

Cyber Playbook

A broker guide to
cyber insurance

Spotlight on cyber crime

As businesses and industries continue to shift towards digitalisation to drive efficiencies in operational processes, cyber threats are increasingly becoming a key risk. Consequently, there's a growing need for businesses to ensure they're protected against such threats.

Increasing awareness of a growing threat

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

¹Cyber Security Breaches Survey 2020, DCMS

Footnote 1: This source contains public sector information licensed under the Open Government Licence v3.0.

²Action Fraud statistics, December 2020

³Coronavirus-related fraud reports up 400% in March, Action Fraud press release, 2020

⁴Phishing dominates UK cyber threat landscape, shows analysis of latest ICO figures, CybSafe press release, 2020

46%

of businesses experienced a cyber breach or attack in the last 12 months¹

£21.8m

the losses from cyber crime reported to Action Fraud in 2020²

400%

increase in cyber-related fraud in March 2020³

90%

of cyber breaches can be attributed to human error⁴

Increasing need for cyber insurance



Demand for cyber insurance is increasing due to growing exposures, regulatory and contractual obligations and a heightened understanding of the risks.¹

 **Hover over each subtitle for more information**

¹Aon Inpoint research, July 2020

²Cyber Security Breaches Survey, 2020, DCMS
Refer to footnote 1

³Cyber Threat Report Q1, Beaming 2020

⁴About Cyber Essentials, NCSC
Refer to footnote 1

Building resilience through cyber insurance

Research shows that 98% of businesses rely on some form of digital communication or service, for example cloud storage, email, online banking or an online presence.¹

These shifts to digitalisation can all offer avenues for cyber criminals to exploit. Criminals often rely on tools to search the internet for system vulnerabilities, meaning any business, small or large, can be targeted.

Cyber insurance as a service

You'd know what to do if you discovered you'd been a victim of burglary, but would you know how to act if your network was down due to a ransomware attack? A rapid response to a breach is essential and recovering quickly requires co-ordinated expert support. Despite this, our research highlights that less than a third of businesses undertake regular business impact or continuity testing.²

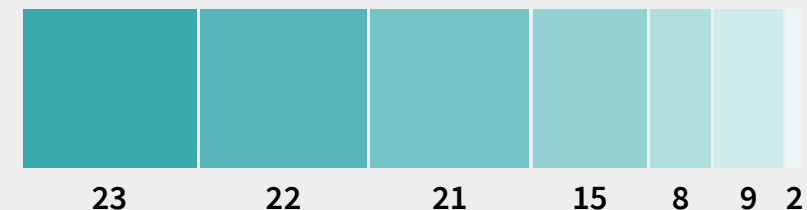
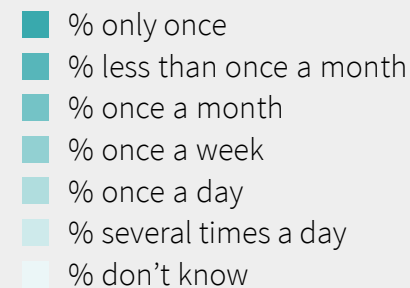
And while cyber risk is a top five priority for UK businesses, only three in ten have cyber cover in place.³ This gives us the opportunity to work in partnership to provide your clients with simple, affordable protection in an ever-evolving threat landscape.

¹Cyber Breaches Security Survey 2019, DCMS
Refer to Footnote 1.

²Aviva commissioned YouGov research, 2020

³Cyber Breaches Security Survey 2020, DCMS
Refer to Footnote 1.

How often organisations have experienced breaches or attacks in the last 12 months.³



Industry-specific threats

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale	—
Manufacturing & Industry	+
Professional services	+
Business services	+
Construction	+
Property owners	+
Technology	+
Motor industry	+
Education	+
Health & Public Sector	+
Charities & Not for Profit	+
Arts & Culture	+



Retail & Wholesale

A prime target for criminals due to an increasing reliance on online purchases and the large quantities of customer data stored. Prioritising user-friendly web shopping experiences over robust security risk (e.g. multi factor secure payments) increases risk of losing confidential customer information. Criminals can use stolen details to hack into customer accounts and use stolen bank details to order goods.

Impacts of a cyber event

⚠ Payment Card Industry Data Security Standards non-compliance

⚠ Inability to take card payments

⚠ Reputational damage

⚠ Customer switching

Industry-specific threats

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale	+
Manufacturing & Industry	—
Professional services	+
Business services	+
Construction	+
Property owners	+
Technology	+
Motor industry	+
Education	+
Health & Public Sector	+
Charities & Not for Profit	+
Arts & Culture	+



Manufacturing & Industry

The manufacturing sector relies on continually evolving technology, making cyber threats an ever-present vulnerability. Valuable intellectual property can be stolen, and processes can be severely disrupted if the software running an operating system is attacked.

Impacts of a cyber event

- ⚠ Halted production resulting in contractual penalties
- ⚠ Disruption to production resulting in loss of revenue
- ⚠ Loss of intellectual property
- ⚠ Reputational damage

Industry-specific threats

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale	+
Manufacturing & Industry	+
Professional services	-
Business services	+
Construction	+
Property owners	+
Technology	+
Motor industry	+
Education	+
Health & Public Sector	+
Charities & Not for Profit	+
Arts & Culture	+



Professional services

Professional services are particularly vulnerable to cyber attack as they handle sensitive and confidential data, have fiduciary and regulatory requirements to keep client data secure, and handle money on behalf of clients.

A growing trend has been to target law firms' residential and commercial property teams, where criminals use social engineering or business email compromise to steal funds.

Impacts of a cyber event

⚠ Data breach

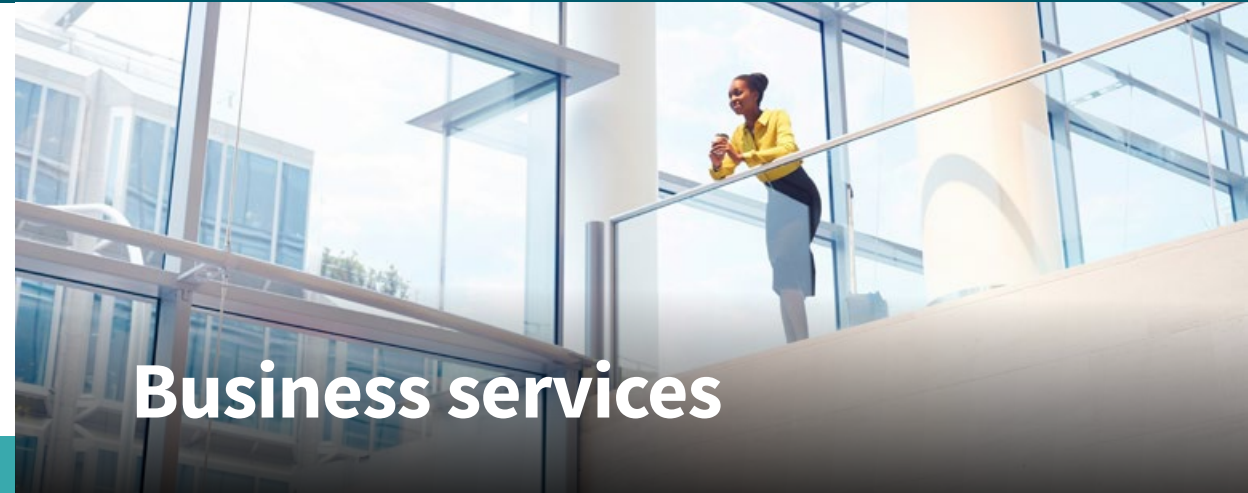
⚠ Loss of customer funds

⚠ Loss of customer trust

Industry-specific threats

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale	+
Manufacturing & Industry	+
Professional services	+
Business services	-
Construction	+
Property owners	+
Technology	+
Motor industry	+
Education	+
Health & Public Sector	+
Charities & Not for Profit	+
Arts & Culture	+



Business services

Business services rely increasingly on technology to deliver their services. This could be storing and processing customer data or providing outsourced services critical to their clients. Having remote access to their clients' systems makes them vulnerable as hackers look for the weakest link to attack a system.

Furthermore, because business services tend to deal with multiple clients, one attack can go on to impact many businesses.

Impacts of a cyber event

- ⚠ Loss of confidential commercial information leading to contractual penalties
- ⚠ Loss of contracts due to perceived low standards

- ⚠ Interruption to the business impacts other businesses to whom services are provided
- ⚠ Service providers can be a route for cyber criminals to access third party systems making them more of a target

Industry-specific threats

◀ 05 ▶

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.



Construction

Construction firms hold vast amounts of information of interest to cyber criminals. Although they rarely hold sensitive credit card information, they're responsible for confidential files containing employee data, tenders, property proposals, plans, drawings and client data. If accessed and exploited, the firms could suffer great financial loss.

Impacts of a cyber event

- ⚠ Social engineering or funds transfer fraud due to frequent movement of significant funds along supply chain
- ⚠ Contractual penalties due to delays in work
- ⚠ Reputational damage leading to loss of contracts
- ⚠ Breach of bid data could mean a loss of competitive advantage
- ⚠ Software with multiple users, i.e. architect, contractors and planners, means more access points and opportunities for exposure

Retail & Wholesale	+
Manufacturing & Industry	+
Professional services	+
Business services	+
Construction	-
Property owners	+
Technology	+
Motor industry	+
Education	+
Health & Public Sector	+
Charities & Not for Profit	+
Arts & Culture	+

Industry-specific threats

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale	+
Manufacturing & Industry	+
Professional services	+
Business services	+
Construction	+
Property owners	-
Technology	+
Motor industry	+
Education	+
Health & Public Sector	+
Charities & Not for Profit	+
Arts & Culture	+



Property owners are a prime target for cyber criminals due to the volume of personal information, signed contracts and digital payments exchanged online between an agent, landlord and tenant. Once accessed, criminals can carry out identity theft and use personal information to forge documents such as passports and driving licences – potentially resulting in legal action against the agent. There's an additional risk of property/mortgage fraud where criminals obtain fake identify documents and proceed to sell or remortgage a property, escaping with the money. Financial fraud is particularly rife due to the large sums of money transferred online.

Impacts of a cyber event

⚠ Social engineering fraud due to frequent movement of significant funds

⚠ Reputational damage

⚠ Data breaches could lead to regulator involvement

Industry-specific threats

◀ 05 ▶

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale	+
Manufacturing & Industry	+
Professional services	+
Business services	+
Construction	+
Property owners	+
Technology	-
Motor industry	+
Education	+
Health & Public Sector	+
Charities & Not for Profit	+
Arts & Culture	+



The technology sector covers a wide range of industries, manufacturers of computers, software houses and telecommunication. All of them use technology and are therefore vulnerable to cyber risks, for example hacking of connected devices and ransomware, which can cause large losses.

Impacts of a cyber event

- ⚠ Customer data breaches could lead to regulatory involvement
- ⚠ Halted production resulting in contractual penalties
- ⚠ Loss of intellectual property
- ⚠ Reputational damage

Industry-specific threats

◀ 05 ▶

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale +

Manufacturing & Industry +

Professional services +

Business services +

Construction +

Property owners +

Technology +

Motor industry -

Education +

Health & Public Sector +

Charities & Not for Profit +

Arts & Culture +



Motor industry

Motor traders hold a great deal of personal data about their customers, such as phone number, home and email address and car registration. If finance is provided as part of a sale, they'll hold even more sensitive data. This data is valuable to cyber criminals, who make money selling stolen information, blocking access to computer files until a ransom is paid, or using scams to steal funds from bank accounts.

Impacts of a cyber event

⚠ **Data breach could lead to regulator involvement**

⚠ **Social engineering fraud resulting in significant financial loss**

Industry-specific threats

◀ 05 ▶

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.



Education

From recording and reporting detailed performance data to staff sharing content and collaborating with students, schools and universities are increasingly reliant on computers and connectivity – and are at risk due to the sensitive data they hold on students and staff. Threats are both internal and external – for example, there's the risk of students connecting their own mobile phones or laptops to the network, which could introduce malware inadvertently, or a staff member not following protocol leading to a data breach.

Impacts of a cyber event

- ⚠ **Data breach and class actions due to high numbers of students and records**
- ⚠ **Social engineering, e.g. targeting school fees**

- ⚠ **Timing of events can have a huge impact, i.e. delay in exam results**
- ⚠ **Bad publicity impacting future enrolment**

Retail & Wholesale	+
Manufacturing & Industry	+
Professional services	+
Business services	+
Construction	+
Property owners	+
Technology	+
Motor industry	+
Education	–
Health & Public Sector	+
Charities & Not for Profit	+
Arts & Culture	+

Industry-specific threats

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale	+
Manufacturing & Industry	+
Professional services	+
Business services	+
Construction	+
Property owners	+
Technology	+
Motor industry	+
Education	+
Health & Public Sector	–
Charities & Not for Profit	+
Arts & Culture	+



Health & Public Sector

The health and public sector are two of the most exposed sectors to cyber risk. They are susceptible to supply chain risks, they store and process valuable and sensitive data, and they have open systems that are easily attacked.

A supplier who may have lower cyber security but full access to the healthcare provider's system is an access point for hackers to obtain lucrative confidential patient data. In this instance, the healthcare provider has to rectify the breach, but is also open to fines and penalties under data protection legislation.

Impacts of a cyber event

- ⚠ **Liability losses due to sensitive patient data held – accidental release can be as damaging to the patients as a malicious release**
- ⚠ **Healthcare data can be more valuable on the dark web than other personal information, making it a key target**
- ⚠ **Regulatory focus, again due to nature of data**
- ⚠ **Potential human impact if files cannot be accessed when needed, i.e. in a hospital setting**

Industry-specific threats

◀ 05 ▶

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale	+
Manufacturing & Industry	+
Professional services	+
Business services	+
Construction	+
Property owners	+
Technology	+
Motor industry	+
Education	+
Health & Public Sector	+
Charities & Not for Profit	-
Arts & Culture	+



The charities and not for profit sector is wide-ranging, covering faith-based organisations, social services, health provision and retail. But they all rely on volunteers, and often lack the centralised IT infrastructure and support you'd see in the commercial sector.

Charities can be vulnerable due to the data they store about beneficiaries, those they support, and the volunteers and staff running the charity.

Charities compete for funds, meaning a cyber attack could discourage donors, which could have a huge impact on a small charity.

Impacts of a cyber event

⚠ **Loss of desperately needed charity funds due to cybercrime**

⚠ **Social engineering using data harvested from a hack**

Industry-specific threats

Any business that gathers or stores data, or is reliant on computer systems (a growing trend across all industries), has an increased vulnerability to cyber risk exposures.

Retail & Wholesale	+
Manufacturing & Industry	+
Professional services	+
Business services	+
Construction	+
Property owners	+
Technology	+
Motor industry	+
Education	+
Health & Public Sector	+
Charities & Not for Profit	+
Arts & Culture	—



Arts & Culture

The struggle for companies in this industry is the need to be at the cutting edge of new technology –from recommendation and review functionality to booking apps, live chat and loyalty schemes – while ensuring customer data is stored and managed appropriately.

Impacts of a cyber event

- ⚠ **Business interruption and higher liability losses as a result of reduced donations from high net worth beneficiaries**
- ⚠ **Media liability exposures such as libel, slander and copyright infringement**
- ⚠ **Loss of credit card data and compliance with PCI Data Security Standards**
- ⚠ **Turnover impacted by an inability to take bookings**

Cyber claims scenarios

Cyber threats can take many forms, and can have a devastating effect on a business. The following scenarios show some typical examples of different types of cyber attack, how our input can help reduce the damaging impact of events, and plausible claims outcomes where applicable.

Disclaimer

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

The scenarios used represent general information and guidance only and should not be construed as giving advice or recommendation. You should obtain specific advice relevant to your circumstances.

Disclaimer	—
Phishing	+
Ransomware	+
Unauthorised access	+
Social engineering fraud	+
Negligent employee	+
Malicious employee	+

Cyber claims scenarios

Cyber threats can take many forms, and can have a devastating effect on a business. The following scenarios show some typical examples of different types of cyber attack, how our input helped reduce the damaging impact of events, and eventual claims outcomes where applicable.

Disclaimer	+
Phishing	-
Ransomware	+
Unauthorised access	+
Social engineering fraud	+
Negligent employee	+
Malicious employee	+

Phishing

Fraser is a small business owner and receives an email from one of his suppliers requesting a BACS payment of £5,000. Fraser emails the supplier to verify the bank details are correct and receives a reply confirming all is in order to proceed with the payment. He makes the payment.

Four days later, Fraser then receives another email from the same supplier querying where the payment is as it is now overdue.

Fraser notifies Aviva and our investigators work with the company's IT team. They are able to 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.

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

Total cost of loss is £4,000.

Cyber claims scenarios

Cyber threats can take many forms, and can have a devastating effect on a business. The following scenarios show some typical examples of different types of cyber attack, how our input helped reduce the damaging impact of events, and eventual claims outcomes where applicable.

Disclaimer	+
Phishing	+
Ransomware	-
Unauthorised access	+
Social engineering fraud	+
Negligent employee	+
Malicious employee	+

Ransomware

With ransomware attacks, time is of the essence, as these two examples demonstrate.

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

She immediately contacts Aviva. Upon receiving the call, our response team act straight away, appointing IT forensic specialists, reviewing policy coverage, and offering mitigation advice. Within 48 hours solutions are in progress.

Total cost of loss is less than £10,000.

Contrast this with another case where the computer systems of a manufacturer are compromised. The attack halts production and there is a ransom demand for £30,000 issued to release the decryption key.

The company's IT team work for five days to manage the attack before notifying Aviva. Once we are notified we begin supporting the IT team and investigating the incident.

Due to the delay in notifying Aviva the total cost of loss is over £80,000.

Cyber claims scenarios

Cyber threats can take many forms, and can have a devastating effect on a business. The following scenarios show some typical examples of different types of cyber attack, how our input helped reduce the damaging impact of events, and eventual claims outcomes where applicable.

Disclaimer	+
Phishing	+
Ransomware	+
Unauthorised access	—
Social engineering fraud	+
Negligent employee	+
Malicious employee	+

Unauthorised access

Odin is a senior manager at a professional services company. His business email credentials are compromised and a malicious third party now has access to his log-in details.

They send an email to the accounts team from Odin's email account requesting a fund transfer of £12,000 to be made. The payment is processed before an alert is raised.

Aviva is notified and we begin investigating. We are able to trace the unauthorised access to an unknown IP address and put preventative measures in place to ensure a similar event doesn't reoccur.

As the hacker had access to Odin's emails there was a chance personal data had been breached. The Aviva team were able to confirm no data was harvested. However, the hacker would have been able to see the contents of the email therefore the ICO was notified of the incident.

As the relevant authorities are notified within the set deadline, no fine is incurred.

Total cost of loss is over £25,000.

Cyber claims scenarios

Cyber threats can take many forms, and can have a devastating effect on a business. The following scenarios show some typical examples of different types of cyber attack, how our input helped reduce the damaging impact of events, and eventual claims outcomes where applicable.

Disclaimer	+
Phishing	+
Ransomware	+
Unauthorised access	+
Social engineering fraud	—
Negligent employee	+
Malicious employee	+

Social engineering fraud

Jareth works in the administration team at a construction company. He receives an email from a self-employed sub-contractor they use on a regular basis requesting an invoice of £20,000 to be paid urgently. While the email appears legitimate, Jareth notices the sub-contractor's bank account details have changed. Jareth verbally checks with his team if anyone knows whether the sub-contractor has changed their bank details, and a colleague confirms there has been talk of them being amended. Jareth transfers £20,000 to the new account.

A week later the sub-contractor phones the accounts team to find out when the invoice will be paid. The accounts team contacts their bank and notifies Aviva of the potential fraudulent activity.

Our investigators quickly discover that cyber criminals have spoofed the sub-contractor's email address and altered the bank account details in the invoice. As internet banking has made money transfers almost immediate and criminals have sophisticated ways of moving money to avoid detection, the company's bank are unable to recover the money.

Fortunately, the event is an isolated incident and the company networks remain unaffected.

Total cost of loss is over £22,000.

Cyber claims scenarios

Cyber threats can take many forms, and can have a devastating effect on a business. The following scenarios show some typical examples of different types of cyber attack, how our input helped reduce the damaging impact of events, and eventual claims outcomes where applicable.

Disclaimer	+
Phishing	+
Ransomware	+
Unauthorised access	+
Social engineering fraud	+
Negligent employee	—
Malicious employee	+

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.

Total cost of loss is £227,000.

Cyber claims scenarios

Cyber threats can take many forms, and can have a devastating effect on a business. The following scenarios show some typical examples of different types of cyber attack, how our input helped reduce the damaging impact of events, and eventual claims outcomes where applicable.

Disclaimer	+
Phishing	+
Ransomware	+
Unauthorised access	+
Social engineering fraud	+
Negligent employee	+
Malicious employee	—

Malicious employee

Anneka is a senior manager at a healthcare company. She is unable to access the network and receives an extortion demand from an unknown third party threatening to release confidential patient data unless 5 Bitcoin (equivalent to around £125,000) is paid.

She notifies Aviva and we begin our investigation. We discover that the company IT manager has used their privileged access to create the ransom demand, but the forensic investigation finds that no data had been harvested due to the quick response.

The employee is prosecuted and convicted.

Total cost of loss is £45,000 to cover the forensic investigation.

Our cyber proposition at a glance



Cyber Insurance from Aviva removes the complication from protecting against cyber attacks. We provide comprehensive cover for first party, third party and reputational management costs, alongside expert support – throughout the cyber value chain.



*Limits can be increased subject to additional information and premium.

The Aviva **difference**

We are committed to continued innovation and investment to ensure we provide simple, affordable protection alongside exceptional service and support; helping you and your clients trade, adapt and evolve in an increasingly complex cyber landscape.



One policy wording traded your way

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



Access to 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.



Data-led simplicity and streamlined processes

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



Cyber education for you and your handlers

Access to training around the key trends in the cyber market, including technical product training.

➤ [**Visit Aviva Development Zone for more information on broker training**](#)

Our underwriting appetite



We have a broad underwriting appetite across industries, trades and occupations, with capacity to cover businesses with turnovers up to £250m.

Within appetite

Retail & Wholesale

- Clothing & Accessories
- Health & Beauty
- DIY & Garden
- Haulage

Professional Services

- Accountants
- Law Firms
- Insurance Brokers

Business Services

- Marketing
- Graphic Design

Manufacturing & Industry

- Food and Drink
- Textiles
- Metals
- Woodworking

Construction

- Carpenters & Joiners
- Kitchen Installation
- Painters & Decorators
- Builders

Charities & Not for Profit

Education

- Nurseries
- Schools (with less than 100 pupils)

Arts & Culture

- Galleries
- Museums
- Theatres

Leisure

- Restaurants
- Hotels
- Cafes

Agriculture

- Livestock Farming
- Horticulture
- Forestry

Motor Industry

- Service & Repair
- Vehicle Sales

Selected Healthcare & Social Care

- Physiotherapists
- Optometrists
- Alternative Healthcare Practitioners
- Counsellors
- Veterinary Surgeons
- Child Minding Services

Property Owners

Out of appetite

- **E-service Providers** Application Service Providers, Internet Service Providers, Data Networks, Data Storage and Internet Cafés
- **E-commerce risks** 100% Online Retailers, Gaming, Gambling and social Media, including Dating
- **Financial Institutions and Financial Services** Banks, Building Societies, Stockbroking & Other Currency and Securities Trading
- **Utility & Telecommunications Companies**
- **Employment Agencies & Call Centres**
- **Media** Market Research & Advertising Agencies, Animation Production, Film/TV Studios, Journalists, TV/Radio Broadcasting
- **Software Houses / Developers** including Games Developers
- **Selected Healthcare and Social Care** Social Services, Children's Homes, Nursing Homes, Hospitals, Dentists and Doctors

Comprehensive protection **as standard**



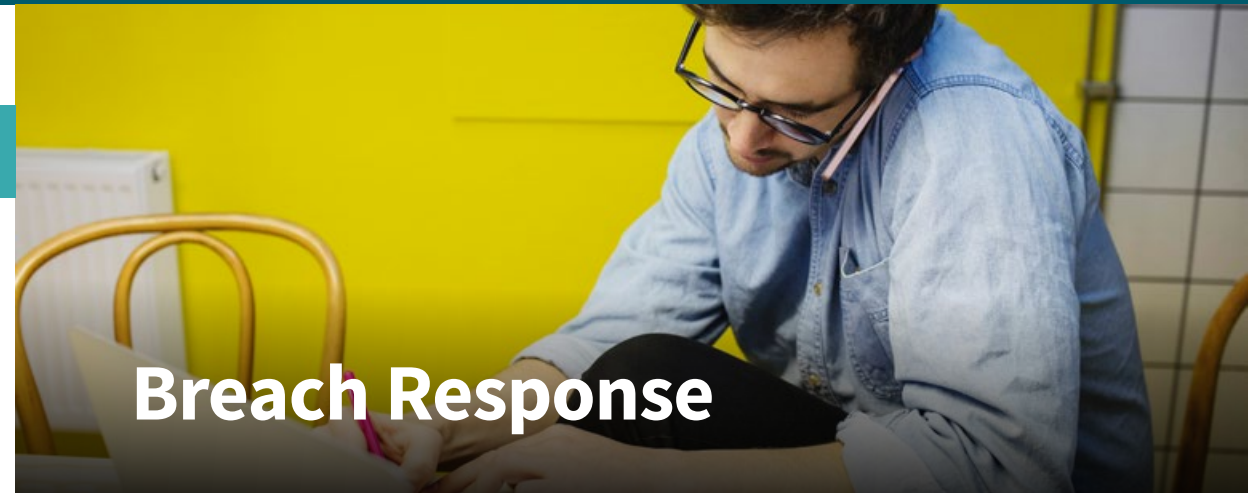
Breach Response —

First Party – Business Loss +

Third Party – Liabilities +

External Cyber Crime +

Cover Limits and Minimum Premiums +



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

Comprehensive protection **as standard**



Breach Response +



First Party – Business Loss –



Third Party – Liabilities +



External Cyber Crime +



Cover Limits and 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

Expenses to respond to actual or threatened compromise of the insured's network or data, including ransom payments (where insurable by law).

Business interruption

Cover for loss of revenue and additional increase 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

Comprehensive protection **as standard**



Breach Response +



First Party – Business Loss +



Third Party – Liabilities —



External Cyber Crime +



Cover Limits and Minimum Premiums +



Third Party – Liabilities

Data privacy and confidentiality

Cover for claims made against you due to:

- breach of confidence or misuse of individuals private information or personal data
- breach of data protection legislation
- loss or disclosure of third party confidential 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 assessment costs resulting from non-compliance with Payment Card Industry Data Security Standards due to a breach of personal data.

Comprehensive protection **as standard**



Breach Response +



First Party – Business Loss +



Third Party – Liabilities +



External Cyber Crime –



Cover Limits and 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 identity.

Theft of personal money

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

Comprehensive protection **as standard**

Breach Response



First Party – Business Loss



Third Party – Liabilities



External Cyber Crime



Cover Limits and Minimum Premiums



Cover Limits and Minimum Premiums

- Capacity to underwrite risks up to £250m annual turnover
- Standard indemnity limits range from £25k to £2m with independent limits applying to First and Third Party cover
- Increased limits of indemnity up to £5m
- Minimum premium £200+IPT
- Minimum excess of £1,000 applies

Clear and transparent terms & conditions



Comprehensive cover needn't be complicated, and our jargon-free policy wording leaves no doubt what's covered. Our policy conditions are clear, simple, and follow the recommended minimum levels of cyber security for all businesses. These conditions are also reinforced by our Statement of Fact.

Access and passwords	–
Data backup	+
Data storage	+
Payment controls	+
Software updates	+
Protection – firewall	+
Protection – virus or similar mechanism	+
Additional Statement of Fact requirements	+



Access and passwords

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

Clear and transparent terms & conditions



Comprehensive cover needn't be complicated, and our jargon-free policy wording leaves no doubt what's covered. Our policy conditions are clear, simple, and follow the recommended minimum levels of cyber security for all businesses. These conditions are also reinforced by our Statement of Fact.

Access and passwords	+
Data backup	-
Data storage	+
Payment controls	+
Software updates	+
Protection – firewall	+
Protection – virus or similar mechanism	+
Additional Statement of Fact requirements	+



Data backup

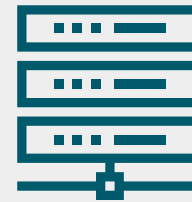
Back up no less than every seven days. Backup routine must be working, and stored securely and separately from the original data or programs.

Clear and transparent terms & conditions



Comprehensive cover needn't be complicated, and our jargon-free policy wording leaves no doubt what's covered. Our policy conditions are clear, simple, and follow the recommended minimum levels of cyber security for all businesses. These conditions are also reinforced by our Statement of Fact.

Access and passwords	+
Data backup	+
Data storage	-
Payment controls	+
Software updates	+
Protection - firewall	+
Protection - virus or similar mechanism	+
Additional Statement of Fact requirements	+



Data storage

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

Clear and transparent terms & conditions



Comprehensive cover needn't be complicated, and our jargon-free policy wording leaves no doubt what's covered. Our policy conditions are clear, simple, and follow the recommended minimum levels of cyber security for all businesses. These conditions are also reinforced by our Statement of Fact.

Access and passwords	+
Data backup	+
Data storage	+
Payment controls	—
Software updates	+
Protection – firewall	+
Protection – virus or similar mechanism	+
Additional Statement of Fact requirements	+



Payment controls

Partners, directors and employees must:

- be trained in the dangers of social engineering fraud and how to spot attempts
- be instructed in writing to follow the business's payment procedures and verify the legitimacy of payment instructions using a different contact method before making a payment for the first time or amending bank details of a supplier or customer.

Clear and transparent terms & conditions



Comprehensive cover needn't be complicated, and our jargon-free policy wording leaves no doubt what's covered. Our policy conditions are clear, simple, and follow the recommended minimum levels of cyber security for all businesses. These conditions are also reinforced by our Statement of Fact.

Access and passwords	+
Data backup	+
Data storage	+
Payment controls	+
Software updates	-
Protection – firewall	+
Protection – virus or similar mechanism	+
Additional Statement of Fact requirements	+



Software updates

Updates to software must be carried out within 14 days of an update being released, where the software supplier describes the issue as critical, important or high risk.

Clear and transparent terms & conditions



Comprehensive cover needn't be complicated, and our jargon-free policy wording leaves no doubt what's covered. Our policy conditions are clear, simple, and follow the recommended minimum levels of cyber security for all businesses. These conditions are also reinforced by our Statement of Fact.

Access and passwords	+
Data backup	+
Data storage	+
Payment controls	+
Software updates	+
Protection – firewall	–
Protection – virus or similar mechanism	+
Additional Statement of Fact requirements	+



Protection – firewall

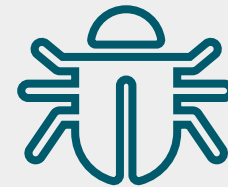
Computer equipment connected to the internet or an external network is protected against unauthorised access by a suitable and active firewall updated at least once a month.

Clear and transparent terms & conditions



Comprehensive cover needn't be complicated, and our jargon-free policy wording leaves no doubt what's covered. Our policy conditions are clear, simple, and follow the recommended minimum levels of cyber security for all businesses. These conditions are also reinforced by our Statement of Fact.

Access and passwords	+
Data backup	+
Data storage	+
Payment controls	+
Software updates	+
Protection – firewall	+
Protection – virus or similar mechanism	–
Additional Statement of Fact requirements	+



Protection – virus or similar mechanism

Install effective and up-to-date software protecting against virus and malware that's updated at least once a month.

Clear and transparent terms & conditions



Comprehensive cover needn't be complicated, and our jargon-free policy wording leaves no doubt what's covered. Our policy conditions are clear, simple, and follow the recommended minimum levels of cyber security for all businesses. These conditions are also reinforced by our Statement of Fact.

Access and Passwords	+
Data Backup	+
Data Storage	+
Payment Controls (if External Crime included)	+
Software updates	+
Protection – Firewall	+
Protection – Virus or Similar Mechanism	+
Additional Statement of Fact requirements	–



Additional Statement of Fact requirements

- You are not aware of any incidents in the past three years which would or could have led to a claim under any of these cyber covers had they been in place at the time.
- An appointed individual has responsibility for your IT policy and data security.
- You are payment card industry compliant, if applicable to your business activities.

Cyber loss prevention **services and training**



Access to Aviva experts and third party specialists means clients can better understand, protect against and prepare for cyber incidents, as well as stay ahead and informed in an ever-changing landscape. We can help them:



Understand their risks

Cyber security consultancy

Larger mid-market customers benefit from two hours' consultancy in relation to cyber security and business continuity planning.*



Protect their data

Innovative IT security solutions

Access to [Kaspersky's](#) suite of IT and endpoint security solutions at discounted rates.



Prepare their business

Cyber essentials accreditation

The [CyberSmart](#) platform is designed to assist your clients to achieve the UK government backed Cyber Essentials Accreditation, alongside the provision of ongoing device status monitoring and rapid threat detection. Available to Aviva clients at discounted rates.

Crisis simulation exercises

Designed and delivered through [HorizonScan](#), this course provides an opportunity to test the resilience of your clients' Crisis Team and the robustness of their plans. Available to Aviva clients at discounted rates.



Stay informed

Aviva risk insights

Access to a wealth of material on cyber, including webinars, loss prevention standards and whitepapers on the latest trends to keep your clients informed.

➤ [Visit our Risk Management website for more information](#)



Business support funding to help develop risk management strategies


Access to funding to part or fully fund consultancy or cyber loss prevention solutions.*

*Available for risks over £5k spend and subject to acceptance and availability

Our cyber loss prevention partners

We've partnered with key specialists in the cyber security industry to bring you access to their services and solutions that can help protect your clients' businesses.

CyberSmart	—
Kaspersky	+
Horizonscan	+



CyberSmart helps businesses protect themselves from cyber attacks through helping them attain Cyber Essentials certification. Amidst an ever-evolving landscape, CyberSmart aims to make security solutions more accessible and less complex, providing organisations with the capability to comply with recognised certification standards.

[Find out more](#)

Our cyber loss prevention partners

We've partnered with key specialists in the cyber security industry to bring you access to their services and solutions that can help protect your clients' businesses.

CyberSmart

+

Kaspersky

-

Horizonscan

+

kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialised security solutions to fight sophisticated and evolving digital threats. Over 400 million users and over 250,000 corporate clients are protected by Kaspersky.*

[Find out more](#)

*<https://www.kaspersky.co.uk/about>

Our cyber loss prevention partners

We've partnered with key specialists in the cyber security industry to bring you access to their services and solutions that can help protect your clients' businesses.

CyberSmart	+
Kaspersky	+
Horizonscan	—

HORIZONSCAN

Horizonscan specialises in increasing the ability of businesses to deal with disruptive events. Their consultants bring real work experience from careers in the emergency services and corporate Business Continuity management. They are employee-owned, which ensures all their staff bring the pride and motivation of business ownership.

[Find out more](#)

Standout 24/7 incident response

When a cyber attack occurs it usually impacts the entire business operation. Once the alarm has been raised the crisis management phase begins. The first hour is the 'golden hour', when effective action can dramatically reduce the damaging impact of the event.

We've partnered with Sedgwick's global technology practice group, to provide a 24/7 incident response service with access to their dedicated cyber and technology experts. With Sedgwick we aim to reduce the damaging impact of the event and help your client's business bounce back.

But it's not enough just to fix a security breach and get back to business as usual. Aviva's team of specialist experts will help your clients learn from an incident, enabling them to become stronger and better prepared in future.

Making a claim

Claims can be reported via our cyber claims team on **0800 051 4473**.

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

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

Specialist PR experts can help ensure the business brand is intact and minimise reputational impact on customers and suppliers.

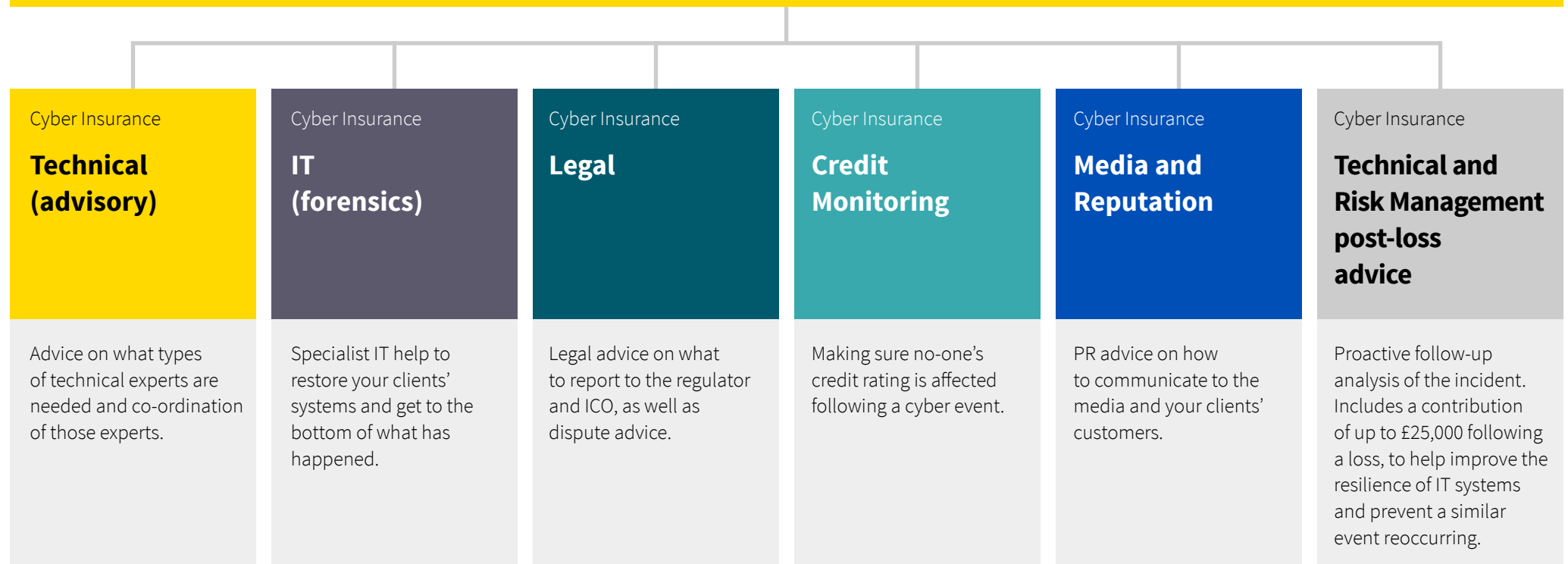
The expert panel work to contain the event, with the dedicated manager supporting your client in their recovery activities.

No excess applies for any expert guidance or initial advice.

Cyber insurance **as a service**

Cyber insurance can provide access to services that complement existing IT resources to protect data, operations, revenue and reputation, as well as manage the initial financial impact.

Our panel of cyber experts is available to businesses 24/7



Common misconceptions

Typically, misconceptions around cyber insurance tend to indicate a lack of understanding of the exposures businesses face. Below are some examples of common misconceptions and how to address them.

We already have measures in place

Cyber risks are constantly evolving. Working with Aviva will give you access to up-to-date solutions that allow you to assess your vulnerabilities and understand if current measures in place are effective.

The financial cost of attacks is not that significant

The average cost of a cyber security breach is estimated to be £5,220,¹ but the impact can extend beyond the initial financial loss. Customers will often have cover for 'tangible' risks like fire, flood and theft, but the costs for specialist forensic IT investigations and the loss of revenue due to damaged reputation can be hugely detrimental to a business.

My industry is not a target for cyber attacks

Most criminal activity isn't specifically targeted to a particular business or industry. Tools are often used to search the internet for any system vulnerability, meaning any business, small or large, can be targeted.

We already have an IT person or department

Focused resource aligned to IT is essential in helping to manage cyber risks, but ever-evolving variations of ransomware and malware, and the increasing use of phishing emails targeting human error and lack of awareness, mean not all attacks will be avoided. Aviva's Cyber Insurance dovetails with your existing strategies and, if you are breached, provides certainty through rapid response and co-ordinated access to a team of dedicated experts.

I don't have an online presence

A recent government survey highlighted that the vast majority of UK businesses (98%) rely on some form of digital communication or solutions, i.e. emails, online banking, cloud storage or digital supply chain.² An online presence is just one avenue cyber criminals can look to exploit.

As a small business, it's not relevant

In the UK, 46% of all UK businesses experienced a cyber incident in the last 12 months.¹ In March 2020, the UK saw a 400% increase in cyber incidents, particularly relevant to many businesses who shifted to remote working environments.³

I have never had a breach, so my business doesn't need it

The cyber environment is ever evolving, with cyber criminals adapting their approach and methods. Being able to proactively manage this risk is important from both a regulatory and customer perspective.

The cost of cyber insurance is too high

The cost of cyber premiums is modest in comparison to the potential cost of a cyber attack, taking into consideration data recovery, reputational and PR management, business interruption and third party liabilities. Cyber insurance is an effective tool in helping manage the impact and associated costs of an incident through a co-ordinated approach.

We don't hold any personal customer data

The definition of 'personal data' is very broad and includes information you hold about suppliers, business emails, and employees data. Cyber attacks don't always involve breach of personal data but loss of money, securities or property and interruption due to system failure.

¹Cyber Security Breaches Survey 2020, DCMS
Refer to Footnote 1.

²Cyber Breaches Security Survey 2019, DCMS
Refer to Footnote 1.

³Coronavirus-related fraud reports up 400% in March,
Action Fraud press release, 2020

About Aviva PLC

As one of the UK's largest commercial insurers, we have the scale and stability, alongside a rich 320 year history, to provide certainty that we will be around when you and your clients need us, now and for the future.



£33.2 billion
in claims*



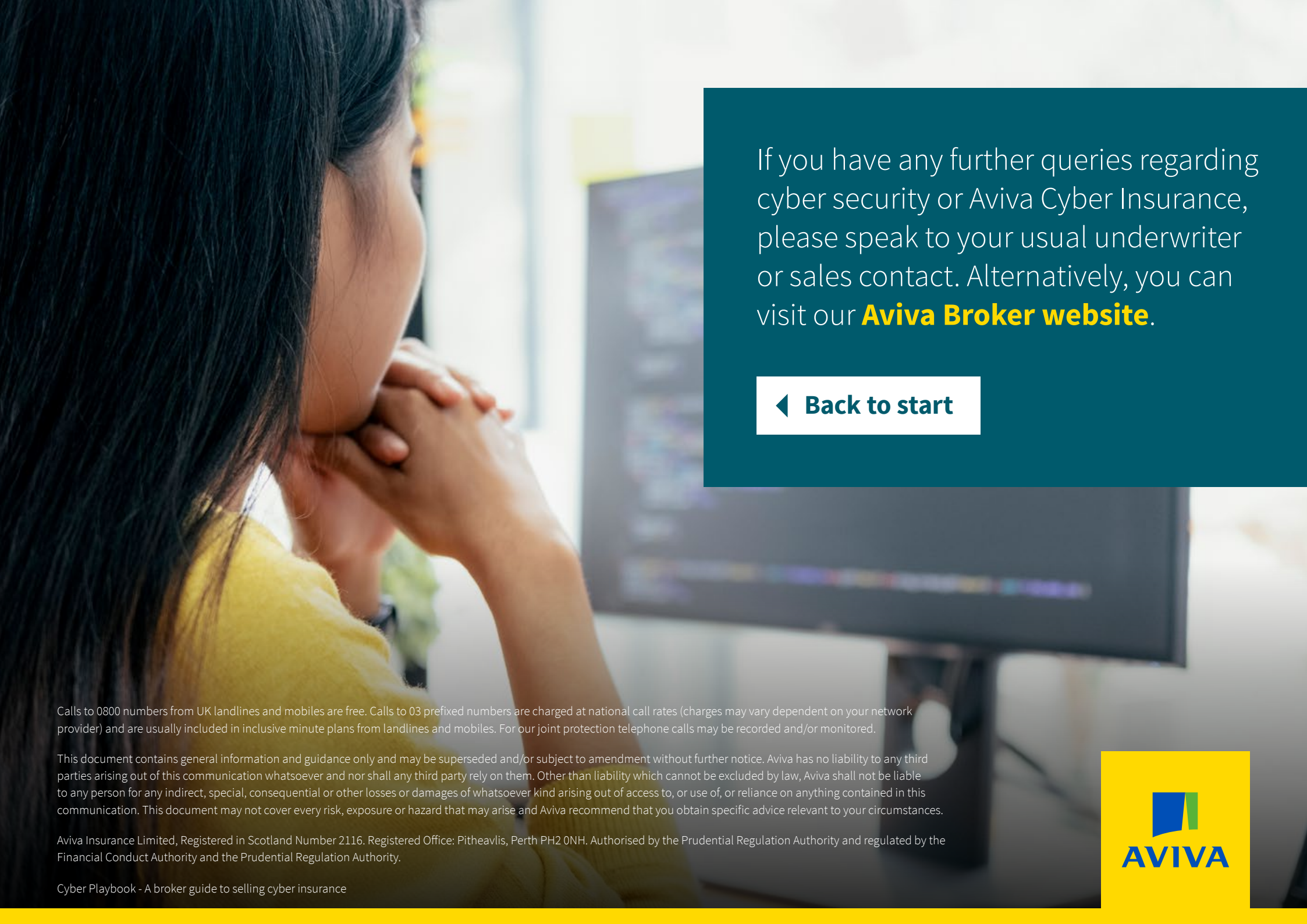
33 million
customers*



AA-
(Stable financial
strength)**

*Source: Aviva Annual Report 2019, published March 2020 on aviva.com

** Source: S&P Insurer Financial Strength Rating for Aviva Insurance Limited



If you have any further queries regarding cyber security or Aviva Cyber Insurance, please speak to your usual underwriter or sales contact. Alternatively, you can visit our **Aviva Broker website**.

◀ **Back to start**

Calls to 0800 numbers from UK landlines and mobiles are free. Calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of this communication whatsoever and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in this communication. This document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to your circumstances.

Aviva Insurance Limited, Registered in Scotland Number 2116. Registered Office: Pitheavlis, Perth PH2 0NH. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.