A broker guide to cyber insurance

AVIVA

Why cyber risk matters

Cyber risk remains one of the most significant threats to organisations, driven by rapid technological change and a threat landscape where the speed and scale of attacks increasingly challenge traditional defences. Phishing continues to be the most common entry point, often leading to credential theft and unauthorised access to systems and data.

43% of businesses experienced a cyber security attack or breach during the last 12 months *

UK government research shows that fewer than half of UK businesses report having cyber insurance in place *

Phishing accounts for 85% of breaches experienced by businesses in the last 12 months *

Artificial Intelligence (AI) is increasing cyber risk by making attacks and defences faster and more powerful. At the same time, geopolitical instability is influencing attacker behaviour. With organisations increasingly reliant on cloud services and interconnected supply chains, a single outage or breach can disrupt operations instantly.

* Cyber Security Breaches Survey 2025 Gov.uk

Our cyber solutions

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

Use this **handy checklist** to see how our **Cyber Respond** and **Digital Complete** cover options compare to your client's existing cyber policy.

Cyber Respond	**Designed for** small businesses traded online with turnover under £1m who need fast, affordable cyber incident support. Available digitally through Fast Trade and Acturis. Ideal for micro-SMEs looking for essential protection and access to expert incident response, with limits up to £100k.
Digital Complete	**Designed for** SMEs and mid-market businesses with turnover up to £100m, available digitally through Fast Trade and Acturis. Suitable for organisations needing comprehensive cyber cover and higher limits, up to £5m.
Underwritten Complete	**Designed for** larger businesses with turnover over £100m that need tailored underwriting and enhanced limit options. Quoted offline through our regional and specialist underwriters, with limits up to £10m.
Excess of Loss	* **Designed for** organisations needing additional layers of protection above their primary cyber policy. Available offline through our specialist teams, with excess cover offering up to £10m additional limits.

Find out more about our cyber products...

Cyber support for your clients business

Our dedicated in-house cyber risk management function, helps organisations better understand, manage and reduce cyber risks. Our specialists combine technical expertise with practical industry insight to deliver clear, actionable guidance throughout your cyber insurance journey.

This approach helps clients reduce risk in practice, supported by:

- **Aviva Risk Training Solutions (ARTS)**
- **Comprehensive Cyber Risk Assessments**
- **Loss Prevention Standards**
- **Specialist Partner Network**
- **External Attack Surface Assessment**
- **Incident response planning support**

For full details of our risk management services and support, visit the ARMS website

Global cyber support

Our global network and expert in-house team respond quickly to cyber incidents anywhere in the world. We work to restore systems fast, keep you and your clients informed, and provide 24/7 access to cyber security specialists, incident responders and claims experts. Support includes IT forensics, legal advice, PR support and credit monitoring.

1. Incident reporting

1. Cyber incident reported to our dedicated team

24/7 Global Cyber Incident Response

0800 0 51 4473

@ cyberclaims@aviva.com

2. Initial expert guidance

Immediate advice from a Cyber Incident Manager - without triggering the policy excess.

2. Incident management

3. Dedicated manager assigned

To co-ordinate response and keep all parties informed.

4. Forensic Investigation

IT specialists assess the nature, scope and impact of the incident.

5. Legal guidance

Receive initial legal advice on regulatory and contractual obligations.

6. Ransom negotiations

Strategic engagement to help resolve extortion threats effectively.

3. Response and recovery

7. System restoration

Rebuild IT infrastructure to reduce business interruption.

8. Reputation management

Manage madia narratives and restore stakeholder confidence.

9. Ongoing legal support

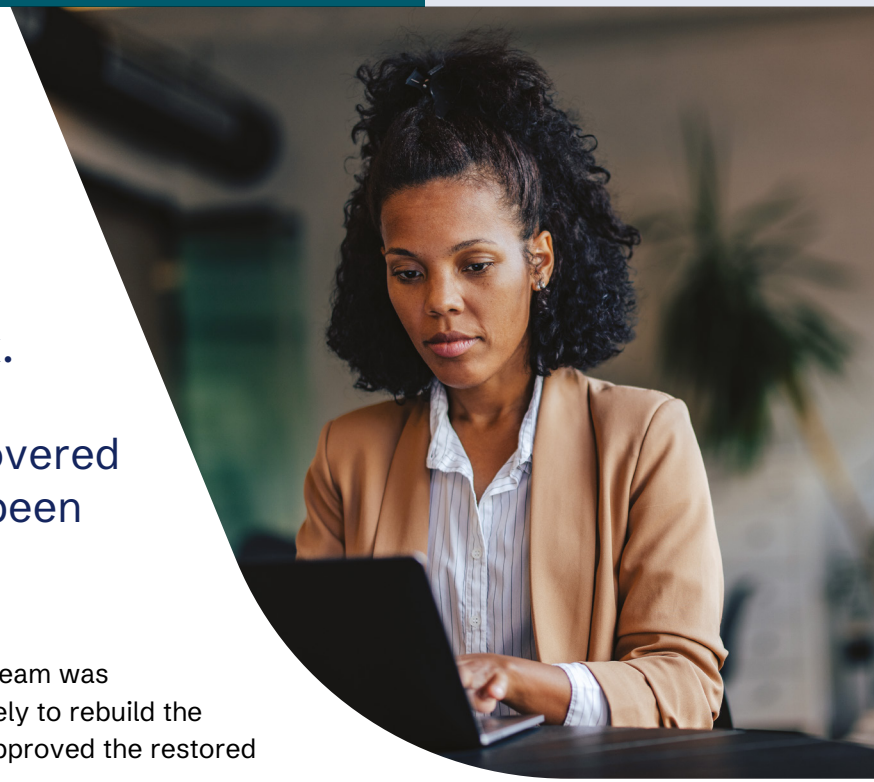
Further legal advice as the situation evolves.

4. Incident resolution

10. Business interruption review

Assess and address financial losses resulting from operational downtime.

Claims story: Ransomware attack



A professional sports club was targeted by a ransomware attack. The club's Remote Monitoring and Management (RMM) system generated multiple offline alerts. Upon investigation, it was discovered that all affected systems had been encrypted, and backups had been deleted, leaving the club with severely impacted operations.

Response:

The club reported the incident to Aviva immediately. Within two hours, a specialist breach response team was deployed, including on-site experts. Despite the loss of backups, IT forensics teams worked intensively to rebuild the club's systems from available data and system artefacts. The local safety committee reviewed and approved the restored systems, enabling the club to proceed with their next match within a week.

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
Cost of incident:	c.£280,000 in breach response and recovery services
	c.£155,000 in fees to the relevant specialists, including IT forensics and recovery experts
	c.£65,000 in legal and incident management fee

Outcome:	The club avoided long-term disruption and resumed operations within a week. The incident did not result in a data breach but caused significant operational and financial impact.
Total cost:	**c.£500,000**

The scenario shown in this document is based on a real-life case, but has been heavily anonymised to protect identities and sensitive details.

Any questions?

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

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority

aviva.co.uk

PCCAM6314 05.2026

AVIVA