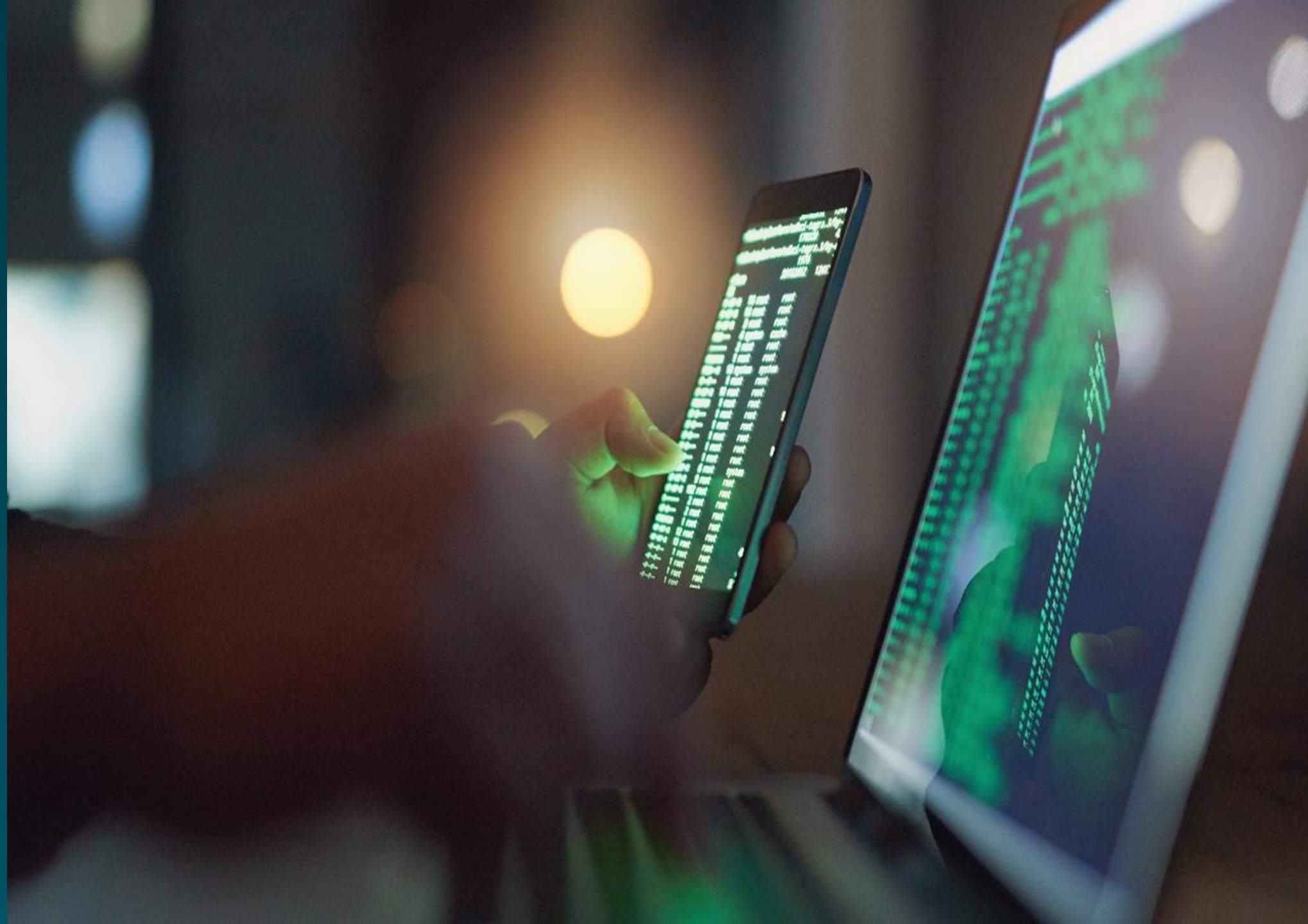
Club 110

Cyber



Introductions

Sarah Kent

Digital Trading Manager

Sarah Johnson

Specialty Lines Digital Underwriting Manager

Jake McCanney

Regional Cyber Underwriter

Digital Capability

AVIVA

Digital Capability

Our commitment is to make it easier to trade with Aviva online, no matter how a broker chooses to place their business. Here's a look at the Aviva digital products an where, and the support available.

Commercial Lines	Fast Trade	Acturis eTrade
Self-employed	✓	✓
Shop & Salon	✓	✓
Office & Surgery	✓	✓
Property Owners	✓	✓
Commercial Combined	✓	✓
Minifleet	✓	✗

Specialty Lines	Fast Trade	Acturis eTrade
Computer	✓	✗
Freight	✓	✗
Cargo	✓	✓
Group PA & Bus Travel	✓	✓
Management Liability	✓	✓
Professional Indemnity	✓	✗
Cyber	✓	✓
Plant and Equipment	✓	✓

Functionality	Fast Trade	Acturis eTrade
Insurer-led renewals	✓	✓
Submit to U/W	✓	✓
Premium flexibility	✓	✓
Commission flexibility	Minifleet/Man Liab/Group PA/PI/Cyber/P&E	Man Liab/Group PA/Cyber/P&E
Live chat	✓	✗
Dedicated team	✓	✓
Quote versioning	✓	✗
Prospecting	✓	✗
Cross-sell	✓	✗
Online2offline	Commercial Combined/Property Owners	Commercial Combined
Under Insurance Flag	Property Owners/Office & Surgery/Shop & Salon/ Commercial Combined	✗

Contact our digital teams on **0800 015 2578**

To register for Fast Trade access please visit Aviva Broker: Fast Trade - Aviva (avivab2b.co.uk). For further information on accessing our eTrade products via Acturis please visit Aviva Broker: Integrated Trading - Aviva (avivab2b.co.uk)

Digital Specialty Lines

AVIVA

Service you can count on

More support than ever

12 specialist trained UW's across Speciality Lines

Flexibility

Phone

E-mail

Live Chat

M-F 9-5

Great outcomes

- 60 mins on referrals
- Max 24-hour email response – frequently within the hour
- Speedy response times with both telephone and live chat wait times under 30 Secs

Chris Vine – Senior Specialty Lines Manager
Kat Halbert – Head of Digital Operations

Sarah Johnson
Underwriting and Performance Manager

Sarah has worked for Aviva since May 2004 and as the Digital Specialty Lines Underwriting Manager since March 2020 and has recently expanded her role to include the performance side of SL Digital

Lisa Caton
Trading Underwriter

Lisa joined the team in January 2021 having previously worked as a marine underwriter.

Stewart Hares
Trading Underwriter

Stewart has worked for Aviva for almost 30 years and joined the Digital team in 2018 from the regional engineering team.

Safdar Ali
Trading Underwriter

Safdar has worked for Aviva since 2006 and joined the Digital team in 2018 from the regional engineering team.

Jane Hulbert-McQuaide
Trading Underwriter

Jane has worked for Aviva since 1989 in a variety of roles. Jane joined the Digital team in 2018 from the regional engineering team.

Susan Freer
Trading Underwriter

Sue has worked for Aviva since March 2000 and moved into the Digital team from the regional marine team.

Fahmina Mimme
Trading Underwriter

Mimme has worked for Aviva for almost 5 years having worked previously in a customer service role

Mark Blackburn
Trading Underwriter

Mark has worked for Aviva since 2014 and moved from our Motor Claims teams to our Digital team in 2022.

George McAlindon
Trading Underwriter

George has worked for Aviva for almost 5 years and moved from our Life team in 2022.

Saqib Ali
Trading Underwriter

Saqib joined us in December 2022 having worked previously in a customer service role

Kelly Fleming
Trading Underwriter

Kelly joined us in January 2023 having previously worked in a doctors surgery

Ryan Johnston
Trading Underwriter

Ryan joined us in January 2023 having worked previously in a customer service role

Ben Scarborough
Trading Underwriter

Ben joined us in January 2023 having worked previously in a customer service role

An introduction to Cyber

Why buy Cyber Insurance

1. All businesses are at risk

Most criminal activity isn't targeted at a particular business or industry. Instead, sophisticated tools are used to search the internet for system vulnerabilities. This means any business, large or small, can be targeted – with 46% of UK businesses suffering a cyber incident in the last 12 months.

2. People make mistakes

According to research, 90% of attacks seen by the ICO in 2019, could likely be attributed to human error or mistake rather than hardware or software security vulnerabilities

3. Time is of the essence

Aviva's cyber insurance can dovetail with existing risk management strategies to provide a rapid response to any attack, and co-ordinated access to a team of dedicated experts. The first hour is the "golden Hour", where effective action can dramatically reduce the impact of the event. Small-to-medium sized companies, in particular, may not have the necessary systems in place to achieve this on their own.

4. Operations & reputations need protecting

Any businesses are heavily reliant on technology to carry out day-to-day business operations. Not being able to access vital IT systems due to a cyber attack or data breach could result in significant business interruption and reputational impact. Cyber insurance covers the loss of revenue and any subsequent increased working costs, as well as PR costs.

5. Third parties need reassurance

Cyber insurance sends a clear message to both third parties and customers that cyber security is taken seriously, and provides reassurance that adequate protection in in place should an attack occur.

6. Regulations are always evolving

With the accelerated pace of digitalisation, there is increasing focus on the Data Protection Legislation. Aviva's cyber insurance may cover against defence costs, regulatory fines and penalties, where insurable by law.

Clear and comprehensive cover

Our core coverage included as standard with the option to add External Cyber Crime

Breach Response

Experts
- Costs of an incident manager, IT forensics and legal support

Notification Costs
- Costs to notify and provide credit or identify fraud monitoring services

Reputation Management
- Costs of PR consultants

Resilient Improvements
- Costs to improve resilience of computer systems following a loss. 15% of corresponding claim up to £25k

Criminal Reward
- Costs for reward, paid by you, which leads to a conviction or recovery of a financial loss following covered cyber event

First Party – Business Loss

IT Systems and Data
- Restore, recover or repair data, software, websites or damage to computer system

Cyber Extortion*
- Expenses to respond to actual or threatened compromise of the insured's network or data

Business Interruption
- Loss of revenue and additional increase cost of working including loss of future customers due to reputational damage

Outsourced Service Providers
- BI cover extends to include interruption to your contracted providers of IT, data hosting or processing services.

System Failure
- Loss of income and additional expenses

Manufacturing and other industrial processes – up to £25K limit

Third Party - Liabilities

Data Privacy and Confidentiality
- 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
- Where insurable by law

Network Security
- Negligent transmission of a virus
- Failure to prevent unauthorised access that results in a denial-of-service attack

Multimedia*
- Copyright infringement, defamation, libel, slander and costs to remove media to minimise a loss

Payment Card Industry
- Fines, penalties and assessments resulting from the breach

External Cyber Crime

Unauthorised use of computer equipment, social engineering fraud, funds transfer fraud, telecommunications fraud, corporate identity fraud available as optional cover
- Loss of money, securities or property

* Optional cover on our digital cyber product

Considerations when placing cyber cover

Aggregate Basis

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

Claims Made

- Cyber liability policies generally written on a 'claims made' basis
- This means cover is only for claims first made against the insured and notified to the insurer during the period of insurance
- Cover can pick up events which happened prior to the inception of the policy, but only if the insured did not know about them

Excess

- Most cyber policies have a:
  - monetary excess – payable as part of a claim
  - time excess / waiting period – as part of the Business Interruption cover. This is the defined period an interruption to the business must exceed before a BI claim is payable
- Check 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.

Underwriting Appetite – Cyber

Within Appetite

Digital

- Up to £50m Turnover
- Up to £2m Cover Limit
- UK Companies
- Retail & Wholesale
- Professional Services
- Business Services
- Manufacturing & Industry
- Construction
- Education
- Agriculture
- Leisure
- Arts and Culture
- Motor Industry
- Selected Healthcare & Social Care

Regional & London

- Digital capability plus:
- Technology
- Large and Complex Risks
- Overseas Subsidiaries
- £5m Cover Limit
- Larger SMEs and mid-market organisations with a turnover of up to £250m.
- Cyber Excess of Loss - Corporate businesses and larger SMEs who require higher indemnity limits than their primary insurer can provide to manage their cyber risk exposure.

Out of Appetite

Digital & Regional

- E-Commerce Risks
- Financial Institutions and Financial Services
- Utility & Telecommunication Companies
- Media and Marketing
- Selected Healthcare & Social Care

Underwriting Appetite – Security Assumptions

Digital

- You are payment card industry compliant if applicable to your business activities
- Computer equipment and any personal devices used for accessing your computer systems have effective and up to date software protecting against virus and malicious code that is updated at least once a month.
- Computer Equipment is protected from unauthorised access by a suitable and active firewall that is updated at least once a month.
- All Data is backed up on at least a weekly basis and validated by checks. Personal and other sensitive business data is stored securely.
- Access to Your Computer Equipment is authenticated by the use of individual identification and passwords. Any default passwords or access codes are changed and kept secure.
- Updates to firmware, operating systems and software are completed to address identified vulnerabilities within 14 days from release with a severity that the provider has described as critical, important or high.
- You, their partners, directors and Employees are trained in the dangers of Social Engineering Fraud and how to spot these attempts.
- You have formal payment procedures in place which require partners, directors and Employees to independently verify the legitimacy of payment instructions before amending bank details of a supplier or customer or making a payment for the first time.

Common Objections

We don't hold any personal data.

We already have an IT person or department.

The cost of cyber insurance is too high.

I don't have an online presence.

My data is held in the cloud.

As a small business it's not relevant.

My industry isn't a target for cyber attacks.

Cyber Claims Scenarios

Ransomware – *Time is of the essence*

Scenario 1

A managing director of a retail company 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.

Fortunately she has Cyber insurance and 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 the loss is less than £10,000

Scenario 2

Similar cases 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 – Employee Error

Employee Error

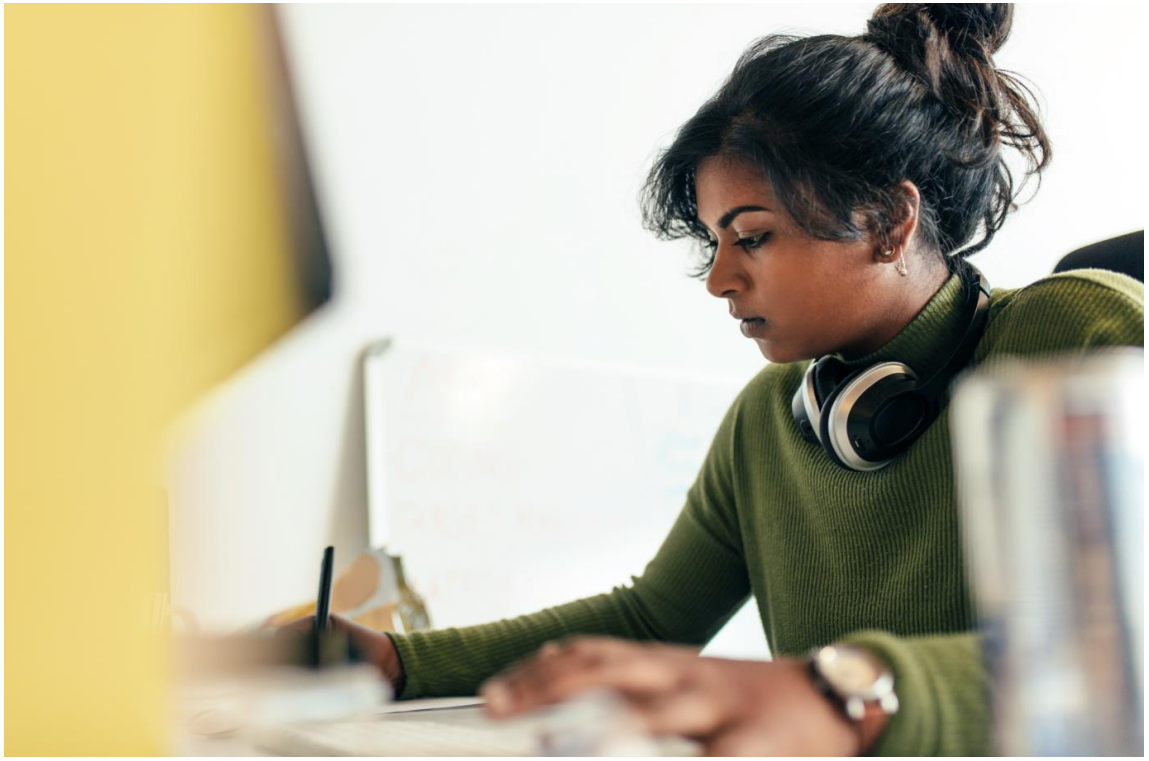
Scenario 3

An employee working in HR at an estate agency inadvertently sends an email to a colleague in another branch. The email 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. Approximately 200 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.



Meet the Cyber Team

Stephen Ridley

Head of Cyber

Tim Horsfall

Regional Cyber
Underwriting Manager

Casper Stops

London Cyber
Underwriting Manager

Jake McCanney

Sam Mullett

Harshitha Malladi

Rachel Redmond

Emily Harty

Sam Mack

Poppy Hartwell

John Clarke

Regional Team Phone Number : 0207 764 6032

Why Aviva for Digital?

we listen & act

we quote

we convert

we support

we trade

we win*

Questions?

Find out more
For more information about the products and services we provide, visit

https://connect.avivab2b.co.uk/broker/

Aviva Broker: Specialty Lines Hub - Aviva - Aviva (avivab2b.co.uk)
Today.

Risk Management Support
Our dedicated Risk Solutions website has helpful resources, guides and expert advice to help mitigate the day to day risks businesses face. Head to Aviva Risk Management Solutions - Aviva Risk Management Solutions today.

Thank you

AVIVA