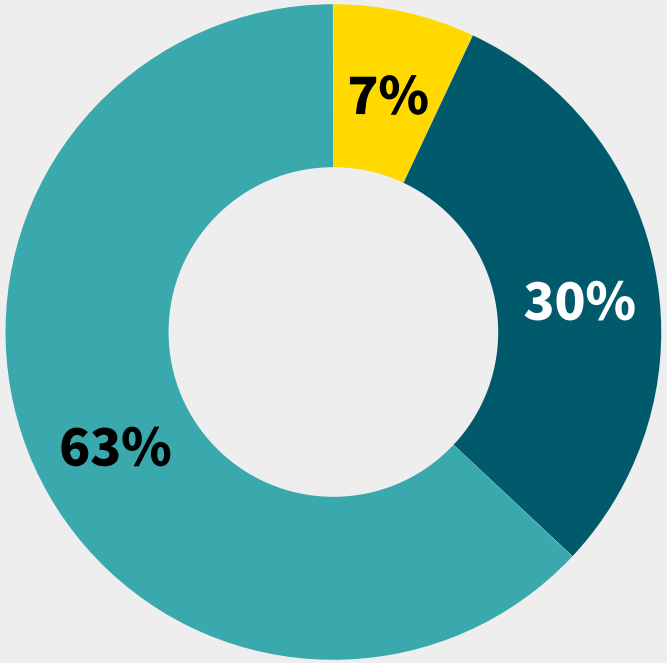
Anyone can be a victim. According to the National Cyber Security Centre (NCSC), "...the majority of the initial accesses to victims are gained opportunistically and are not targeted against a particular organisation."[1]

Obligation +

With the accelerated pace of digitalisation, there's increasing focus on data protection regulations and contractual obligations.

Greater understanding +

Due to high-profile incidents reported in the media, there's an increasing awareness of the operational and reputational damage a cyber attack could cause, leading to a greater focus among business owners.



- 7% have a specific cyber insurance policy in place[2]
- 30% of businesses have cyber security cover as part of a wider insurance policy[2]
- 63% do not have adequate cover in place[2]

[1] Ransomware, extortion and the cybercrime ecosystem whitepaper, 2023, NCSC.gov.uk
[2] Cyber Security Breaches Survey, 2023, DCMS

Increasing need for cyber insurance

Click each heading for more information

Growing risk −

Anyone can be a victim. According to the National Cyber Security Centre (NCSC), "...the majority of the initial accesses to victims are gained opportunistically and are not targeted against a particular organisation."[1]

Obligation +

With the accelerated pace of digitalisation, there's increasing focus on data protection regulations and contractual obligations.

Greater understanding +

Due to high-profile incidents reported in the media, there's an increasing awareness of the operational and reputational damage a cyber attack could cause, leading to a greater focus among business owners.

An evolving threat

Cyber threats are continually evolving, moving from viruses and malware to more sophisticated methods such as ransomware, social engineering/psychological manipulation, and information harvesting and phishing via social media. Shifts to cloud computing, Internet of Things (IoT) devices and AI-powered interfaces are growing areas of potential risk.

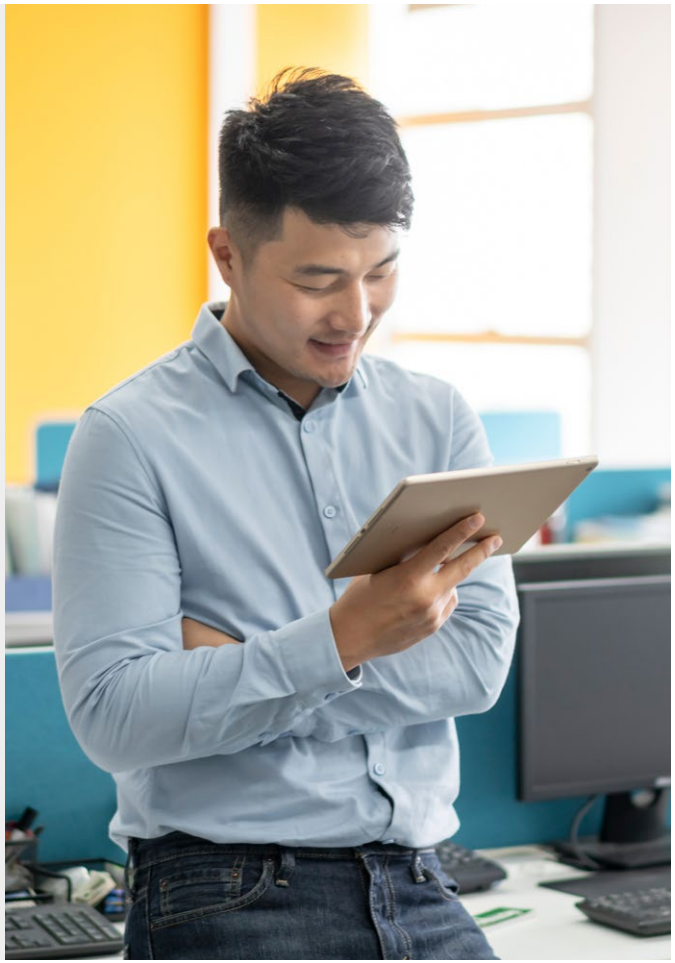
Increased exposure

Businesses of all types hold valuable information, from credit card details to employee data. The risk is no longer limited to the traditional 'data handler' businesses such as healthcare or financial services. Even a micro business with a website is at risk.

Additional exposure can come from supply chains; only 13% of businesses review the risks posed by their immediate suppliers and only 8% review the risks within their wider supply chain.[2]

Severity of breach

Cyber hackers have moved beyond simply capturing data, focusing instead on achieving more sizeable payouts by threatening to publish confidential data if a ransom is not paid.



[1] Ransomware, extortion and the cybercrime ecosystem whitepaper, 2023, NCSC.gov.uk
[2] Cyber Security Breaches Survey, 2023, DCMS

Increasing need for cyber insurance

Click each heading for more information

Growing risk +

Anyone can be a victim. According to the National Cyber Security Centre (NCSC), "...the majority of the initial accesses to victims are gained opportunistically and are not targeted against a particular organisation."[1]

Obligation −

With the accelerated pace of digitalisation, there's increasing focus on data protection regulations and contractual obligations.

Regulatory

Many businesses understand their regulatory obligations when it comes to protecting their customer data, but don't always understand how to ensure they meet these obligations in practice.

Contractual

Businesses are often required by suppliers and customers to uphold data protection standards and minimum levels of cyber security such as the Government-backed 'Cyber Essentials' scheme.[3]

There's also a growing trend of businesses being contractually required to hold cyber insurance.

Greater understanding +

Due to high-profile incidents reported in the media, there's an increasing awareness of the operational and reputational damage a cyber attack could cause, leading to a greater focus among business owners.

[1] Ransomware, extortion and the cybercrime ecosystem whitepaper, 2023, NCSC.gov.uk
[3] www.ncsc.gov.uk/cyberessentials/overview

Increasing need for cyber insurance

Click each heading for more information

Growing risk +

Anyone can be a victim. According to the National Cyber Security Centre (NCSC), "...the majority of the initial accesses to victims are gained opportunistically and are not targeted against a particular organisation."[1]

Obligation +

With the accelerated pace of digitalisation, there's increasing focus on data protection regulations and contractual obligations.

Greater understanding −

Due to high-profile incidents reported in the media, there's an increasing awareness of the operational and reputational damage a cyber attack could cause, leading to a greater focus among business owners.

Awareness

First-hand experience, combined with some well-publicised cyber attacks, are driving businesses to consider the full extent of their cyber exposures. 96% of large businesses and 91% of medium businesses report that cyber security is a high priority for their senior management. Certain sectors see it as more of a priority than others, particularly those in the information and communications, and finance and insurance sectors.[2]

Expertise

Of the 7% of companies that did have a cyber insurance in place, their insurance provider's expertise on breach recovery was cited as a key reason for doing so.[2] Companies are recognising that their own in-house IT capabilities may not be sufficient should an attack or breach take place.

Working patterns

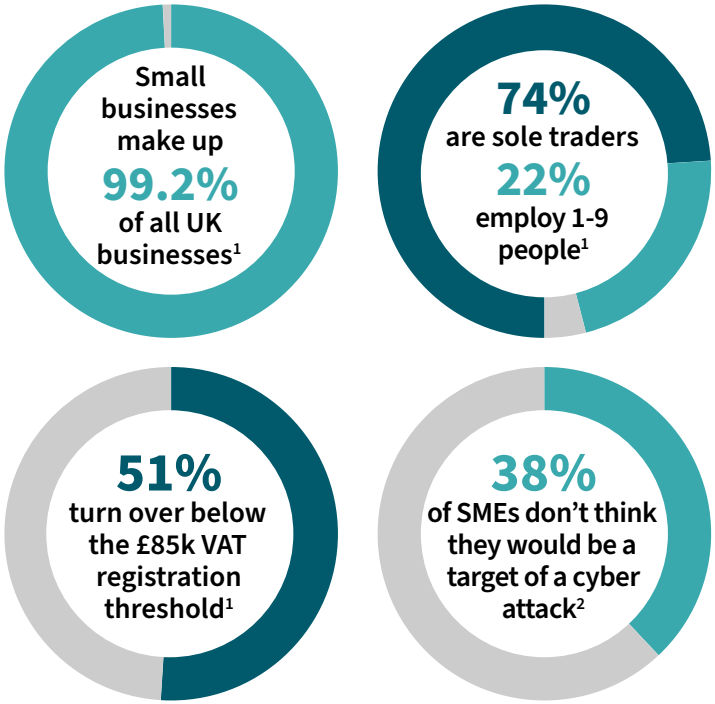
The rise in hybrid working patterns brings with it with greater IT infrastructure challenges and a risk of inadequate cyber and data security, making it easier for cyber criminals to exploit weaknesses in remote arrangements.

[1] Ransomware, extortion and the cybercrime ecosystem whitepaper, 2023, NCSC.gov.uk
[2] Cyber Security Breaches Survey, 2023, DCMS

Supporting small businesses in an evolving landscape

Cyber attacks come in all shapes and sizes – as do cyber crime victims. Many small businesses believe they can fly under the radar of cyber criminals. But, with less sophisticated cyber security measures than bigger organisations, small businesses can be an enticing target for criminals.

Small business is huge



[1]Business population estimates for the UK and regions 2022, BEIS, gov.uk
[2]Aviva SME Yougov survey

Small and micro businesses make up the vast majority of the UK business population, yet many are underprepared to deal with cyber attacks and unaware of what they'd do in the event of a breach.

29% would expect their managed service provider to deal with it[2]

25% would go to the police[2]

17% wouldn't know where to turn for help[2]

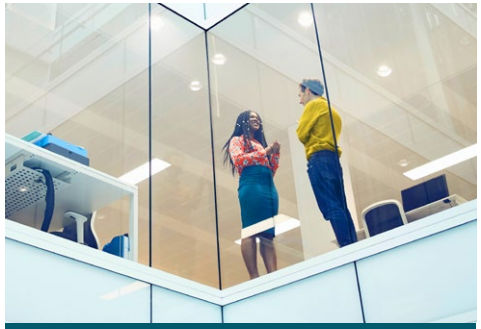
This is where cyber insurance can provide real value. Without continuity plans in place or access to specialist IT support, an attack could have a huge impact on an SME, compromising reputation and livelihoods. By taking the opportunity to work together to educate your SME clients, we can provide them with the right protection in an ever-evolving threat landscape.

Aviva's cyber solutions

We recognise that your clients have different cyber needs depending on the size, scale and sector of their business. As such, we now offer three cyber insurance products tailored to differing business sizes, alongside Cyber Excess of Loss for those who require higher indemnity limits.*

Cyber Respond

Suitable for: small businesses and micro enterprises with fewer than 10 employees and a turnover of less than £1m. Minimum premium of £50** + IPT.



Cyber Complete

Suitable for: larger SMEs and mid-market organisations with a turnover of up to £500m.

Cyber Enhanced

Suitable for: large corporates with an annual turnover of over £500m.

Excess of Loss

Suitable for: corporate businesses and larger SMEs who require higher indemnity limits than their primary insurer can provide to manage their cyber risk exposure.

*Product eligibility may depend on trade. **Subject to individual circumstances and the cover level.

Rapid 24/7 incident response

If your client came into work one morning to find themselves locked out of their system and facing a ransom demand, would they know what to do? A rapid response to an incident or breach is vital. Recovering quickly and effectively requires co-ordinated expert support to reduce the damaging impact of the event.

At the heart of our Cyber offering is a 24/7 incident response service.

Any cyber incident – actual or suspected – can be reported to our dedicated cyber and technology experts on 0800 051 4473.

They are available at any time to provide:

A dedicated incident manager will co-ordinate the incident from the outset, bringing in the right experts when necessary.

Specialist IT forensics and consultants will identify the type of attack, the extent of the damage and if data has been compromised.

Reputational experts can help minimise any negative impact on the brand, customers or suppliers, across press and social media.

No excess for any expert guidance or initial advice, applicable as standard.

Support throughout your client's recovery activities, including access to free counselling services for any staff affected by a cyber event or online incident.

Why a swift response matters

Cyber Respond

Vanessa owns a small online retail chain.

She receives an email from a third party informing her they have access to the company network and demanding a ransom payment of 2 Bitcoin (equivalent to around £50,000) or they will leak customer data.

She immediately contacts Aviva. Our response team act straight away, giving immediate mitigation advice to Vanessa. Within two hours of the notification a call is arranged with Vanessa, her outsourced IT provider and her broker, to understand the issue and ensure the correct specialists are appointed. IT forensic specialists investigate the source of the breach, identifying if data has been compromised and resolving the incident. Meanwhile legal experts review if any regulator notification is required. Within 48 hours remedial action is close to completion.

Cost of loss:

- **c£8,000 in fees to the relevant specialists, including IT forensics**
- **c£2,000 in legal and incident management fees**
- **No excess payable**

Total cost: c£10,000

Cyber Complete

A national firm of solicitors employs 75 staff across six locations.

Odin from the finance team receives an email from a named but unrecognised sender containing an attachment claiming to be an invoice. The attachment turns out to be malicious and, once opened, results in a CryptoLocker attack which encrypts all data on the company network, demanding a ransom for the decryption key.

Odin notifies his Managing Director who calls Aviva immediately. The breach response team co-ordinate relevant experts to assist, including IT forensics to decrypt the data and regain access to the systems.

Fortunately, the attack didn't cause a data breach, but it did leave the firm

unable to access their network or records for two days, significantly impacting their trading and client servicing abilities.

Cost of loss:

- **c£50,000 in fees to the relevant specialists, including IT forensics**
- **c£20,000 in legal and incident management fees**
- **c£30,000 in overtime payments to staff**
- **c£100,000 in loss of revenue**

Total cost: c£200,000

Please note, the scenarios referenced in this document are fictitious examples based on our claims experiences, and the resolutions stated are not definitive but one feasible response to the issue described.

Prevention best practice and cyber risk management

The world is increasingly complex, unpredictable and interconnected. Being able to identify, evaluate and quantify new cyber risks as they emerge is key to keeping ahead of any potential attackers. As part of our cyber insurance proposition we offer free risk management guidance and prevention solutions.

Available through our Aviva Risk Management Solutions website, resources include a library of Loss Prevention Standards on topics such as ransomware and social engineering, as well as access to a variety of trusted Specialist Partners. These partners can support clients with their cyber exposures.

In-house, we have Risk Managers ready to support you and your customers in assessing their cyber resilience and preparing for potential cyber incidents.

Find out more

Our underwriting appetite

We have a broad underwriting appetite across industries, trades and occupations, with capacity to cover businesses across a variety of sizes and sectors.

- UK domiciled business
- Max revenue £500m
- Max 40% revenue from overseas
- Max £5m limit

Core appetite

Retail and wholesale
- Clothing and accessories
- Health and beauty
- DIY and garden
- Haulage

Professional Services
- Accountants
- Law firms
- Insurance brokers
- Employment agencies

Business services
- Marketing
- Graphic design

Charities and not-for-profits

Manufacturing and industry
- Food and drink
- Textiles
- Metals
- Woodworking

Construction
- Carpenters and joiners
- Kitchen installation
- Painters and decorators
- Builders

Technology
- Software development
- Hardware sales
- Outsourced services
- IT consultancy

Education
- Nurseries
- Schools (with fewer than 100 pupils)

Arts and culture
- Galleries
- Museums
- Theatres

Leisure
- Restaurants
- Hotels
- Cafes

Agriculture
- Farming
- Horticulture
- Forestry

Motor industry
- Service and repair
- Vehicle sales

Selected healthcare and social care
- Physiotherapists
- Optometrists
- Alternative healthcare practitioners
- Counsellors
- Veterinary surgeons
- Child-minding services

Property owners

Out of appetite

- **e-commerce risks** 100% online retailers, gaming, gambling and social media including dating
- **Financial institutions and financial services** Banks, building societies, stockbroking and other currency and securities trading
- **Utility & telecommunications companies**
- **Media** Market Research & Advertising Agencies, Animation Production, Film/TV Studios, Journalists, TV/Radio Broadcasting
- **Selected healthcare and social care** Social Services, Children's Homes, Nursing Homes, Hospitals, Dentists and Doctors
- **Selected technology trades** Artificial Intelligence, Domain Name Registrars, Games Publishers, SCADA, Payment Processors

Our cyber cover at a glance

Cover	Cyber Respond	Cyber Complete
Breach response		
24/7/365 Incident response	✓	✓
Cover for costs of an incident manager	✓	✓
Cover for costs of specialist IT forensics	✓	✓
Cover for costs of specialists to resolve the event	✓	✓
Legal support	✓	✓
Support with any regulatory reporting required	✓	✓
Notification costs following a data security breach	✓	✓
Reputation management	✓	✓
Resilience improvements	✘	✓
Criminal reward fund	✘	✓
First-party: business loss		
IT systems and data	✓	✓
Cyber terrorism	✓	✓
Increased cost of working	✓	✓
Business interruption	✘	✓
Outsourced service providers interruption	✘	✓
System failure	✘	✓
Optional customer and supplier extensions for certain risks	✘	✓
Cyber extortion ransom payment	✘	✓
Manufacturing and other industrial processes	✘	✓
Regulatory fines and penalties (where insurable by law)	✘	✓

Cover	Cyber Respond	Cyber Complete
External cyber crime (optional)		
Unauthorised use of computer equipment	✓	✓
Social engineering fraud	✓	✓
Funds transfer fraud	✓	✓
Telecommunications fraud	✘	✓
Corporate identity fraud	✘	✓
Theft of personal money	✓	✓
Virtual currency	✓	✓
Third-party: liabilities		
Network security	✘	✓
Data privacy	✘	✓
Multimedia	✘	✓
Media removal costs	✘	✓
Payment card industry	✘	✓
Additional benefits		
Minimum excess	**£0**	**£1,000**
Excess not applicable if advice provided by incident response is able to resolve the issue	✓	✓
Cover applies to both electronic and physical data	✓	✓
Legal helpline and support available at no additional cost	✓	✓
Counselling service for employees affected by a cyber event	✓	✓
Free cyber and data risk management materials and resources	✓	✓
Access to cyber specialist partners at preferential rates	✓	✓
Free 2-hour cyber risk management consultancy session with an Aviva Risk Management Consultant (for policyholders paying £5,000 premium)	✘	✓

Understanding our covers

- Incident response +
- First-party: business loss +
- Third-party: liabilities +
- External cyber crime +
- Cover limits +
- Minimum premiums +

Understanding our covers

- Incident response −
- First-party: business loss +
- Third-party: liabilities +
- External cyber crime +
- Cover limits +
- Minimum premiums +

Incident response

Experts

- Cover for the costs of an incident manager, specialist IT forensics and legal support to guide you through a cyber event.
- Experts will identify the type of attack and the extent of the damage, and if data has been compromised, they will resolve the attack and support with any regulatory reporting required.

Notification costs

- Cover for the costs to notify and provide credit or identity fraud monitoring services to individuals affected by a data security breach.
- Also includes the costs of reporting events to the regulator.

Reputation management

Cover for the costs of public relations consultants to minimise adverse publicity following a cyber event.

Resilient improvements

Cover for the additional costs to improve the resilience of your computer system following a loss, to prevent a similar incident in the future. 15% of corresponding claim up to £25k.*

Criminal reward

Cover for a reward, paid by you, which leads to a conviction or the recovery of a financial loss following a covered cyber event.

*Limits can be increased subject to additional information and premium

Understanding our covers

- Incident response +
- First-party: business loss –
- Third-party: liabilities +
- External cyber crime +
- Cover limits +
- Minimum premiums +

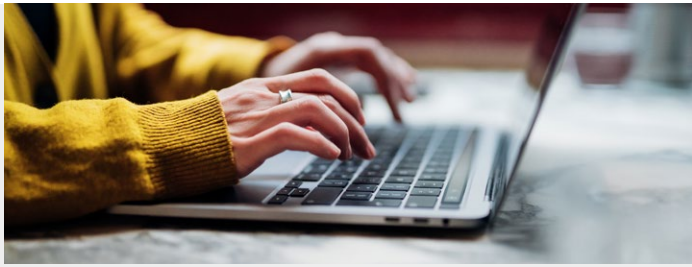
First-party: business loss

IT systems and data
Reinstate, recreate or restore data, software or websites and repair or replace damaged computer equipment following a virus, hack or denial-of-service attack.

Cyber extortion
We cover the costs for expert negotiators to resolve a cyber extortion incident and ransom payments (where insurable by law).

Business interruption
Cover for loss of revenue and additional increased cost of working, including loss of future customers due to reputational damage, following a cyber event.

Outsourced service providers
Business interruption cover extends to include interruption to your contracted providers of information technology, data hosting or data processing services as standard.



System failure
Cover for loss of income and additional expenses as a result of an unintentional and unplanned malfunction or outage of your computer equipment – up to £25k as standard.*

Manufacturing and other industrial processes
Cover extended to include cyber events which affect industrial control systems – up to £25k limit.*

Optional customers and suppliers extensions
For larger risks we can provide cover for loss of revenue and increased costs of working caused by a cyber event affecting the computer equipment of your client's suppliers or customers.

*Limits can be increased subject to additional information and premium

Understanding our covers

- Incident response +
- First-party: business loss +
- Third-party: liabilities –
- External cyber crime +
- Cover limits +
- Minimum premiums +

Third-party: liabilities

Data privacy and confidentiality

Cover for claims made against you due to:

- breach of confidence or misuse of an individual's private information or personal data
- breach of data protection legislation
- loss or disclosure of confidential third-party commercial information.

Regulatory fines and penalties

Cover for lawfully insurable regulatory fines and penalties, including legal costs, following a breach of data protection regulations.

Network security

Cover for claims made against you due to your:

- negligent transmission of a virus
- failure to prevent unauthorised access that results in a denial-of-service attack.

Multimedia

Cover for claims made against you due to copyright infringement, defamation, libel, slander and costs to remove online media to minimise a loss.

- Media removal costs – cover for costs to remove online content which avoids a multimedia liability claim being made against you.

Payment card industry

Cover for the fines, penalties and reassessment costs resulting from non-compliance with Payment Card Industry Data Security Standards due to a breach of personal data.

Understanding our covers

- Incident response +
- First-party: business loss +
- Third-party: liabilities +
- External cyber crime –
- Cover limits +
- Minimum premiums +

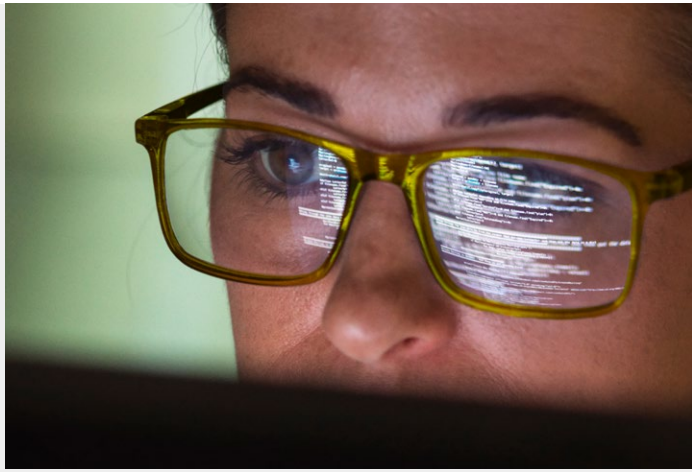
External cyber crime

Unauthorised use of computer equipment
Cover for financial loss resulting from the unauthorised use of your computer equipment by a third party.

Social engineering fraud
Cover for financial loss resulting from a third party inducing or deceiving your employee by impersonating or claiming to be another person or organisation entitled to the funds.

Funds transfer fraud
Cover for financial loss resulting from a fraudulent instruction sent to your bank.

Telecommunications fraud
Cover for charges payable to your telecommunications supplier due to the unauthorised use of your telephone systems.



Corporate identity fraud
Cover for the costs and expenses incurred to reinstate public records following fraudulent modification, alteration or theft of your corporate identity.

Theft of personal money
Cover for the loss of personal money due to unauthorised access to the business network.

Understanding our covers

- Incident response +
- First-party: business loss +
- Third-party: liabilities +
- External cyber crime +
- Cover limits –
- Minimum premiums +

Cover limits

Cyber Respond

- Capacity to underwrite risks up to £1m annual turnover
- Standard indemnity limits range from £25k to £100k (with up to an additional £10k if Cyber Crime is selected as an optional cover)

Cyber Complete

- Capacity to underwrite risks up to £500m annual turnover (up to £50m on digital platforms).
- Standard indemnity limits range from £25k to £2m with independent limits applying to first- and third-party cover
- Increased limits of indemnity up to £10m

Cyber Enhanced

- Cover and limits agreed on a case-by-case basis

Cyber Excess of Loss

- SME – minimum attachment point £2m, with limits up to £5m available
- Lead or follow coinsurance options available
- Corporate – minimum attachment point £20m, with limits up to £10m available
- Maximum net line £2.5m in the aggregate

Understanding our covers

- Incident response +
- First-party: business loss +
- Third-party: liabilities +
- External cyber crime +
- Cover limits +
- Minimum premiums –

Minimum premiums

Cyber Respond

£50* + IPT (excluding External Cyber Crime cover)

Cyber Complete

£200 + IPT

*Subject to individual circumstances and the cover level.

Your client's responsibilities

In order for your client's cyber insurance policy to provide full protection, it's important that they comply with the following minimum actions:

Passwords

Any default or manufacturers' passwords or access codes must be changed and kept secure.

Data storage

Personal, sensitive, protected or confidential data must be stored and disposed of in a secure manner.

Data backup

Data must be backed up at least every seven days. Backups must be stored securely and separately from the original. The backup routine must be checked to ensure it's working.

Firewall

Equipment connected to the internet or an external network must be protected against unauthorised access by a suitable and active firewall.

Payment instruction policies

A documented policy must be in place, stating that any new payee requests or amended payment instructions are checked verbally using details held on file or a published website and actions are not taken solely based on the new instruction. This policy must be accepted by all partners, directors and employees, with such acceptance recorded.

Social engineering fraud

The business's owner/partners/directors and employees must be trained in the dangers and identification of social engineering fraud. A record should be kept of such training.

Software updates

Updates must be carried out within 14 days of update release, where the issue is described as 'critical', 'high risk' or addresses a vulnerability with a CVSS v3 score of 7 or above.

Viruses

Computers and personal devices used for accessing IT systems must have effective anti-virus software.

Incident reporting

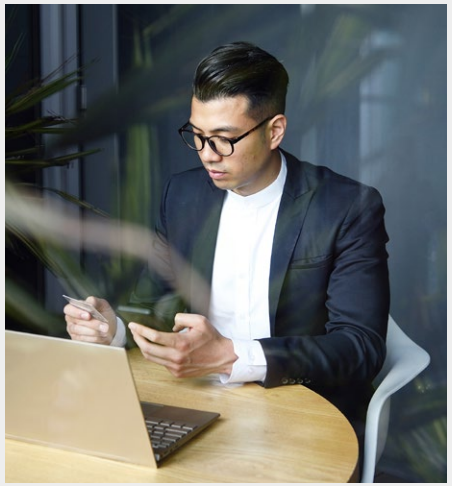
On receiving a cyber extortion demand clients must immediately notify us and comply with any requirements, as well as reporting the crime to Action Fraud.

Cyber claims scenarios

Phishing

Fraser, a small business owner, receives an email from one of his suppliers requesting a BACS payment of £5,000. He emails the supplier to verify bank details and receives a reply confirming all is in order to proceed. He makes the payment. Four days later, Fraser receives another email from the same supplier querying where the now overdue payment is.

Fraser notifies Aviva and our investigators work with the company's IT team. They identify a suspicious spam email which has led to Fraser's email account being compromised. The investigators discover the rules for the account have been set up to forward emails to an unknown external account. This means the original supplier email has been intercepted and incorrect bank details provided to Fraser.



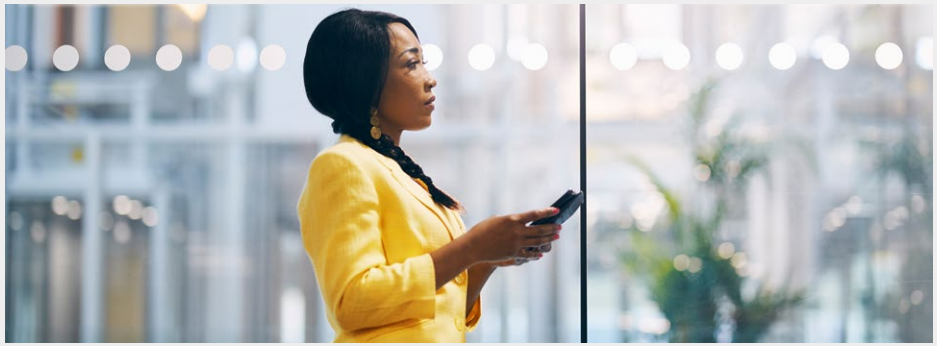
He notifies the relevant authorities and the business's bank, but unfortunately the money cannot be traced.

Cost of loss:

- **c£1,000 in IT forensics fees**
- **£5,000 covers the amount lost**

Total cost of loss: c.£6,000.

Negligent employee



Sam works in HR at an estate agency and inadvertently sends an email to a colleague in another branch which includes personal information of a large number of staff members, including payroll data and home addresses.

Once the data breach is identified, Aviva investigates the incident and works with the company to notify the ICO within the 72-hour timeframe. Around 200 of the employees pursue the matter and sue the company for material distress as a result of the data leak.

The employees are awarded £1,000 each for emotional distress and significant third-party legal costs are incurred.

Cost of loss:

- **£1,000 x 200 employees = £200,000 in compensation**
- **c£27,000 in legal fees**

Total cost of loss is c£227,000.

Considerations when placing cyber cover

Aggregate basis

The majority of cyber policies in the market are written on an aggregate basis. This means the cover limit selected is the maximum amount the insurance will pay in a policy period. If this limit is exhausted through one or many claims, coverage under the policy will cease.

It's therefore very important to help your customer select a limit which provides sufficient cover for a worst-case-scenario loss.

Claims made – basis of settlement

Cyber liability policies are generally written on a 'claims made' basis, meaning they only cover claims first made against the insured, or incidents first discovered by the insured, and notified to the insurer during the period of insurance.

Excess

Most cyber policies have a:

- monetary excess – payable as part of a claim
- time excess/waiting period – as part of the business interruption (BI) cover. This is the defined period an interruption to the business must exceed before a BI claim is payable.

It's also worth checking when an excess will be payable. Is it payable as soon as contact is made with the incident response line, or once specialist support is instructed? Aviva will not request an excess payment if the customer's issue is resolved via advice given by our incident response team.

Considerations when placing cyber cover

Business interruption

Not all cyber business interruption covers are issued on the same basis, so it's important to be able to identify these differences and how they may impact your customer in the event of a claim:

Does the policy have a time excess? How long is this, and is it suitable for your customer profile?

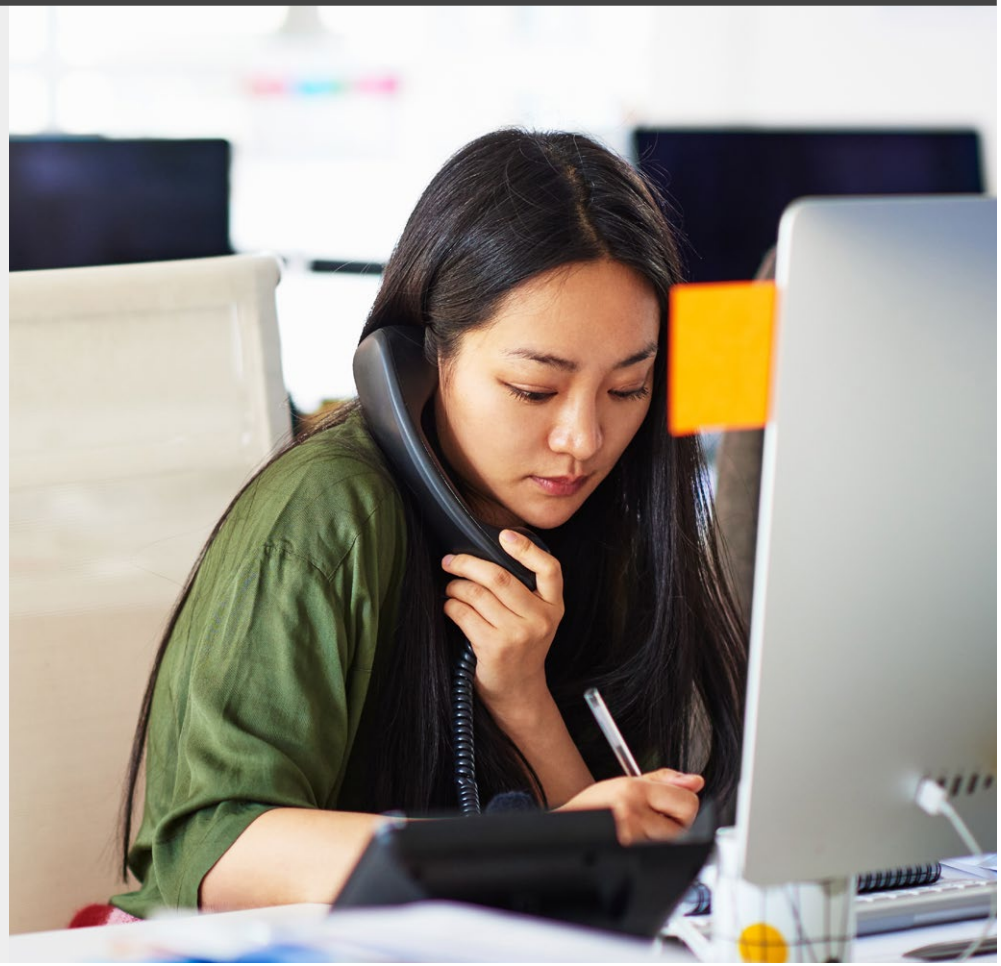
Does the policy have an indemnity period or a restoration period?

An indemnity period means the policy will continue to respond until the business income reaches pre-incident levels or the indemnity period runs out.

A restoration period means cover for a reduction in the business income will only be paid until the cyber incident has been resolved or for a defined period after the resolution. Many policies may have a period as short as three months – would this be sufficient to allow your customer's business to fully recover?

Does the policy include outsourced service provider cover?

If your insured uses cloud services or other third-party data processing services, would their business be impacted if a cyber event interrupted these services? This cover is included within some policies available in the market, but not all.



Enjoy the Aviva difference

We're committed to helping you and your clients trade, adapt and evolve in an increasingly complex cyber landscape by offering:

Flexible trading options

Available across e-trade, Fast Trade and our regional branch network; purchased stand-alone or as part of a package.

Dedicated cyber expertise

Available locally through our specialist underwriters across our regional branch network or on-demand via live chat for online quotes and renewals.

A simple data-led processes

Instant quotes and limited (or no) question sets for existing policyholders. No proposal forms for risks with annual turnovers up to £50m.

Cyber training for you and your team

Access to learning modules, including our brand-new cyber qualification for brokers, so you can speak to your clients with confidence about cyber risks and solutions.

Visit The Aviva Development Zone

All underpinned by the scale and stability of the Aviva brand.

[1]Aviva Annual Report 2022, published March 2023
[2]Source: S&P Insurer Financial Strength Rating for Aviva Insurance Limited

£23.2 billion in claims paid[1]

18.7 million customers across our core markets[1]

S&P AA-rated Stable financial strength[2]

If you have any questions about any of our cyber insurance solutions, please speak to your usual underwriter or sales contact. Alternately, you can visit our **Aviva Broker website**.

Return to start

BMGI1066102023. 09/2023.

AVIVA