



CYBER READINESS REPORT 2025

SMEs take action against
current and future cyber
security threats



Contents

- 03 Introduction
- 04 Executive summary
- 05 Key findings
- 06 State of attacks
- 09 Taking action
- 10 Cyber resilience
- 11 AI and future threats
- 13 Mandatory disclosures
- 14 Country comparisons
- 15 Cyber security tips for SMEs

The Hiscox Cyber Readiness Report is based on research conducted by Wakefield Research with 5,750 businesses, where the individuals responsible for their organisation's cyber security strategy were interviewed. This means the owner, principal or partner for those companies with fewer than 50 employees, and either the CIO, CISO, or the director/VP of security or IT for those companies with 50-249 employees.

Research was conducted between 29 July and 8 August 2025, using an email invitation and an online survey, and respondents can be broken down by geography as follows: 1,000 respondents in the USA, UK, France, Germany and Spain respectively, 500 respondents in Ireland and 250 in Portugal.

As research data, this represents a cross-section of insured and uninsured businesses that may or may not have made an insurance claim following an incident. It is not necessarily indicative of our own claims experience or that of the wider insurance industry.

Introduction



Eddie Lamb
Global Head of Cyber
Hiscox

The rise of digital commerce has created tremendous opportunities for small businesses, empowering them to innovate, reach new markets, and play an increasingly vital role in the global economy. Perhaps most powerful of these recent developments is artificial intelligence (AI), allowing SMEs to deploy tools and resources that would previously have been out of reach.

But these opportunities also present challenges. As businesses embrace new technologies, they must also navigate a landscape where evolving cyber threats can jeopardise their success in new ways. This ninth edition of the Hiscox Cyber Readiness Report is designed to help small- and medium-sized enterprises (SMEs) better understand the risks they face in our fast-evolving, technologically driven world, and the steps they can take to minimise their exposure to those risks. Having previously built and grown my own small business, it's something I'm particularly passionate about.

We spoke to 5,750 business across the UK, USA, France, Germany, Spain, Ireland and Portugal to understand the impact cyber attacks have on their business, and the most common exposures they face. More than half told us they had experienced a cyber attack in the last 12 months, and a third of those said they had faced a regulatory fine as a result of a data breach that was substantial enough to impact the financial health of their business.

This underscores the importance of SMEs taking all necessary steps to protect customer data, in line with regulatory requirements such as the General Data Protection Regulation (GDPR) in Europe or the consumer protection laws enforced in the US by the Federal Trade Commission (FTC).

Ransomware attacks remain a particularly persistent threat for many businesses. The SMEs we spoke to lifted the lid on their own ransomware attack experiences, with some paying multiple times in an attempt to safeguard their sensitive data but where paying a ransom is no guarantee of recovering your data. Three-out-of-five SMEs who paid a ransom said they got some or all of their data back, but for almost a third of those who paid a ransom, the attackers went on to demand more money.

Our report also looks at the impact of AI on small businesses, for whom it can be both friend and foe. While AI brings opportunities and new ways to detect and respond to threats, it also introduces new vulnerabilities – creating blind spot entry points and exposing gaps in data security that hackers can exploit in much the same way as they did with cyber ten to 15 years ago. With AI increasingly integrated into daily business activities, our specialist teams at Hiscox are focused on defining its risks, establishing cover for it, and creating the necessary knowledge and training around it to support small business owners around the world.

And yet, while the cyber landscape may be built on shifting sands, the SME response to it is proactive and pragmatic. The vast majority of SMEs (94%) plan to increase their cyber security and data protection investments over the next 12 months. That includes hiring cyber specialists, updating training programmes, conducting regular vulnerability checks, and reassessing risks across their supply chains.

At Hiscox, we're proud to stand alongside these businesses, offering not just insurance, but insight, expertise, and support. Our 20+ years' experience in privacy and cyber insurance, and our work with more than 80,000 cyber insurance customers worldwide, means that every day we are helping businesses recover from incidents, strengthen their defences, and build long-term resilience.

When it comes to cyber security and business resilience, we cannot afford to rest on our laurels and consider our work finished. Instead, we must maintain our collective resolve to overcome cyber crime, and prioritise an ongoing commitment to cyber risk management.

We hope this report inspires more businesses to benchmark their own cyber readiness using our [cyber maturity model](#), sparks conversation, and contributes to even more informed cyber strategies.

Executive summary

83%

reported improvement
in cyber resilience.

Nobody ever said keeping SMEs (small-to-medium-sized enterprises) secure was an easy task. This crucial group powers 50% of the global economy, and those leading them handle a wide range of challenges, in many cases juggling responsibilities for everything from operations, sales, marketing, brand, technology, HR and more.

One of their most challenging roles is that of risk assessor, which requires them to understand the constant evolution of threats facing their businesses. The complexity of these threats continues to ramp up as technological advancements such as agentic artificial intelligence change the world around us.

In this ninth edition of Hiscox's annual Cyber Readiness Report, we look at the impact of these fast-changing digital risks, what they mean, and how small businesses can take action to mitigate their exposure.

Almost all SMEs (94%) are expecting to increase cyber security and data protection investments in the next 12 months, updating employee cyber training (70%) and hiring additional staff to increase cyber resilience (60%).

This year's report uncovers a determination among SMEs to not only invest in software and training, but to remain diligent with frequent risk assessments and vulnerability checks, in addition to keeping up with cyber insurance policies for when things go wrong.

Thanks to this proactive approach, organisations are showing increased confidence, with 83% reporting improved cyber resilience at their company in the past 12 months.

The complexity of digital risk continues to grow. Businesses are grappling with how to handle the after-effects of ransomware attacks, including regulatory changes such as a new law in Australia that requires companies to disclose the amounts of ransom demands paid. It's a rule that could be adopted in other countries too. A significant majority (71%) of firms believe those disclosures should be mandatory.

Despite this support, opinions vary over whether such requirements should apply to private companies. The majority (53%) believe private companies should not be obligated to disclose their finances publicly when it comes to ransomware payments.

While it's never been more challenging to be doing business when it comes to online threats – with 60% viewing AI driven social engineering and AI malware and phishing attacks as top emerging AI threats over the next five years – it's clear that cyber security experts and decision-makers are working tirelessly to protect their organisations, employees, and customers.

Over the past 12 months, 59% of SMEs have faced a cyber attack, but rather than standing still they are investing, training and updating systems to keep pace with the evolving landscape.

Key findings

59%

of respondents experienced a cyber attack in the last 12 months.



94%

are increasing investment in cyber security and data protection.



88%

conduct quarterly supplier and partner risk assessments.



27%

experienced a ransomware attack in the last 12 months.



33%

were fined a significant amount after a cyber incident.



60%

are recruiting additional staff to increase their cyber resilience.



91%

perform cyber vulnerability checks at least once a quarter.



71%

support mandatory disclosure of ransomware payments.



State of attacks

60%

paid a ransom and achieved full or partial data recovery.

Organisations that have dealt with a cyber attack in the past year didn't just grapple with one incident – they're likely to have been hit multiple times. Nearly three-out-of-five (59%) companies have experienced at least one cyber attack in the last 12 months.

Among organisations that suffered an attack, those that are larger or have higher revenue were more likely to experience a larger number of incidents. For example, companies with \$10 million or more in annual revenue and those with \$1 million but less than \$10 million in revenue that experienced an attack in the past year had more of them on average (about six) than those making less than \$1 million in revenue (about four).

Likewise, among companies that experienced an attack, businesses with 50-249 employees had an average of seven attacks in the past year compared to companies with 11-49 employees (an average of about five attacks), and those with one-to-ten employees (an average of four attacks).

Among firms that reported incidents, the average number of attacks ranged from about three in sectors like chemicals, property, and media to roughly eight in nonprofits. A successful cyber attack can inflict immediate and significant harm – disrupting operations, driving up costs, and exposing sensitive data.

Companies are seeing attackers take advantage of vulnerabilities in their own hardware and through partners they deal with. Internet of Things (IoT) devices owned by the companies themselves were the most common point of entry for cyber attacks in the last year (33%), followed by vulnerabilities in supply chains such as vendor websites (28%), as well as cloud-based corporate servers (27%). AI tools and software were the first point of entry for 15% of businesses.

No company enjoys rewarding bad players for hijacking their data, but when it comes to ransomware attacks, it is common for organisations to make every effort to recover what could be lost. That includes paying the ransom where that is demanded. For those who paid a ransom, 60% recovered some or all of their data. Two-out-of-five (41%) were given a recovery key, but still had to rebuild their systems.

Paying a ransom does not always solve the problem. Instead, for 31% who paid, attackers demanded more money. An additional attack was sustained by 27% of those who paid a ransom, though not necessarily an attack from the same entity.

State of attacks

Outcomes of attacks experienced by businesses in the past 12 months.

44%
Payment diversion fraud.

42%
Distributed denial of service.

42%
IT resource misuse.

State of attacks

continued

71%

majority of firms have some form of cyber insurance.

The after-effects of a cyber attack can be severe and long-lasting – sometimes threatening a company's survival. One third (33%) of affected firms incurred fines significant enough to damage their financial health, while many also reported lower business performance indicators (30%), higher costs to notify customers (29%), and greater difficulty attracting new clients (29%).

For those facing a fine, the landscape is complex. Businesses operating abroad can be subject not only to penalties at home, but in the country or region where they do business. A data breach may lead to fines for failing to protect the privacy of customers in markets such as California, Canada, the EU, or others where regulatory penalties could cost companies anywhere from thousands to millions.

Insurance is one tool companies are using to mitigate the effects of these attacks. The majority of firms (71%) surveyed have a cyber insurance policy or cyber insurance coverage as part of another policy.

Those at companies with ten or fewer employees are less likely (65%) to have cyber insurance than those with 11-49 employees (79%), or those with 50-249 employees (82%).

The impact of cyber attacks on people within the business is significant. Cyber incidents cause high stress for employees (39%) and can lead to burnout (32%) or an uptick in sick days (31%).

While the experience can create a sense of improved camaraderie (38%) and loyalty to the company (43%) – this only throws into sharper relief the need for companies to support their people during and after an attack.



This year's report reveals how artificial intelligence is truly transforming the cyber threat landscape. But beyond that, it highlights the dual role of this technology: on the one hand, while it is emerging as a strategic asset for strengthening a company's cyber resilience, it has also become a tool for cyber criminals, increasing the sophistication and complexity of cyber attacks.

Ana Silva

Head of PSC
Hiscox Iberia

Key cyber risks

The top three biggest risks for organisations.

37%
The inability to protect customer or internal data from breaches.

37%
Regulatory or legislative changes around cyber security and data.

36%
Any event where company data is potentially compromised.

“

The human impact of a cyber attack should never be underestimated. Employees face immense stress, which can lead to increased absence or even burnout. Supporting staff through the aftermath isn't just the right thing to do, it helps the business recover and builds greater resilience for the future.

Mike Maletsky
VP, Practice Leader
Technology and Cyber
Hiscox USA



Taking action

79%

investing in additional cyber security for remote employees.

Nearly all companies are allocating resources to prevent attacks, with 94% expecting to increase investment in cyber security and data protection in the next year. Portugal (45%) and Spain (40%) lead the countries where investment is expected to increase significantly.

More than half (54%) in the automotive industry globally plan to considerably increase their investment in cyber security and data protection. This is followed by government (49%), telecommunications (47%), and chemicals (45%).

Compliance also plays an important part, as 81% of companies are actively adapting to meet increasing cyber security regulatory requirements. Companies that experienced a cyber attack in the past year were more likely (87%) to report adapting to regulations than those who didn't experience an attack (72%).

Remote working represents another security challenge for businesses, with 79% having invested in additional cyber security training for remote workers to help prevent attacks.

Frequent security checks are another way companies are mitigating cyber threats. 91% conduct cyber vulnerability checks, such as simulations or penetration tests, at least once a quarter.

And companies are investigating beyond their own systems and staff when they consider where threats might originate. To that end, 88% of companies do risk assessments at least once a quarter to determine the cyber security risks of their suppliers and partners.

Experience drives action

Companies that were attacked in the past 12 months are more likely to invest in training than those that were not.

87%

investing in training and experienced a cyber attack.

68%

investing in training but did not experience a cyber attack.

Cyber resilience



Our [cyber maturity model](#) is a free-to-all tool that helps companies understand their cyber security strengths and weaknesses.

Companies believe that despite continued threats and consequences, they are making headway: the vast majority (83%) have improved their cyber resilience in the last 12 months. These improvements have been achieved by a combination of factors including ramping-up staffing for security positions, investing in software and increased cyber security training for employees.

Despite the confidence in their company's increased resilience, those tasked with cyber security are not resting on their laurels: they are keenly aware of new threats, many of them AI-driven, that will require even more vigilance and hard work.

“

Cyber risk is as much about people as it is about technology. We work with thousands of micro and nano businesses on their cyber protection and time and again the most important risk factor is the human factor. When you're building a business, you often have to juggle a lot of different roles – sales, HR, marketing, finance, tech – so getting support with the range of cyber risks your business faces – things like business email compromise, payment diversion fraud, and social engineering – is crucial. That's why, at Hiscox, we provide our customers with extensive prevention resources, training and phishing simulations to strengthen their resilience to everyday scammers and threat actors and free them up to focus on doing what they do best.

Diva Aoun
Head of Cyber
Hiscox Europe

Improving cyber resilience

Organisations are safeguarding against future threats.

70%
hiring additional staff members to boost their cyber resilience.

60%
updating the types of cyber security training for employees.

54%
investing in software to help identify and manage threats.

“

AI is a game-changing tool for businesses of all shapes and sizes, but it does increase an organisation's vulnerability to cyber-related risks if they don't have the right expertise or protection in place. Our professional liability and cyber insurance products protect against claims arising from the use of AI, including situations where a hack involves AI.

Nicolas Kaddeche

Technical Underwriting
and Direct Sales Director
Hiscox France



AI and future threats

49%

believe more decisive leadership is needed during an attack.

The rapid rise of integrated generative AI services creates new ways to fight threats, even as bad actors are using the technology to create new attacks.

Almost two-thirds (65%) of those responsible for their SME's security consider AI more of an asset than a vulnerability to their business. Portugal is especially likely to view AI as security support at 86%, while the USA and UK are less likely to feel this way at 58% and 59% respectively.

The top three emerging AI-driven threats in the next five years are social engineering attacks (60%), AI malware and phishing attacks (60%) and AI taking control of their company's data (60%).

For 22% of organisations, facilities (via a physical or proxy attack on utilities) and employees (via social engineering or phishing) are the most likely points of entry for breaches or ransomware attacks. Software and systems (20%) and third-party partners (20%) are also considered to be common entry points.

Companies can more effectively deal with cyber threats if employees are more aware of what those threats might be and what to do in the event of an attack.

Nearly all who have experienced an attack (96%) believe better awareness or understanding of cyber attacks and procedures is key to better response times for future breaches.

Improving the time it takes to assess an attack that has happened or is in progress and responding accordingly is essential to mitigating damage. Many who have experienced an attack believe being more aware of potential threats before they happen would help response times to improve (57%).

Having a better understanding of what to look for while it's happening (56%) is another way to speed up a response. In terms of what to do next, nearly half (49%) suggest a better understanding of who to report an attack to would help. Similarly, for 49%, response times could improve if leadership was more decisive when responding to an attack.

Planning for the AI threat

Organisations are taking action to protect themselves against evolving threats and plan to do the following over the next three years.

37%
ensure insurance policies include AI risks.

36%
train employees on AI threat awareness.

36%
perform regular AI usage audits.

33%
hire AI-savvy employees.

33%
employ AI security consultants.

Mandatory disclosures

71%

agree with the concept of disclosing ransom payment costs.

A first-of-its-kind law in Australia came into effect earlier this year, requiring all companies to disclose to government authorities, within 72 hours, the cost of any ransom payment made as part of a ransomware attack.

While most (71%) agreed with the concept of disclosing ransom payment costs, the pros and cons of this regulation continue to attract debate.

Owners, CIOs, CISOs and directors/VPs of IT were closely aligned in agreement (a range of 71% to 77%), but we found that directors/VPs of security were notably less likely to agree (50%).

Companies that have not experienced a cyber attack in the past year were more likely (85%) to agree that disclosures should be mandatory, than those who did experience an attack (61%).

54% of businesses say mandatory disclosures can help customers and stakeholders assess financial health, with 52% believing they aid authorities in tackling ransomware. The majority of firms in Portugal (52%) and Spain (52%) also view this as a way to remove the stigma of paying to secure data.

Yet concerns persist: 49% warn that mandatory disclosures could encourage attackers, and 53% say private firms should have no obligation to publicly disclose their finances.

While it seems likely that ransoms will continue to be paid, with varying results, the debate over payment disclosures – particularly for private companies – is likely to heat up, especially if new laws or regulations force the issue.



The introduction of mandatory reporting will inevitably be met with some resistance, but the need to dismantle the cyber criminal business model is universally recognised. As the UK moves ahead with bold measures aimed at tackling ransomware and bolstering national security, the need for small businesses to take ownership of their cyber security and keep investing in their people and defences remains.

Alana Muir
Head of Cyber
Hiscox UK

The disclosure debate

Reasons why companies should or should not be required to disclose ransom payments made in ransomware attacks.

Support for disclosure

54%

say disclosures give customers and stakeholders a clearer picture of a company's financial health.

52%

think increased transparency could help authorities respond to other ransomware incidents.

Opposition to disclosure

53%

feel private firms should not be obligated to reveal financial details.

49%

warn that disclosures could incentivise bad actors to engage in ransomware schemes.

Country comparisons



Cyber vulnerability

Ireland (42%) had the lowest rate of experiencing a cyber attack in the last 12 months. Germany (67%) and the UK (65%) were most likely to experience at least one attack.



Data recovery

For those who paid a ransom, the USA (74%) had the highest rate of data recovery after a ransomware attack, with Ireland (53%*) at the other end of the scale.



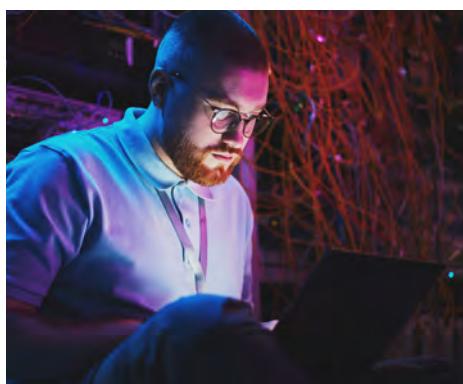
Regulation

Portugal (86%) and Ireland (85%) are more confident in their company's ability to adapt to new cyber security regulatory requirements compared to the USA (76%).



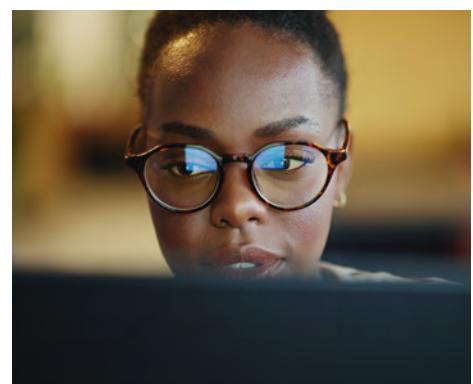
AI

Portugal (86%) is much more likely to view AI as a security asset rather than a vulnerability. The USA (58%) and the UK (59%) are less inclined to feel this way.



Mandatory disclosure

The USA (80%) has the strongest support for mandatory ransomware payment disclosure. Support is lower in Germany (65%), Portugal (65%) and Spain (62%).



Insurance

Cyber insurance coverage – either as a stand-alone policy or as part of another policy – varies by country, with the lowest take-up rate in France at 61%.



Cyber security tips for SMEs



Install a reputable software security package.

Probably one of the most effective ways to mitigate the latest cyber threats is to install security software on all your devices. These combine multiple tools and features that can help to automatically identify and block suspicious activity, then take proactive steps to remove the cause of the threat. The latest generation of security software is powered by AI and often combines crucial features such as antivirus, network firewall, password managers and data back-up to offer a holistic set of complementary controls to protect against threats such as ransomware.



Use a password manager and robust authentication.

Weak or reused passwords are prime targets for hackers seeking unauthorised access to business systems. A good password manager can help you to create complex passwords and store these securely. Many can now also monitor for password breaches and notify you of the need to make changes. When combined with the use of biometrics and multi factor authentication (MFA), they provide enhanced layers of security for your digital identities. Not only can a password manager help reduce cyber risks, but they are also more convenient for users and improve the overall digital experience.



Keep your systems and software up-to-date.

Outdated operating systems and applications often contain security vulnerabilities that cyber attackers can exploit. Develop a routine for regularly installing updates across all your company devices and software platforms. Consider enabling automated software updates for ease of security patching, as this can help ensure critical updates are applied quickly and only from the verified vendor. Not only are routine updates great for security; they will also help ensure your devices and software are working at peak performance with all the latest features.



Back-up company data securely and test those processes regularly.

Even with robust defences, there is always a risk of data loss or ransomware attacks. Frequent, secure back-ups – stored either offline or in the cloud – ensure that businesses can recover quickly if the worst happens. Today, data back-ups can often be automated through the use of software to ensure they are seamlessly captured and stored securely, but it is always worth testing your back-ups regularly to confirm that the data can be restored effectively and minimise costly downtime.



Be selective about who can access data.

Not every employee needs access to all company data. By restricting permissions so that individuals have access only to the information and systems necessary for their specific roles, you reduce the risk of internal threats and accidental data leaks. Regularly review and update these permissions, especially after role changes or staff departures, to maintain your security position. If you are using AI, then it is equally important to manage access permissions associated with AI agents and applications. If configured incorrectly, these can often highlight unintentional weaknesses in data access controls and lead to accidental data disclosure.

Hiscox

22 Bishopsgate
London EC2N 4BQ
United Kingdom

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