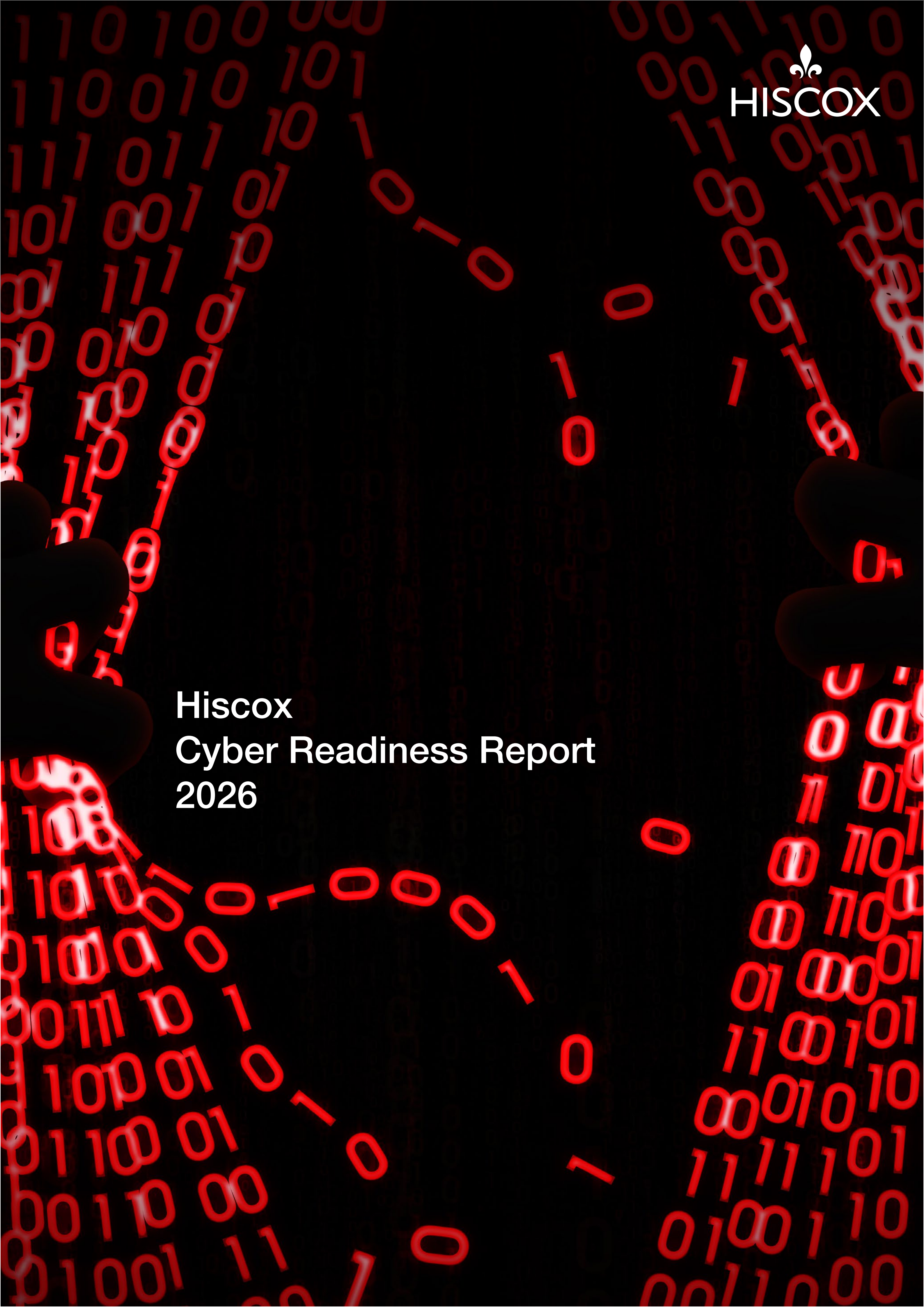


Hiscox
Cyber Readiness Report
2026

A DECADE OF CHANGE: FROM DEFENCE TO RESILIENCE

Now in its tenth year, the Hiscox Cyber Readiness Report shows how dramatically the cyber risk landscape has evolved, with companies now treating it as a core business risk.

Over the past decade of our cyber readiness research, we've seen a clear shift in how businesses approach cyber risk – from reacting to incidents to building true resilience into their day-to-day operations.

That progress is visible in how organisations are investing more consistently in training, technology and specialist expertise, and how cyber security is now being embedded firmly into business strategy. It's no longer viewed as a standalone operational challenge, but as a board-level priority that can shape continuity, reputation and growth, and that's an important step forward.

What's also changing is accountability. Cyber risk is now widely recognised as a business risk, not just a technical one, and nearly a third of organisations now link leadership performance and remuneration directly to cyber security outcomes following an attack.

Resilience today is about being prepared, responding effectively, and continuing to operate in the face of disruption. That's where we see the most meaningful progress and where continued focus will matter most.

Eddie Lamb
Global Head of Cyber
Hiscox

The Hiscox Cyber Readiness Report tracks the cyber preparedness and experiences of organisations across the USA, UK and mainland Europe (France, Germany, Spain, Ireland, Portugal, Italy, the Netherlands and Belgium). The 2026 study was conducted by Wakefield Research between 5th and 17th June 2026 and is based on responses from 6,800 cyber security decision-makers working in organisations with fewer than 250 employees.

TEN YEARS OF CYBER READINESS: WHAT'S CHANGED?

When the first Hiscox Cyber Readiness Report was published in 2017, many businesses were still asking whether cyber security was primarily an IT issue. A decade later, that question has been answered.

THEN VS. NOW

2017	2026
> Cyber security seen primarily as an IT challenge	> Cyber risk recognised as a business risk
> Concern centred on hackers and breaches	> Concern extends to AI, supply chains, reputation and people
> Cyber security focused on technology and prevention	> Resilience defined by preparedness, response and recovery
> 53% of businesses were classified as cyber novices	> 97% now actively taking steps to improve cyber resilience
> 40% had cyber insurance	> 64% now have cyber insurance
> 55% involved executive leadership in cyber strategy	> 32% now link executive performance or compensation to cyber security outcomes
> 57% experienced at least one cyber attack in the previous year	> 29% experienced at least one cyber attack in the previous year

Figures are indicative of how business attitudes and behaviours have evolved over the past decade. Findings are not directly comparable due to changes in survey scope and methodology.

Ten years ago the question was how to stop cyber attacks. Today the question is how organisations continue to operate and grow despite them.

THREE LESSONS FROM A DECADE OF RESEARCH

Technology alone is not enough

The 2017 report found that many organisations viewed technology as the primary solution to cyber risk. A decade later, the strongest performers combine technology with governance, training, process and accountability.

Cyber security is a leadership issue

Early research highlighted the importance of board involvement. Today, cyber security is increasingly embedded in leadership decision-making and business strategy.

Resilience creates competitive advantage

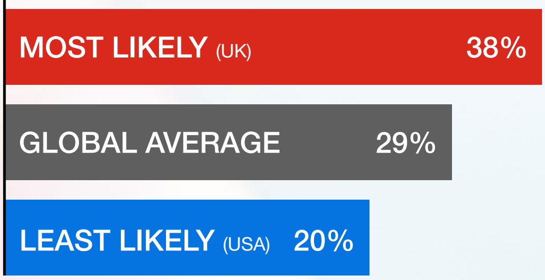
Organisations are increasingly judged not simply by whether an incident occurs, but by how effectively they respond, recover and maintain stakeholder trust when disruption happens.

CYBER ATTACKS IN 2026:
A ROUTINE COST OF DOING BUSINESS

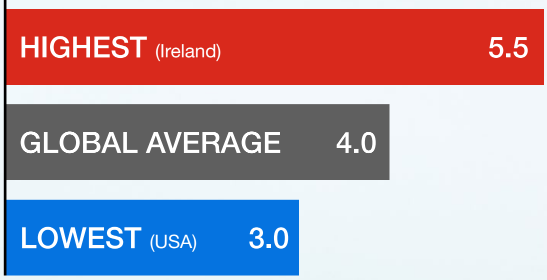
Cyber attacks are no longer an occasional threat but a regular feature for businesses operating in the digital economy. Nearly **one-in-three** organisations globally (29%) have been hit by at least one successful cyber attack in the past 12 months, with those affected reporting an average of **four incidents** over the same period.

The financial and operational consequences are significant. On average, cyber incidents now cost organisations around **$52,000 annually**, in addition to approximately **32 hours** of operational disruption on average.

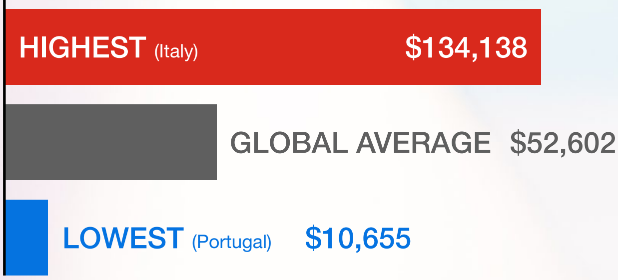
LIKELIHOOD OF EXPERIENCING A SUCCESSFUL CYBER ATTACK:



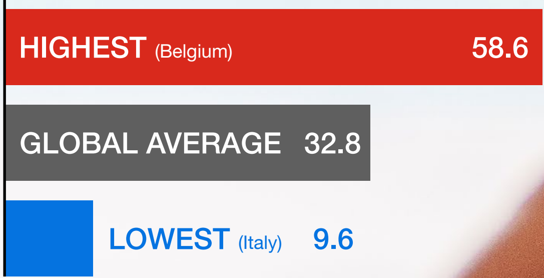
AVERAGE NUMBER OF SUCCESSFUL ATTACKS IN LAST 12 MONTHS:



AVERAGE COST OF ATTACK:



AVERAGE DOWNTIME IN HOURS:



FROM OPERATIONAL DISRUPTION TO BUSINESS IMPACT

The effects of cyber attacks extend well beyond immediate financial loss, with clear implications for business performance and growth.

Among organisations that have experienced an attack:

32% report delays to growth and expansion or new business initiatives.

31% cite increased staffing or external expertise costs.

30% report a negative impact on financial performance, valuation or credit rating.

29% have lost business opportunities or partnerships as a result of a hack.

This shows the extent to which cyber incidents have the potential to shape strategic decision-making, slow growth and put additional strain on resources.

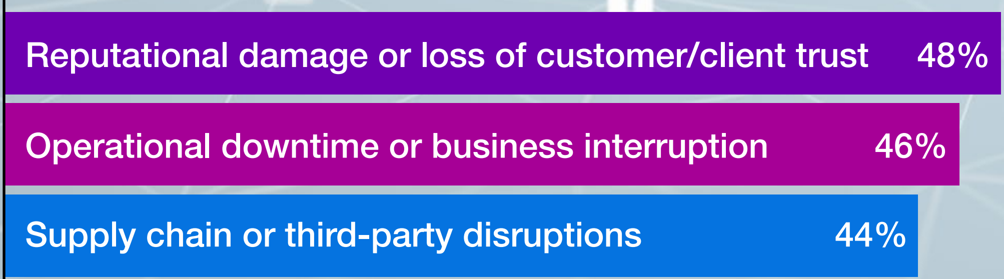
THE IMPACT BEYOND THE BALANCE SHEET

Reputational damage or **loss of customer/client trust** now rank as the most significant risk for nearly half of businesses (48%), reflecting the importance of brand resilience in a highly connected environment.

Among those organisations that experienced a hack, a significant proportion also report being impacted by **financial penalties** (28%) or **negative publicity** (26%).

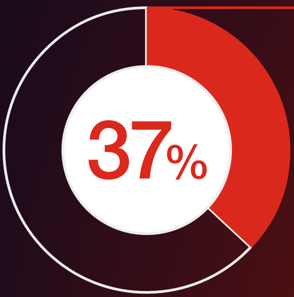
This shift underscores a broader evolution in how cyber risk is understood: from a technical challenge to a core business issue with direct implications for competitiveness and long-term value.

TOP THREE RISKS FACING BUSINESSES TODAY

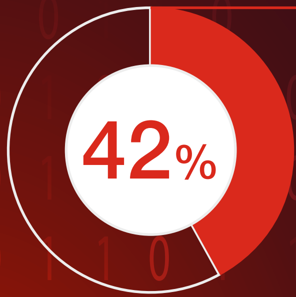


COUNTRY COMPARISONS

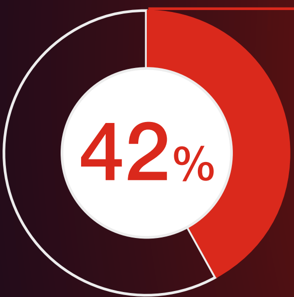
From financial losses and delayed growth to reputational damage, the impact of cyber attacks differs considerably between markets. These findings reveal where businesses are feeling the effects most strongly.



German businesses are most likely to delay growth, expansion or new business initiatives as a result of a hack.

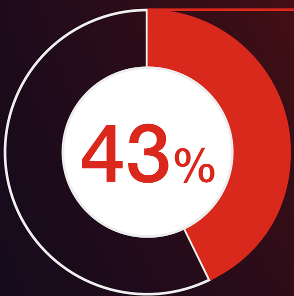


Businesses in the Netherlands are most likely to face increased staffing or external expertise costs.

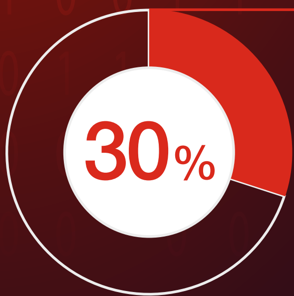


Businesses in Portugal are most likely to delay adoption of AI or other new technologies.

Italian businesses are most likely to lose business opportunities or partnerships.



Irish businesses are most likely to be hit by a substantial fine that had a significant impact on the financial health of the business.



French businesses are most likely to experience bad publicity impacting brand and reputation.

While the nature of the impact differs, cyber incidents are affecting growth, profitability and reputation across every market surveyed.

AI RISK MOVES MAINSTREAM

Artificial intelligence is already reshaping the cyber threat landscape. While businesses increasingly see AI as an opportunity, they are also facing a new generation of risks, from manipulated AI models and compromised training data to sophisticated phishing and social engineering attacks.

Businesses are responding by increasing investment in skills, governance and oversight, recognising that resilience must evolve alongside adoption.

17% identify AI tools and software as an entry point for successful cyber attacks.

TOP AI CYBER CONCERNS OVER THE NEXT FIVE YEARS

48%	AI data poisoning
43%	Over-reliance on AI reducing human oversight
43%	Vulnerabilities from third-party AI tools
41%	AI-powered malware and phishing

THE BIGGEST AI RISK ISN'T THE TECHNOLOGY. IT'S HOW IT'S USED.

Businesses are less concerned about speculative future AI scenarios than practical risks that already exist today, including corrupted training data, vulnerable third-party tools and reduced human oversight.

HOW BUSINESSES ARE RESPONDING

Plan to upskill employees in AI and cyber security	33%
Expanding AI awareness and training programmes	33%
Reviewing cyber insurance arrangements to ensure AI risks are covered	32%
Planning regular AI audits	31%

BUILDING RESILIENCE WHERE IT MATTERS MOST: PEOPLE, PROCESSES AND TECHNOLOGY

Companies are moving beyond technical fixes by strengthening their cyber resilience through a coordinated approach spanning skills, systems and governance. In fact, businesses are investing on average around **$51,000** a year in strengthening their cyber resilience.

PEOPLE

62% are updating employee cyber security training.

EXPERTISE

55% are hiring additional cyber security personnel.

TECHNOLOGY

51% are investing in new software and tools.

ACCOUNTABILITY

32% link executive compensation or performance metrics directly to cyber security outcomes following an attack.

Cyber resilience investment (US Dollars), by country	
Spain	$80,900
Italy	$73,800
UK	$59,700
Average	$51,000
USA	$49,500
Germany	$43,600
Ireland	$43,600
Belgium	$34,600
France	$32,700
Netherlands	$26,400
Portugal	$10,700

Executive compensation/ performance linked to cyber security outcomes, by country	
Germany	41%
Ireland	36%
Belgium	35%
France	34%
Spain	33%
Netherlands	33%
Average	32%
Portugal	32%
Italy	32%
USA	26%
UK	25%

The countries investing the most are not necessarily the countries demonstrating the highest levels of executive accountability.

THE HUMAN COST OF CYBER ATTACKS

Cyber incidents affect far more than technology and finances. For many organisations, the consequences are felt most acutely by employees through increased stress, burnout and workplace disruption.

As businesses strengthen their cyber resilience, employee well-being, culture and engagement are becoming increasingly important indicators of recovery.

69% report employee burnout, high stress or a toxic workplace culture following a cyber attack.

IMPACT ON EMPLOYEES

- **33%** High employee stress
- **31%** Employee burnout
- **30%** Increased sick days
- **27%** Toxic workplace culture

CYBER ATTACKS ARE RESHAPING HOW PEOPLE WORK

Among organisations that have experienced a cyber attack:

Moved from employee-owned devices to company-managed devices	30%
Limited staff access to critical data	28%
Reduced remote or hybrid working access	25%

RESILIENCE IS A PEOPLE ISSUE

The organisations that recover most effectively are not simply investing in technology. They are strengthening training, access controls, governance and workplace culture to support employees through disruption.

RESILIENCE AS A COMPETITIVE ADVANTAGE

The cyber landscape has changed dramatically over the past decade. The challenge for businesses today is no longer simply preventing attacks, but building the capability to respond, recover and continue operating when disruption occurs.

From our experience insuring cyber risk, the strongest organisations are not necessarily those that suffer the fewest incidents. They are the ones that are prepared, respond decisively and learn from disruption when it happens.

FIVE WAYS TO BUILD CYBER RESILIENCE

01 Use trusted security tools

Install reputable, up-to-date security software across all devices to help identify, block and respond to threats.

02 Strengthen access controls

Use password managers and multi-factor authentication (MFA), and limit access to sensitive data to only those who need it.

03 Keep systems current

Regularly update software and devices to address vulnerabilities and maintain strong protection.

04 Back-up data and test recovery

Ensure data is backed up securely and regularly tested, so operations can be restored quickly after an incident.

05 Manage permissions carefully

Review and update user access regularly to reduce the risk of internal threats and accidental data exposure. This includes managing access to AI systems and agents.

Take the test! Understand more about your cyber security strengths and weaknesses with the **Hiscox cyber maturity model** and compare your performance to thousands of other businesses just like yours.

Hiscox
22 Bishopsgate
London EC2N 4BQ
United Kingdom

T +44 (0)20 7448 6000
E enquiries@hiscox.com
www.hiscoxgroup.com

23383 09/26