
Navigating Tomorrow's Cyber Risks Today

Webinar will commence shortly



Navigating Tomorrow's Cyber Risks Today

Hosted by



Simon Hall
Client Executive
Adler Fairways



Adler Fairways

Chartered Insurance Brokers



NAVIGATING TOMORROW'S CYBER RISKS TODAY

Cyber risks and your business



Robin Knowles
AI & Automation Lead
UKGI Group

The
UKGI
Group

CYBER RISK IS A BUSINESS RISK

It affects how you operate, get paid, protect information and retain trust.

OPERATIONS

PAYMENTS

DATA

TRUST

46%

of surveyed small UK businesses identified a cyber breach or attack in the previous 12 months

Includes attempted attacks such as phishing.
Not a successful-hack rate. Small businesses, 10–49 employees.

OPERATIONS

Systems or Services Interrupted

PAYMENTS

Funds Diverted or Delayed

BUSINESS IMPACT

DATA

Information Lost or Disclosed

TRUST

Customer Confidence Affected

SIX RISKS EVERY SME SHOULD RECOGNISE



PHISHING & PAYMENT DIVERSION

Fake messages lead to unsafe clicks, disclosures or payments.



RANSOMWARE

Data or systems are locked, and data may also be stolen.



ACCOUNT TAKEOVER

Criminals use stolen access to reach business accounts.



DATA EXPOSURE

Confidential or personal information is disclosed or lost.



SUPPLIER COMPROMISE

A connected service provider in your chain is attacked.



SERVICE DISRUPTION

Websites or business systems become unavailable.

EXTERNAL THREAT

Convincing Impersonations

Cloned voices, polished messages and fake video can make familiar scams feel more credible.



"Please change the bank details and pay today."

INTERNAL RISK

Uncontrolled AI Use

Sensitive information entered in unsuitable AI tools can create data protection and confidentiality issues.

Client List.xlsx >

AI Assistant

PAUSE

VERIFY

USE A TRUSTED CHANNEL

THE EU AI ACT. DOES IT MATTER TO A UK SME?

WHAT?

EU rules for certain AI uses, with duties based on risk and role.

WHO?

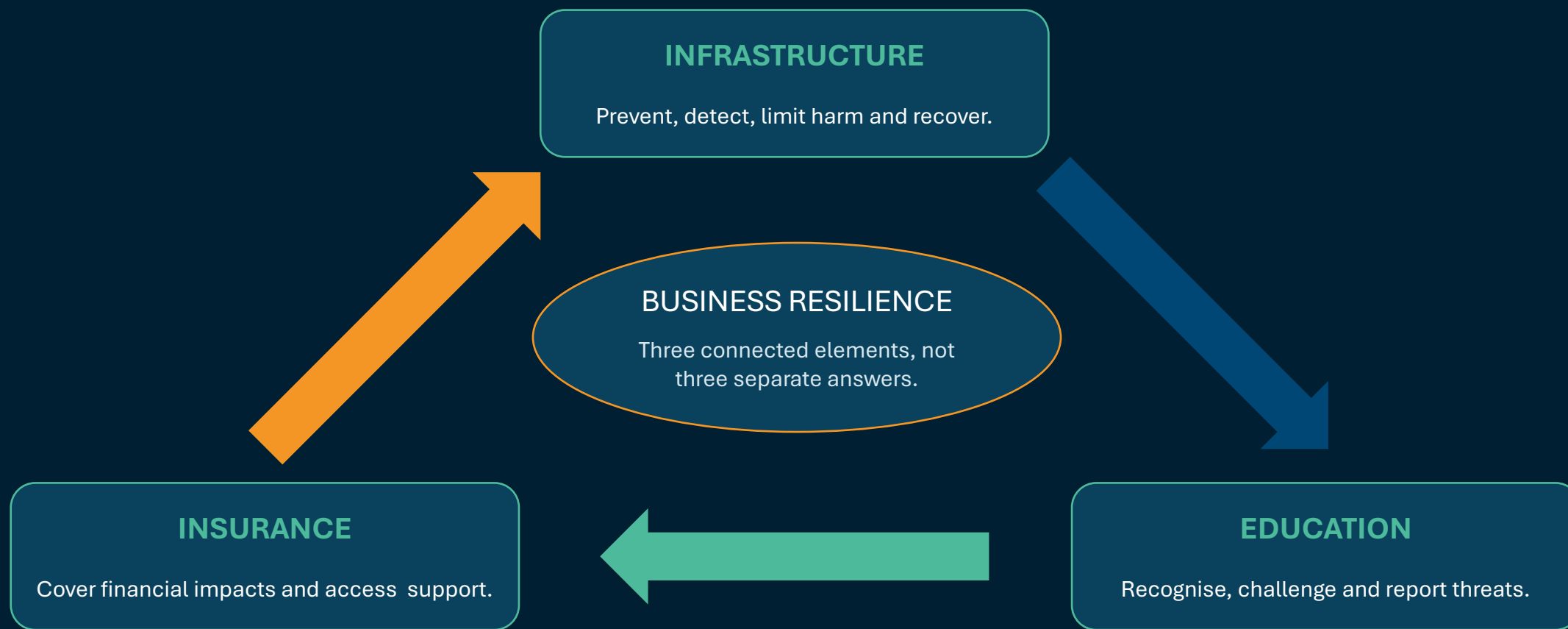
Relevance depends on the AI system, the business's role and the EU connection.

WHEN?

Main rules began applying in August 2026, with exceptions and later high-risk deadlines.

A UK business is neither automatically in scope nor automatically exempt.

THE CYBER SECURITY TRIAD



THREE QUESTIONS TO TAKE AWAY

01

What would stop you trading tomorrow?

Systems | Data | Suppliers

02

Who would spot something suspicious?

Email | Calls | Payments | AI

03

What happens if something gets through?

Response | Recovery | Insurance

Why SMEs are attractive target

And what you can do about it



Nigel Plant MCIIIS
Senior Security Consultant
Cyber Crowd

*Saying “It won’t happen to us”,
is not a security control.*

Small does not mean invisible

Most SME cyber risk is not about Hollywood-style targeting

Cyber criminals do not need to choose your business personally. They scan the internet, phish and automate at scale.

46%

small businesses identified a breach or attack

38%

businesses experienced phishing attacks

88%

of breach reports involved phishing or social engineering

The practical point

If you have email, cloud systems, payment processes, customer data or trusted relationships, you have value.

What attackers can actually use

SMEs often hold more exploitable value than they realise



The criminal does not need everything. One useful account, one payment process, or one trusted relationship can be enough.

You may be the route, not the destination

Supply chain trust can make smaller organisations attractive

Attackers exploit trust

A smaller business can become the steppingstone into a larger customer, partners, supplier or platform.

- Shared portals
- Supplier email chains
- Payment processes and financial data
- Remote access
- Hosted data or files

Ask yourself

Who relies on us, and what could an attacker do if they successfully pretended to be us?

Cyber attacks human decision-making

Criminals try to force fast reactions before slow checks kick in

FAST THINKING

Urgency “I need this Now”

Authority “It’s the CEO asking”

Fear “Your Account is compromised”

Reward “You’re due a refund”

Familiarity

SLOW THINKING

Was I expecting this?

Does the request make sense?

Can I verify another way?

Has the bank detail changed?

Would I be happy explaining this later?

The aim is not to make people perfect. It is to design checks that help people pause and verify.

A realistic SME incident

The attack often looks ordinary until it is too late

Friday, 4:17pm

- A known supplier emails about an overdue invoice
- The thread contains names, context and the right invoice number
- They say bank details have changed and payment is urgent
- **The email is genuine — but the mailbox is compromised**

Question to ask yourself

What would stop this becoming a loss?

What SMEs should do next

Defense In Depth: multiple layers of controls help reduce likelihood, reduce impact, manage what remains

1

Protect identity

MFA/passkeys, no shared accounts, separate admin access

2

Keep systems healthy

Supported software, updates, secure configuration

3

Protect the money

Verify payment changes using a known route

4

Limit blast radius

Least privilege, backups, restore tests

5

Make reporting easy

No-blame culture and clear escalation

6

Use a baseline

NCSC Cyber Action Toolkit and Cyber Essentials

“Cyber security is not about eliminating every risk. It is about making common attacks harder, limiting damage, and being ready to recover.”

Managing Residual Risk

After sensible controls, some risk remains

- ✓ **Manage Cyber Risk.**
- ✓ **Protect against Attack.**
- ✓ **Identify cyber incidents.**
- ✓ **Minimise the impact.**
- **Manage the residual risk.**

That is where the insurance discussion becomes relevant:

What happens if all else fails, operations stop, specialist help is needed, or a claim arises?

Over to Tyne Hill, CFC

You do not have to be perfect, but you do need to be prepared.

When prevention fails, what happens next?

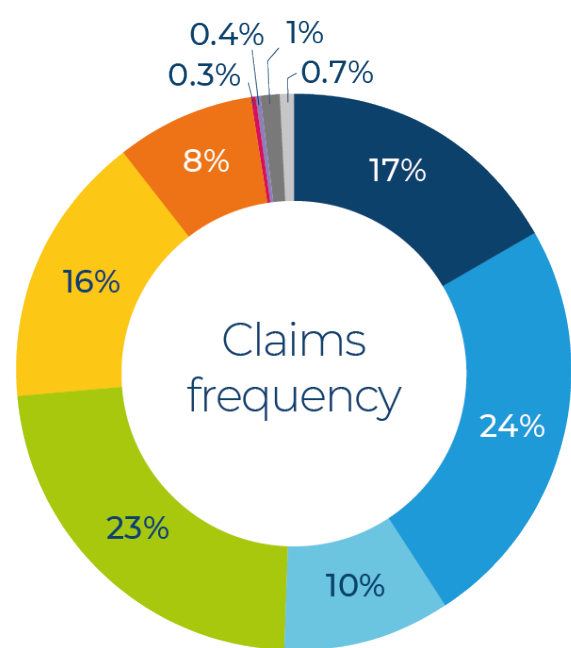
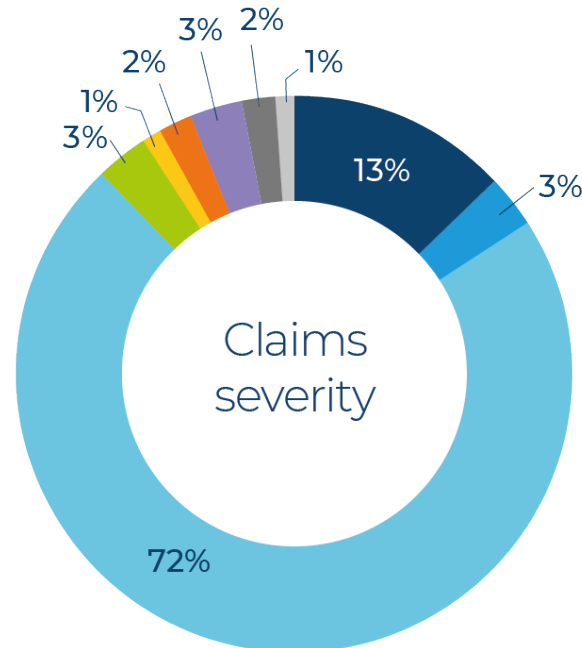


Tyne Hill
Cyber Development
Manager UK&I
CFC



When prevention fails, what happens
next?

UK cyber claims breakdown



**CFC cyber claims data from January – December 2024*

One click became a business-wide incident

Cyber claims

When an employee fails to recognise a malicious attachment, it prompts a full-blown ransomware attack.

Attack method

Employee received a phishing email and opened the attachment which downloaded malicious software



How we remediated the attack?

Ransom demand of £195,000 in exchange for the decryption key

Advised not to pay due to threat actors reputation

Pulled any data leaked online, rebuilt the systems from back-ups



Over 75% of claims are the result of human error. It's important that staff are well versed and trained in identifying phishing emails and content.

What could have happened?

Luckily, they were insured with CFC so they incurred no costs. They avoided the ransom demand and did not have to pay the estimated £61,000 for a forensic investigation and third-party legal assistance. These costs were all covered by CFC.

No costs incurred
by the insured

How we remediate cyber attacks

Technical expertise and real-world experience can make the difference between suffering a catastrophic loss or getting back online quickly.



1

Notify

Available 24/7, the fastest way to notify CFC of a cyber incident is through our mobile app, Response. Customers can also notify via email, phone or the website.

2

Triage

A technical incident responder will be in touch within 15 minutes to assess the situation and identify the necessary resources to address the incident.

3

Contain

CFC activates its expert, in-house team of cyber security engineers, forensic specialists and threat analysts to contain and remediate the incident. We'll also engage third-party specialists to help with activities like reputation management and breach notification.

4

Recover

Once the issue is contained, our team works around the clock to rebuild systems, reconstitute data and get the business back online as soon as possible.

Protecting businesses against cyber risk

Market-leading cyber insurance that starts working from day one, backed by our in-house cyber security and incident response team.



Proactive cyber attack prevention

24/7, always-on services to help stop incidents, at no extra cost.



Incident response and cyber claims

Expert support to contain, investigate and recover from attacks, fast.



Comprehensive cyber cover

Broad cyber risk protection, backed by a 99.4% claims acceptance rate.



Cyber SME Insurer of the Year

Zywave Cyber Risk Awards 2026



Underwriting Team of the Year

Intelligent Insurer Cyber Insurance Awards 2025

85+

Countries

\$800m

Premium

100,000+

Cyber customers

If the worst happened tomorrow, would your business be ready?

#1

Know what keeps you trading

Identify the systems, data, suppliers and processes your business cannot operate without.

#2

Know how you would respond

Agree who takes control, how the incident is escalated, and how people are supported.

#3

Know who you would call

Keep your broker, insurer and incident-response details accessible outside your usual systems.

QUESTIONS

Do you have any questions?

If you have a question for our
presenters, please use the Q&A
button on your screen



CONTACT US

For further help and advice

Cyber Insurance Contact:

Oliver Steppe

Client Adviser – Professional Risks
0117 235 8801
oliver.steppe@adlerfairways.co.uk

Nigel Plant

CyberCrowd
0203 858 7372
nplant@cybercrowd.co.uk

Robin Knowles

UKGI Group
01925 939 055
robin.knowles@ukgigroup.com

Tyne Hill

CFC
0772 111 1478
thill@cfc.co.uk

Adler Fairways, Adler Insurance Brokers and Adler Insurance Group are registered trading names of Adler Fairways Insurance Brokers Limited. Adler Fairways Insurance Brokers Limited is authorised and regulated by the Financial Conduct Authority under Registration Number 309236. Adler Fairways Insurance Brokers Limited is registered in England and Wales under registration number 04525948. Our registered address is Number 22 Mount Ephraim, Tunbridge Wells, Kent TN4 8AS.

The
UKGI
Group

Adler Fairways are part of UKGI Group

