Cyber Readiness Report 2024

Protecting reputation through cyber resilience

Introduction

Eddie Lamb
Chief Information
and Security Officer
Hiscox Group

This year's edition of the Cyber Readiness Report explores the critical role of robust cyber resilience in mitigating evolving organisational risks and safeguarding reputations.

Despite perceptions that cyber security risks are declining, the reality is quite the opposite – attacks are growing in frequency and complexity, exposing significant gaps in business defences. As emerging technologies outpace traditional security measures, many firms are struggling to invest adequately in the right talent, tools and strategies to protect against these evolving threats.

Human error remains one of the greatest liabilities, particularly in the age of remote working. With employees often working from less secure environments, phishing scams, weak passwords and accidental data breaches are all too common.

To safeguard against these risks, organisations need to build a cyber-aware culture, recognising cyber defence as a collective responsibility rather than purely an executive or operational concern.

This means fostering an environment where cyber education is a continuous process, ensuring every member of the organisation understands their role in maintaining security. By promoting awareness and proactive behaviour across all levels, organisations can create a united front against cyber threats.

This is a key area of focus for Hiscox, not only in our own business but with our customers; through the Hiscox CyberClear Academy, we provide online cyber awareness training for policyholders and their teams. Since 2017, training has been provided to over 36,000 people from 7,000 organisations.

While cyber attacks continue to cause financial and operational setbacks, this year's report highlights a less tangible yet equally critical consequence: the damage to a company's reputation.

When sensitive data is compromised, customer trust erodes, business is lost and brand image suffers. Worse still, inadequate cyber security can deter potential partners and investors while attracting regulatory scrutiny. This can trigger a ripple effect that impacts revenue and growth.

In today's business environment, protecting your reputation is just as critical as safeguarding your physical assets – and that's where insurance plays a key role. As well as ensuring a swift recovery from breaches, comprehensive cyber insurance empowers businesses to innovate with confidence, knowing that they're not shouldering all the potential risks themselves. This makes insurance not only an important safety net but also a powerful enabler of business growth.

Executive summary

As technological advances outpace traditional security measures, companies lacking the right cyber security talent, tools and strategies risk falling behind. Building cyber resilience is essential for mitigating evolving threats, protecting reputations and supporting innovation.

Reputations at risk
The impact of cyber attacks on brand trust

Attacks on the rise
Over two-thirds (67%) of firms in this year's study report an increase in the number of times their organisation experienced a cyber attack in the past 12 months.

Reputations held to ransom
Of the organisations that have experienced a cyber attack in the past 12 months, 47% report greater difficulty in attracting new customers, and 43% report losing customers.

The human factor
44% of organisations that have experienced an increase in cyber attack risk over the past 12 months, and rate their risk exposure as high, identify a greater number of employees using their own devices for work as a contributing factor.

Disruptive tech
A double-edged sword for cyber security

The dangers of disruption
70% of firms have already integrated generative AI (GenAI) into their operations, with 56% believing it will significantly impact their cyber security risk profile.

Cyber security vulnerabilities
A third of firms (34%) say their organisation's cyber security measures are compromised due to a lack of expertise in managing emerging tech risks.

Turning risk into opportunity
Businesses should see technological innovation and cyber security as complementary rather than conflicting forces; 64% of leaders believe GenAI will be pivotal in shaping their cyber security approach by 2030.

Cyber resilience
A pillar of long-term business success

Exposed to cyber risks
A third of business leaders (34%) do not feel that their organisation is adequately prepared to handle cyber attacks.

Investing in cyber resilience
On average, firms spent 11% of their IT budget on cyber security in 2023, with smaller firms dedicating a larger proportion of their budget to this area.

Expanding employee awareness
Two-thirds of leaders (65%) say their organisation has invested in additional cyber security training for remote employees to mitigate the risk of cyber attacks.

Innovation anchored in security
When considering the main drivers behind their firm's cyber risk management plan, a quarter of leaders (26%) identify the role of cyber risk management in supporting innovation.

Reputations at risk
The impact of cyber attacks on brand trust

In an era of rapidly evolving technology, cyber security remains firmly on the radar for business leaders. While exposure to a cyber attack ranked as leaders' top perceived risk to their organisations in 2022 and 2023, this year's research sees it drop to third place. However, in today's business landscape, marked by intense competition for talent and economic instability, cyber risk still ranks above economic issues and skills shortages.

Attacks on the rise

Over two-thirds (67%) of firms in this year's study report an increase in the number of times their organisation experienced a cyber attack in the past 12 months. On average, the number of cyber attacks experienced per organisation increased from 63 in 2022/23 to 66 in 2023/24.

Many businesses are not financially prepared for these attacks, with over a quarter of business leaders (26%) saying their organisation does not have sufficient resources to effectively manage the financial risk associated with a cyber security threat.

The most common outcome of cyber attacks experienced by organisations in the past 12 months was financial loss due to payment diversion fraud – experienced by 58% of organisations, up from 34% the previous year.

Businesses are increasingly aware of the threat posed by cyber attacks, demonstrated by the growing adoption of cyber insurance policies. This year's report reveals a rising number of firms with cyber insurance coverage, either as a stand-alone policy or as part of another policy, with uptake increasing in line with the size of the organisation.

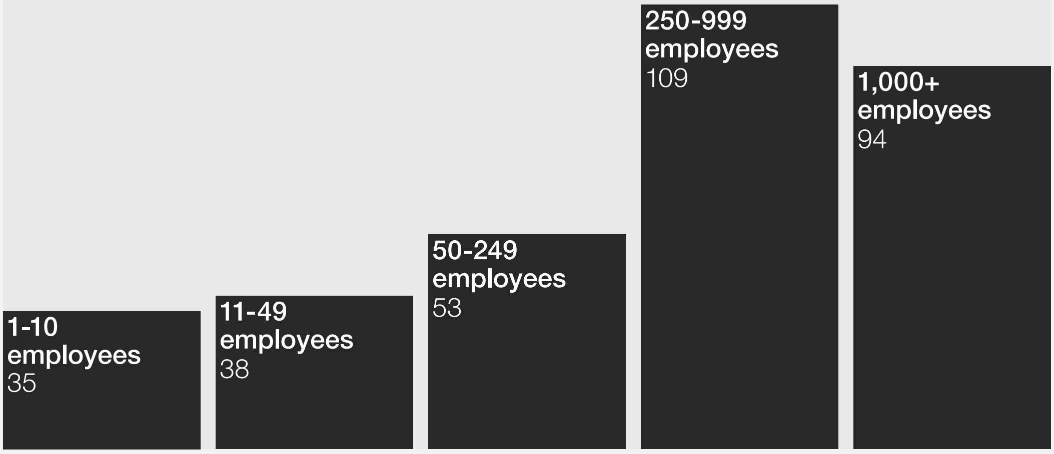
"Cyber attacks can vary widely from phishing emails and Denial of Service attacks to critical infrastructure hijacking. This broad spectrum of threat underscores the need for organisations to implement cyber security measures and insurance tailored to their specific risk profiles."

Diva Aoun
Head of Cyber, Hiscox Europe

Top five perceived business risks

	2024 %	2023 %	2022 %
Fraud and white-collar crime	**40**	32	38
Pandemic or infectious diseases	**37**	33	42
Exposure to a cyber attack	**35**	40	45
Losses due to economic issues	**35**	38	40
Skills shortages	**32**	35	40

Average number of cyber attacks in the past 12 months



Reputations at risk
continued

61%

Organisations that believe reputational damage from a cyber attack would significantly damage their business.

Reputations held to ransom
While the direct financial implications of cyber attacks are a significant concern, business leaders are increasingly focused on the potential impact of a breach on their brand reputation.

Six-in-10 (61%) believe that reputational damage from a cyber attack would significantly damage their business, and 64% believe they risk losing business if they do not handle client and partner data securely.

This year's research reveals that concerns of reputational damage, caused by the loss of sensitive information, is a driving force behind responses to ransomware attacks. Over the past 12 months, the top three reasons organisations paid ransom were: to protect their customer data, to protect their reputation, and to recover their data because they did not have any back-ups.

However, paying a ransom demand does not guarantee data recovery. In fact, only 18% of victims were able to fully recover their data after paying a ransom.

Organisations need to adopt a proactive approach to mitigate risk. Three-in-10 firms (31%) identify a desire to avoid the reputational damage that may be caused by a cyber attack as one of the main drivers behind their cyber risk management plan.

"As businesses learn to combat ransomware attacks, hackers are evolving their tactics. The threat has shifted from operational disruption to data extortion, with hackers targeting highly sensitive information to discredit organisations. Who are they doing business with? And do their actions align with their public values? Hackers are holding reputations to ransom – and no business is too small to be at risk."

Alana Muir
Head of Cyber, Hiscox UK

Impacts of cyber attacks in the past 12 months

	2024 %	2023 %
Greater difficulty attracting new customers	**47**	20
Lost customers	**43**	21
Bad publicity, which impacted brand reputation	**38**	25
Lost business partners	**21**	16

Reputations at risk
continued

The human factor

Business email compromise remains the most common point of entry for cyber attacks for the second year in a row, followed by corporate servers in the cloud (climbing from third place the previous year). Meanwhile, employees have risen from the fourth to the third most common point of entry in the last year. This shift highlights the ongoing challenges in defending against increasingly sophisticated social engineering techniques, such as spoofing and phishing.

44% of organisations that have experienced an increase in cyber attack risk over the past 12 months, and rate their risk exposure as high, identify a greater number of employees using their own devices for work as a contributing factor.

The use of personal devices for work, known as bring your own device (BYOD), introduces significant cyber security risks for organisations. Unlike company-issued devices, personal devices may lack up-to-date security software, making them more vulnerable to malware, phishing attacks and data breaches.

Furthermore, without centralised control, organisations have limited visibility into the apps that employees may be using, as well as how and where data is being accessed, stored and shared. This lack of oversight increases the likelihood of unauthorised access and data leaks.

Most common points of entry for cyber attacks in the past 12 months (%)

Focus on the UK

Attacks rise
Seven out of ten business leaders surveyed in the UK say their organisation has seen an increase in the number of times it has experienced a cyber attack in the past 12 months.

Insider threats
When considering their organisation's exposure to cyber threats, 42% believe insider threats (caused by employees, contractors or business partners) pose a significant risk to their organisation.

Among the UK organisations that have experienced an increase in cyber attack risk over the past 12 months, and rate their risk exposure as high, a greater number of employees working remotely is the most commonly identified factor.

Reputation management
Over a third of UK business leaders (35%) identify a desire to avoid the reputational damage that may be caused by cyber attacks as one the main drivers behind their firm's cyber risk management plan – the highest of all the markets surveyed.

Disruptive tech

A double-edged sword for cyber security

56%

Leaders that believe GenAI will have a significant impact on their cyber security risk profile.

The corporate technology landscape is evolving at remarkable speed, with two-thirds (67%) of business leaders stating that investing in cutting-edge technology is a top priority for their firm. But, while companies are racing to adopt these transformative tools, many are underestimating the cyber security risks that come with them.

As IT systems become more complex and interconnected, companies' attack surfaces are expanding, increasing their vulnerability to cyber threats. Despite this, one in four business leaders do not believe emerging technologies present significant new risks to their organisations.

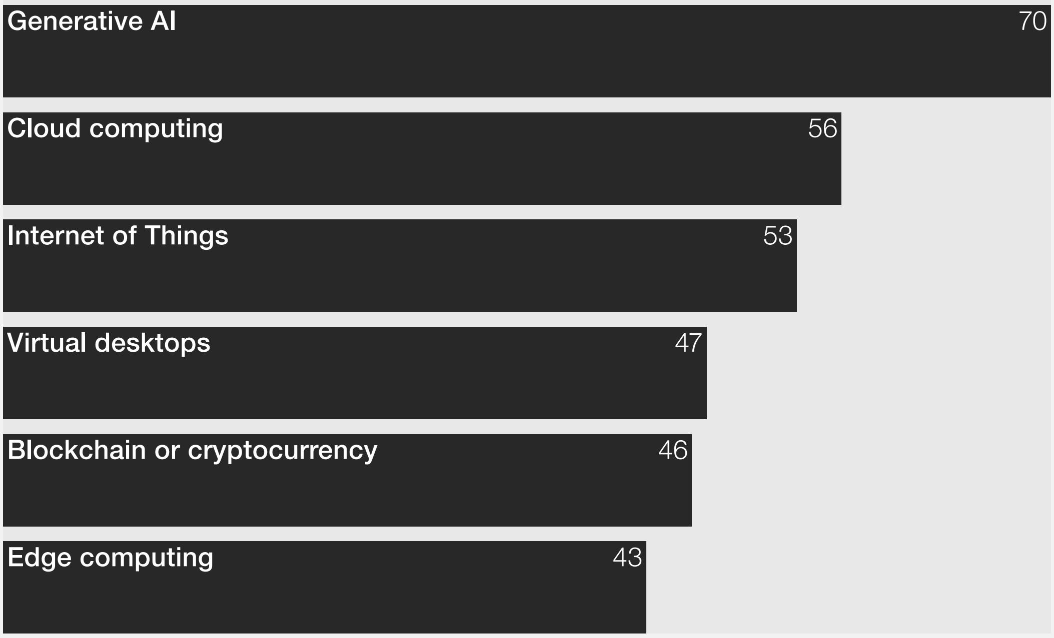
The dangers of disruption

The majority of organisations are already using disruptive technologies such as artificial intelligence (AI), the Internet of Things (IoT) and cloud computing. This wave of innovation has been largely driven by the promise of enhanced efficiency, increased competitive advantage and sustainable business growth.

However, where tech adoption and innovation outpace cyber security measures, this can create vulnerabilities. A key example is the widespread adoption of GenAI: a subset of AI that can create new content (text, images and video) by learning patterns from existing data.

Seven-in-ten organisations surveyed have already integrated GenAI into their operations. At the same time, over half (56%) of leaders believe this technology will have a significant impact on their cyber security risk profile.

Organisations using disruptive technologies (%)



Sustainable and secure: the new tech mandate

Green tech
Organisations are increasingly adopting disruptive technologies as part of their sustainability strategies. Over a third (35%) are currently using green tech as part of their regular operations, and smart buildings are also on the rise – currently being used by 34% of organisations.

Vulnerabilities
Green tech often involves the use of interconnected systems and IoT devices, which can enhance efficiency and reduce environmental impact. However, these networks are only as secure as their most poorly protected device: any vulnerability can be a target (or potential point of entry) for hackers.

Aligning strategies
To safeguard these technologies, it will be important for organisations to align their sustainability and cyber security strategies. This dual focus not only protects the organisation, but also ensures the long-term viability of sustainability initiatives.

52%

Organisations that report a critical shortage of skilled cyber security professionals.

Cyber security vulnerabilities

While emerging technologies can drive efficiencies in managing vast amounts of data, this also makes them prime targets for cyber attacks.

Hackers are also beginning to leverage advanced technologies to launch more sophisticated attacks. For example, large language models (LLMs) can be used to craft convincing phishing emails, imitating style and tone to make attacks more effective and harder to detect.

Security strategies need to adapt but, currently, many businesses feel underprepared. A third of firms (32%) say they are falling behind in adopting necessary cyber security technologies.

The cyber skills gap remains a key problem for organisations. Over half of firms (52%) report a critical shortage of skilled cyber security professionals, and a third (34%) admit that their cyber security measures are compromised due to a lack of expertise in managing emerging technology risks.

Turning risk into opportunity

While advanced technologies may bring increased cyber risk, they can also be leveraged as powerful tools to strengthen organisations' defences. SOAR (security orchestration, automation and response) technologies enhance an organisation's ability to detect, respond to and mitigate security threats.

By bringing together various security tools, data sources and processes into a unified system, SOAR platforms allow cyber security teams to automate complex security processes and reduce incident response times.

Almost two-thirds (64%) of business leaders surveyed believe that GenAI will be pivotal in shaping their cyber security approach by 2030. GenAI systems can swiftly create detailed reports on threat levels and vulnerabilities, empowering organisations to make smarter decisions about their cyber security investments and strategies.

Following an incident, these tools can support in reconstructing the attack to aid investigations and suggest preventive measures to mitigate future breaches. GenAI can also assist in developing stronger security protocols, from enhanced encryption keys to tighter access controls.

Businesses should see technological innovation and cyber security as complementary rather than conflicting forces. By advancing both in tandem, they can foster a secure environment for growth and development.

Focus on the USA

Prioritising cyber security
The US business leaders surveyed report that cyber security is high on the board agenda: 72% believe that cyber resilience is either very or extremely important to their organisation's overall business strategy, and 76% have a dedicated executive or leader who is responsible for cyber security.

Legacy tech
The research also reveals that legacy technology is a key barrier to building cyber resilience. Among the US organisations that have seen an increase in cyber attack risk over the past 12 months, and that rate their risk exposure as high, legacy tech not being decommissioned or being unable to receive security updates is the most commonly identified contributing factor.

Investment needed
In 2023, US firms spent an average of 8% of their annual revenue on their overall IT budget, and 10% of their IT budget on cyber security. Increased investment in updating legacy tech and recruiting skilled cyber security talent will be crucial to mitigating risk and minimising potential financial and reputational damage.

> "As the use of autonomous systems grows, so does the threat, and potential impact, of cyber-attacks. In prior years, technology has been used to mitigate the security compromising effects of human error. With autonomous systems, and particularly the introduction of AI, we start to see the tables turn. Human checkpoints are vital with these systems to ensure the logic is sound, that it is processing information correctly and the outputs are as intended."
>
> **Mike Maletsky**
> Practice Lead for Technology and Cyber, Hiscox USA

Cyber resilience
A pillar of long-term business success

Organisations are grappling with a wide range of risks beyond cyber threats, such as the emergence of new competitors, regulatory or legislative changes, and geopolitical conflicts.

Therefore, organisations need a comprehensive cyber resilience approach that not only protects against current threats but also adapts to the changing landscape of broader organisational risks.

Exposed to cyber risks
Three-quarters of firms included in the study say cyber resilience is very important to their overall business strategy, with 44% saying it is extremely important.

However, while 53% of firms say their cyber resilience has improved in the past 12 months, 40% still classify the maturity of their cyber resilience as either 'basic' or 'ad hoc', lacking formal processes and with limited training and awareness.

A third of leaders (34%) do not feel their organisation is adequately prepared to handle cyber attacks.

When considering their organisations' top priorities for improving cyber resilience over the next 12 months, leaders identify the importance of updating existing security technologies (36%), improving employee awareness (32%) and enhancing threat detection capabilities (31%)

The organisations that dedicate sufficient time and resources to strengthening their cyber security defences will see significant long-term benefits.

By minimising the risk of data breaches and facilitating quicker incident recovery, they will not only reduce financial losses but protect and enhance their reputation, paving the way for sustained business growth and stability.

Cyber resilience maturity
Organisations' self-assessment of their cyber resilience maturity

%	
10	**Basic** — Basic awareness of cyber resilience. — Minimal formal processes. — Ad hoc responses to cyber incidents.
30	**Ad hoc** — Some formal processes in place. — Implementation is inconsistent and often reactive. — Training and awareness programs are limited.
34	**Established** — Established and documented processes with regular reviews and updates. — Moderate level of employee training and awareness. — Periodically tested incident response plans.
20	**Advanced** — Integrated processes across the organisation with performance metrics. — Continuous improvement practices in place. — High level of employee training and proactive incident response.
6	**Leading** — Best-in-class practices fully integrated into the business strategy. — Continuous innovation and improvement in cyber resilience. — Strong collaboration with external partners and stakeholders.

Cyber resilience
continued

11%

Average proportion of IT budget spent on cyber security by organisations.

Investing in cyber resilience
By 2030, two-thirds of firms plan to implement zero trust architecture (ZTA), ensuring that no one inside or outside the network can access sensitive data without strict verification.

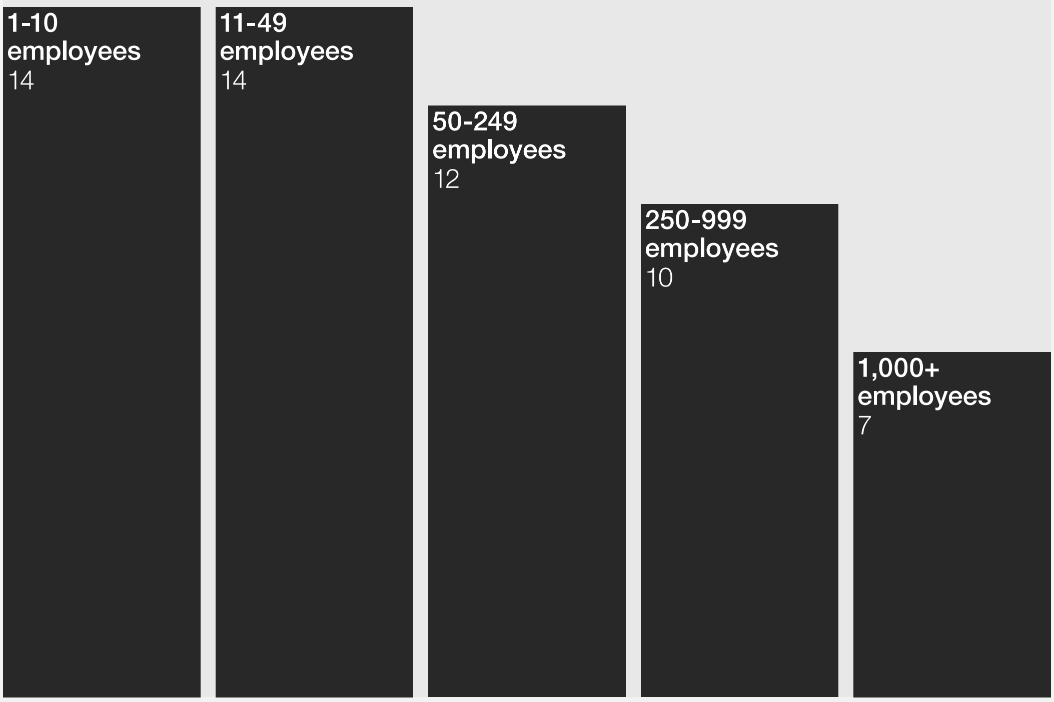
This approach will hugely strengthen security, but implementing it will require significant investment in technology upgrades, network infrastructure changes, security team upskilling and ongoing management.

In 2023, 81% of firms spent up to 10% of their annual revenue on their overall IT budget (including all IT investments and services), with no firms spending more than 20% of their annual revenue on their IT budgets. On average, firms spent 11% of their IT budgets on cyber security.

Smaller firms continue to allocate a larger proportion of their budget to both IT in general and cyber security specifically.

Three-quarters of companies with 1-10 employees and 73% of companies with 11-49 employees spent 11-20% of their annual IT budget on cyber security. Meanwhile, 99% of firms with more than 1,000 employees spent a maximum of 10%.

Proportion of IT budget spent on cyber security (%)



Expanding employee awareness

46% of the organisations that have faced a cyber attack in the past 12 months report that, in at least one of the attacks, an employee was the first point of entry (e.g. via a form of social engineering).

While organisations can implement new security policies and procedures, these will have a limited impact unless employees at all levels of the organisation have an understanding of why this is important and the implications of an attack.

In the 'new normal' of hybrid working, a significant proportion of employees still work remotely at least some of the time. Employees working away from the office may miss guidance on cyber security process updates and best practices, and without regular monitoring, mistakes or breaches may go unnoticed for longer.

Two-thirds of leaders (65%) say their firm has invested in additional cyber security training for remote employees to mitigate the risk of cyber attacks. This proactive approach is essential to safeguard both employee data and sensitive company information.

Executive sponsorship is also key. Currently, 72% of firms have a dedicated leader or executive who is responsible for cyber security. This rises to 97% of companies with over 1,000 employees, compared to 55% of companies with 1-10 employees. By leading from the front and actively engaging in strategic decision making, leaders can create a culture of cyber security awareness and accountability.

> "Innovation and technological development don't come without risk. To navigate these risks, organisations must adopt a resilient cyber security approach that combines robust systems, informed and proactive employees and comprehensive insurance. This integrated approach will empower businesses to confidently tackle the ever-changing threat landscape and take innovative leaps."
>
> **Gisa Kimmerle,**
> Cyber Product Head, Hiscox Germany

Innovation anchored in security

Businesses are increasingly recognising the link between cyber security and innovation. When considering the main drivers behind their organisation's cyber risk management plan, a quarter of business leaders (26%) identify the role of cyber risk management in supporting innovation. By embedding cyber security into their innovation strategies, organisations can create an environment that supports experimentation while protecting intellectual property – and investment – and ensuring regulatory compliance.

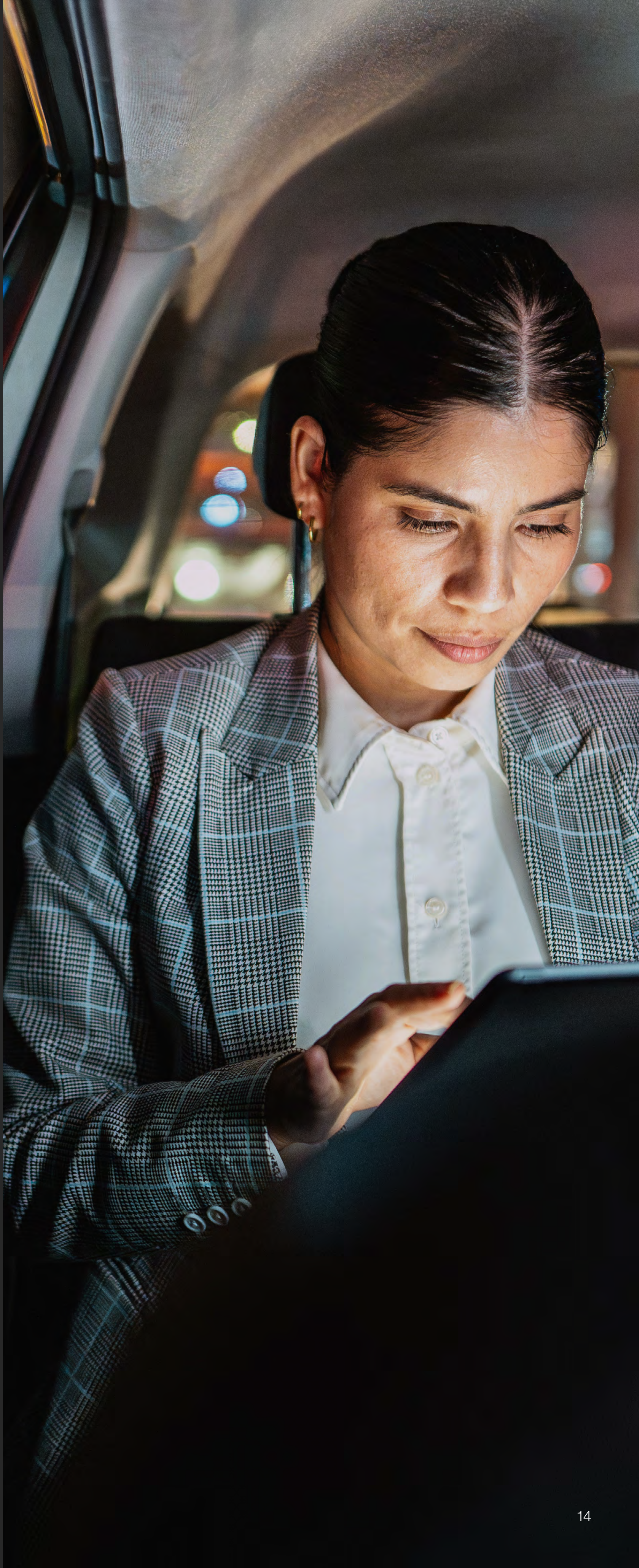
Those organisations that strike the right balance between security and innovation will stay ahead of evolving cyber threats, fortify their defences, and position themselves for business success.

Focus on Belgium

Increased risk
Almost three-quarters (73%) of Belgian business leaders surveyed say economic instability has increased their risk of cyber attacks. However, 72% say cyber security is critical to their ability to compete in their market or industry.

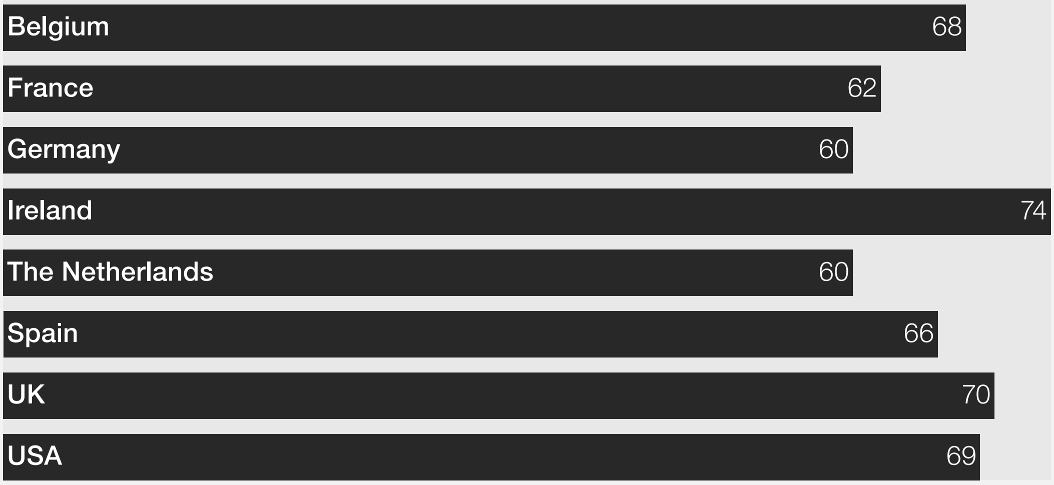
Reputational concerns
Leaders are particularly concerned about the risk of ransomware causing reputational damage, with 38% considering this a significant risk to their organisation.

Cyber maturity
38% of Belgian organisations classify their cyber resilience maturity as either ‘basic’ or ‘ad hoc’. With 57% of firms saying they face a critical shortage of skilled cyber security professionals, attracting top talent will be crucial for progress.

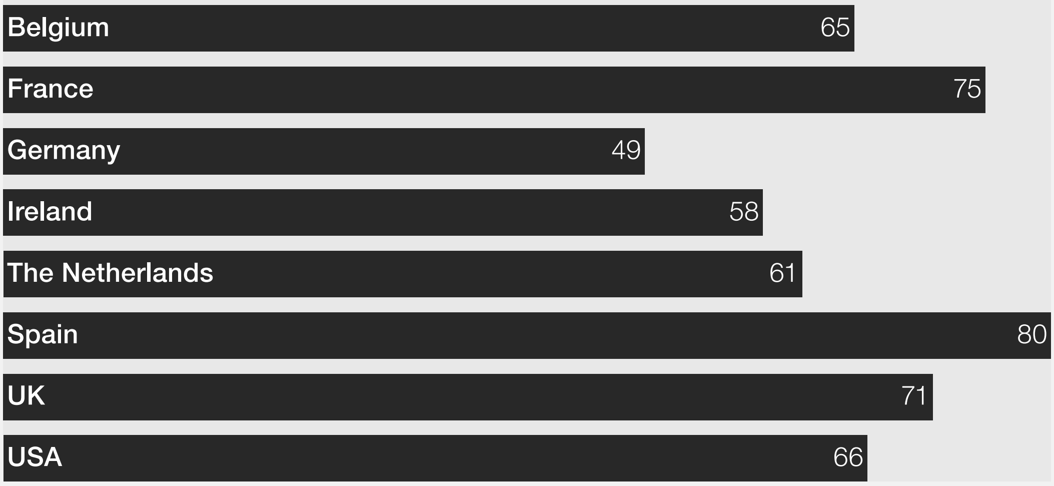


Country comparisons

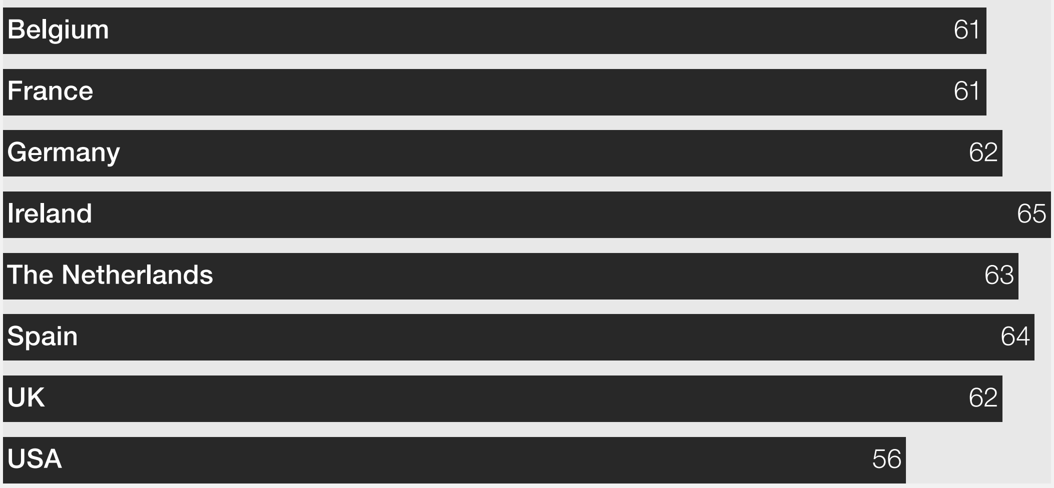
Organisations that have experienced an increase in cyber attacks in the past 12 months (%)



Average number of cyber attacks per organisation in the past 12 months



Leaders who believe reputational damage from a cyber attack would significantly damage their business (%)



Methodology

Hiscox, in partnership with Man Bites Dog, conducted an opinion research study among 2,150 professionals responsible for their organisations' cyber security strategies. This included 400 interviewees from the USA and 250 from each of the following countries: the UK, the Republic of Ireland, France, Germany, Spain, Belgium and The Netherlands. Interviews were conducted between 12 August and 2 September 2024.

This report includes comparisons to previous years' studies, mainly the 2023 Cyber Readiness Report. The 2023 sample of 5,005 professionals included over 900 each from the USA, the UK, France and Germany; over 400 from Spain; and 200-plus from Belgium, the Netherlands and the Republic of Ireland.

The 2024 Cyber Readiness Report is based on a more specialised research sample consisting of business leaders and IT decision-makers. Respondents also included a greater proportion of large organisations (1,000-plus employees) than in previous years. The full makeup of respondents is detailed below.

Job title (%)

	2024	2023
Business leaders (net)	**56**	**100**
Director	16	32
C-level Executive	15	29
Vice President (in charge of one or several large departments)	13	24
Manager (manages a team of functional practitioners)	12	15
IT decision-makers (net)	**44**	**–**
Chief Information Officer	12	–
Chief Technology Officer	10	–
Senior IT Leader	9	–
Chief Information Security Officer	7	–
Chief AI Officer	6	–

Number of employees in organisation (%)

	2024	2023
1	4	9
2-5	10	11
6-10	12	8
11-20	9	8
21-49	10	9
50-99	8	6
100-249	7	9
250-499	7	7
500-999	8	8
1,000-4,999	13	12
5,000-19,999	9	8
20,000+	3	5

Department (%)

	2024	2023
IT and technology	9	18
Finance	9	9
Operations	8	10
Board or executive management	8	9
Marketing and communications	8	5
Sales	7	5
General counsel or legal	7	4
Product management	7	5
Cyber security management	7	–
eCommerce	7	4
Risk management	7	5
Human resources	6	7
Procurement	6	4
Owner	5	14

Sector (%)

	2024	2023
Technology	9	10
Financial services	9	10
Retail and wholesale	7	8
Healthcare	7	6
Manufacturing	7	8
Construction	6	8
Food and drink	6	4
Professional services	6	8
Energy	6	4
Telecommunications	5	4
Business services	5	7
Transport and distribution	5	5
Pharmaceutical	5	3
Media	5	3
Property	4	3
Travel and leisure	4	4
Government	2	3
Non-profit	2	2

Hiscox and cyber

When it comes to cyber insurance, Hiscox delivers expertise
We have over 20 years' experience in privacy and cyber insurance, and in that time have underwritten hundreds of thousands of policies and managed thousands of claims worldwide. Understanding the cyber risks and challenges businesses face is paramount to our success. In 2017, Hiscox built a global, central cyber team to provide product consistency, coordinated insight and collaborative services.

Our new generation insurance product includes a suite of tools and services
Beyond the classic risk transfer, Hiscox cyber insurance offers direct support from real experts, including crisis managers, IT specialists, data protection lawyers and PR consultants. Since 2018, Hiscox has offered free employee training to all our small- and mid-sized insureds around the globe, partnering with various expert providers.

Sharing our expertise and building awareness
We have developed free-to-all tools to help companies understand their cyber security strengths and weaknesses. Using the Hiscox cyber maturity model, firms can compare their performance to over 16,000 other businesses.

Keeping you informed about the cyber security landscape
For the eighth year running, we've produced the Hiscox Cyber Readiness Report. Each year, this report provides a picture of the cyber readiness of businesses, and offers a blueprint for best practice in the fight to counter an ever-evolving threat. Drawn from a representative sample of companies across eight countries by size and sector, it reflects the direct experience of those on the front line of the business battle against cyber crime.

Hiscox
22 Bishopsgate
London EC2N 4BQ
United Kingdom

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

22891 10/24