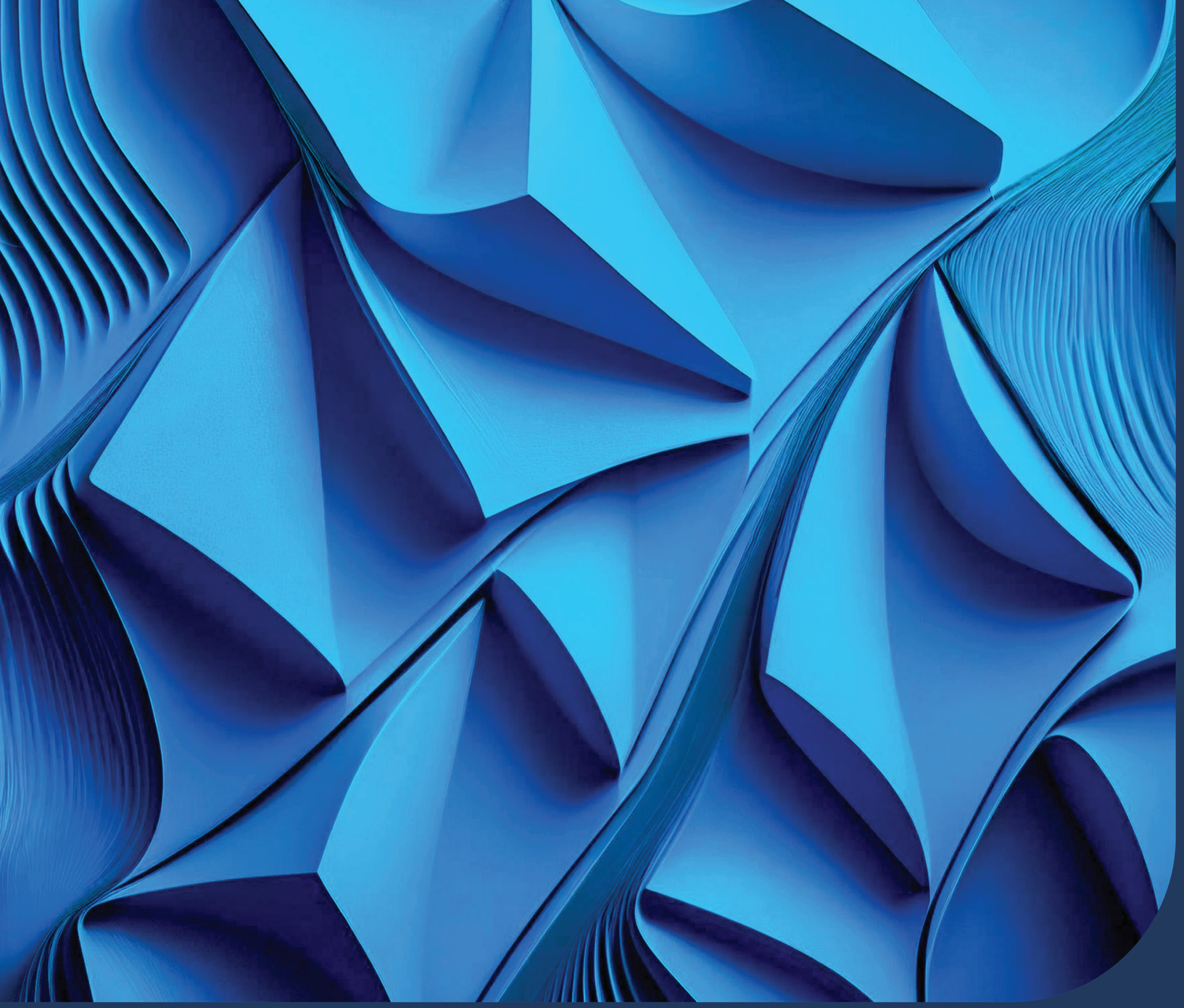


Microsoft Security

Cybersecurity trends **in Ireland 2023**

A report by Microsoft Ireland exploring C-suite perspectives on cybersecurity threats and resilience in Ireland.

Based on research conducted by

amárach research

Contents

Introduction

Kieran McCorry, National Technology Officer, Microsoft Ireland

Cybercrime is ever-changing and omnipresent. Every day, Irish organisations are susceptible and vulnerable to attack, as is evidenced by this latest research exploring C-suite perspectives and experiences of cybersecurity threats faced by organisations in Ireland. This study highlights that many organisations are being compromised by the lack of comprehensive cyber defence strategies and processes that are lived and owned by all decision-makers.

While it is positive to see that organisations are adopting training and cyber defence skills, true resilience requires continuous evolution and investment in multi-layered strategic processes, including risk assessments and business continuity planning. New EU laws, such as the Network and Information Security 2 Directive (NIS2 – see more information on p20), have been introduced to fast-track cyber defences across all markets and it is imperative that Irish organisations are aware of, and investing in, the right infrastructure to ensure compliance with this new cybersecurity regulation.

"Globally we are seeing bad actors execute more sophisticated attack strategies and using very effective 'living off the land' techniques to evade detection."

Globally we are seeing bad actors execute more sophisticated attack strategies and using very effective 'living off the land' techniques to evade detection[1]. Equally, it is clear from this report that Irish executives are increasingly concerned about the changing cyber threat landscape. Organisations must accelerate the move to the cloud, where security innovations will have the most impact. This will ensure AI innovation provides defenders with a durable technological advantage over attackers.

Public-private collaboration should be another key focus for organisations so that we are bringing to bear the best technological and regulatory tools to combat cyber aggression, for all sectors and operating environments. We need deeper alliances in the private sector and stronger partnerships between the private and public sectors. In Ireland we see impactful collaborations with the National Cyber Security Centre (NCSC), industry, and academia that provide a robust ecosystem that can be built upon and leveraged in the future.

What is clear from this study is that executives in Ireland must begin to explore more strategic methods for cyber defence and resilience through which new technologies, such as AI, can be used to embed intelligent threat prediction and prevention, and to bolster incident recovery plans.

Additionally, the processes, behaviours, and cultural attitudes in relation to cyber security are often just as important as the technological defences deployed to successfully prevent and manage attacks.

[1] Microsoft Digital Defense Report 2023

Executive summary

Microsoft Ireland commissioned Amárach Research to survey decision makers in Ireland on cybersecurity trends, including cybersecurity incidents, financial losses, cyber threats, and regulations. The sample size included 200 C-suite leaders, with a representative split in terms of the size of the organisations, spanning all sectors across Ireland, both private and public sector.

Cybersecurity trends

According to the survey, 46% of respondents have experienced one or more cyber incidents in the last three years, and 30% have experienced a data breach. Despite this, only 14% of respondents have had to report one or more cyber incidents to the NCSC or the Data Protection Commissioner in the last three years. Reassuringly, the majority of respondents (74%) have not reduced their spend on cybersecurity in the last three years, and 57% have regular cybersecurity training within their organisation.

Financial loss

Cyber crime has increased exponentially globally in recent years and organisations in Ireland, both in the public and private sector, have experienced attacks causing millions of Euros worth of loss. We can see from our research that organisations in Ireland continue to experience the impact of cyberattacks with 20% of respondents admitting they have suffered a financial loss due to a cyber incident.

Threat landscape and strategic defences

When asked about the biggest cybersecurity threat to their organisation, 38% of respondents selected work email compromise (e.g., phishing, social engineering), followed by increased sophistication of attacks and ransomware (both at 14%). When looking at strategic cyber defence, under half of organisations (44%) have regular risk assessments to identify vulnerabilities in systems and networks, and just 38% have a multi-layered IT strategy with prevention, detection, response, and recovery. Additionally, looking to the future, more than a quarter of organisations (26%) have indicated they won't be investing in their IT security infrastructure in the coming year, despite an increasingly evolving threat landscape.

Artificial intelligence
Only 14% of respondents use AI-enabled technologies within their IT security strategy, while 30% of leaders are unsure if they are in fact using AI technologies for cyber defence. The common purposes of AI within their security posture being cyber intelligence and threat exposure, and cyber incident reporting and explainability (both at 44%).

Regulation and legislation compliance
25% of respondents are aware of the NIS2 Directive and whether or not they are required to be compliant and 20% are currently compliant with the requirements. Only 27% of respondents are aware of the Digital Operational Resilience EU Act (DORA) and how it relates to their business. When asked about risk and information security management systems, the most common systems in place are risk management and information system security policies (41%), incident handling and management (38%), and business continuity and crisis management (36%).

In summary, the findings reveal that the majority of Irish organisations have encountered cyber incidents, some resulting in financial losses, which is consistent with global trends. While it is reassuring that organisations have continued to invest in cybersecurity and in training their people, we also see that there is more work to be done to raise awareness of the upcoming NIS2 Directive, which will impact so many sectors in 2024. More worryingly, there seems to be complacency setting in, with many claiming to have no plan to invest in cybersecurity in the coming year. With increases in cyberattacks, that have greater sophistication and intensity, leaders cannot be complacent. For example, in just two years, the number of password attacks detected by Microsoft has risen from 579 per second to more than 4,000 per second[1]. It is vital that organisations in Ireland prioritise protection rather than managing their security reactively when an attack hits. Leaders can use new technologies, such as AI to provide end-to-end security, while also weaving security into the fabric of everything they do, with a collective responsibility across all roles within the organisation.

"The biggest perceived cybersecurity threat is work email compromise, followed by increased sophistication of attacks."

Footnote 1: Microsoft Digital Defense Report 2023

Key findings at a glance:

46%
of respondents have experienced one or more cyber incidents in the last three years.

30%
have experienced a data breach.

74%
have not reduced their spend on cybersecurity in the last three years.

57%
have regular cybersecurity training.

14%
have had to report one or more cyber incidents to the NCSC or the Data Protection Commissioner in the last three years.

20%
have suffered a financial loss due to a cyber incident.

38%
selected work email compromise (e.g., phishing, social engineering) as the biggest cybersecurity threat to their organisation.

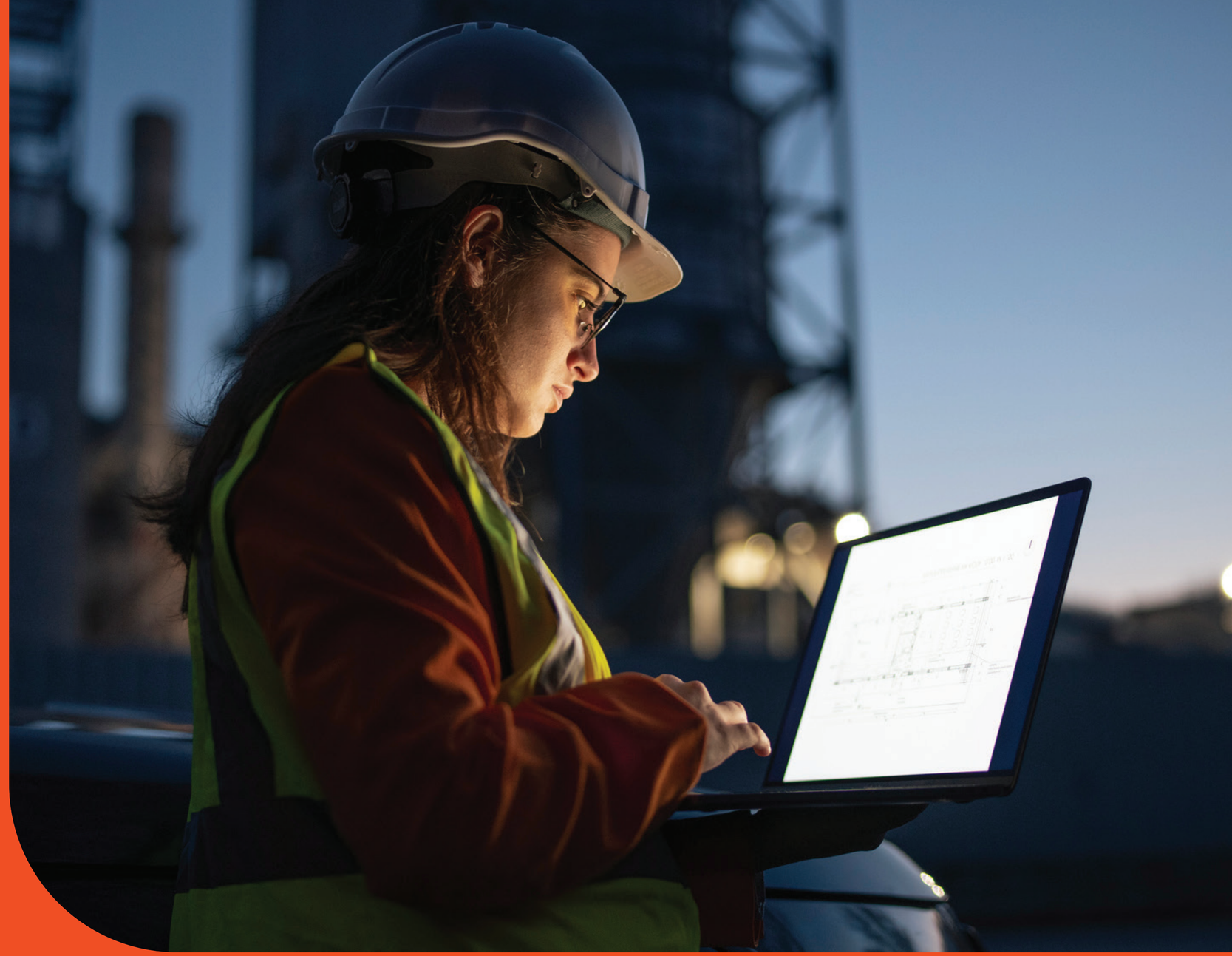
56%
don't have regular risk assessments to identify vulnerabilities in systems and networks.

62%
don't have a multi-layered IT strategy with prevention, detection, response, and recovery.

14%
use AI-enabled technologies within their IT security strategy.

More than
70%
of Irish executives are either unaware or unprepared to be compliant with the NIS2 Directive.

1. Cyber threat landscape in Ireland



Cybercrime is extensive across Irish industries – this is compounded by the lack of comprehensive cyber defence strategies evident within organisations. While organisations are adopting training and embedding cyber defence skills, true resilience requires continuous evolution and investment in technological solutions, and a culture of strict IT governance processes.

According to the survey, 46% of respondents experienced one or more cyber incidents in the last three years, and 30% experienced a data breach. Which makes it surprising that only 14% of respondents reported one or more cyber incidents to the NCSC or the Data Protection Commission (DPC) in the last three years.

We can see that cybersecurity remains a priority, with the majority of respondents (74%) saying they have not reduced their spend on cybersecurity, and 57% providing regular cybersecurity training within their business.

The result of cybercrime can create havoc on an organisation, both reputationally and financially, as is highlighted in this report where a number of organisations admitted to experiencing financial loss.

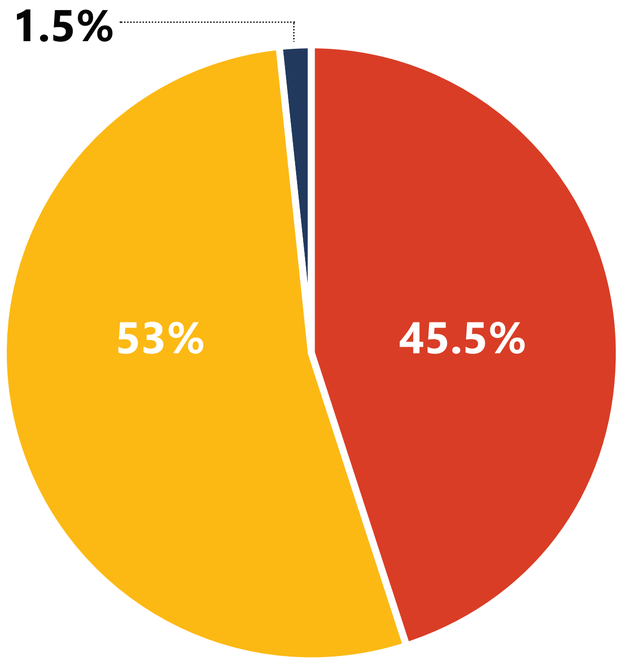
Work email compromise is seen as the number one biggest threat by Irish executives (38%), with increasingly sophisticated attacks coming in as the second greatest cybersecurity fear (14%). Positively, according to the research, organisations are taking steps to manage cybersecurity – they have maintained their spend on IT security protections in the last three years (74%) and 57% of leaders feel they have strong cybersecurity resilience and regular training in their business.

That said, the study indicates that the necessary strategic processes for cyber defences are not in place in over half of organisations. For example, only 44% of organisation have risk assessments to identify vulnerabilities, only 38% have a multi-layered strategy that includes prevention, detection, response and recovery, and just 31% have a practiced IT business continuity plan in place with training and drilling. Additionally, looking to the future, more than a quarter of organisations (26%) have indicated they won't be investing in their IT security infrastructure in the coming year, despite an increasingly evolving threat landscape.

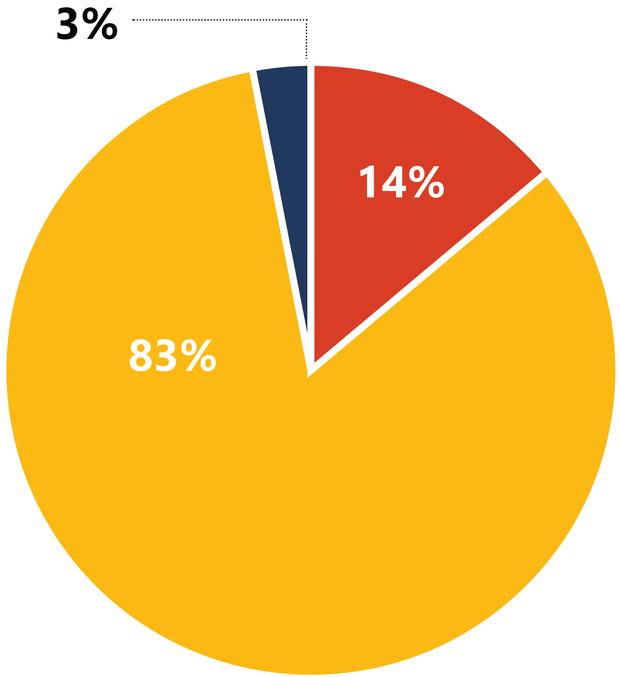
The scale of cyber crime in Ireland

Almost half of Irish businesses (46%) have experienced a cyber incident in the last three years and 14% have had to report an incident to the NCSC or Data Protection Commissioner.

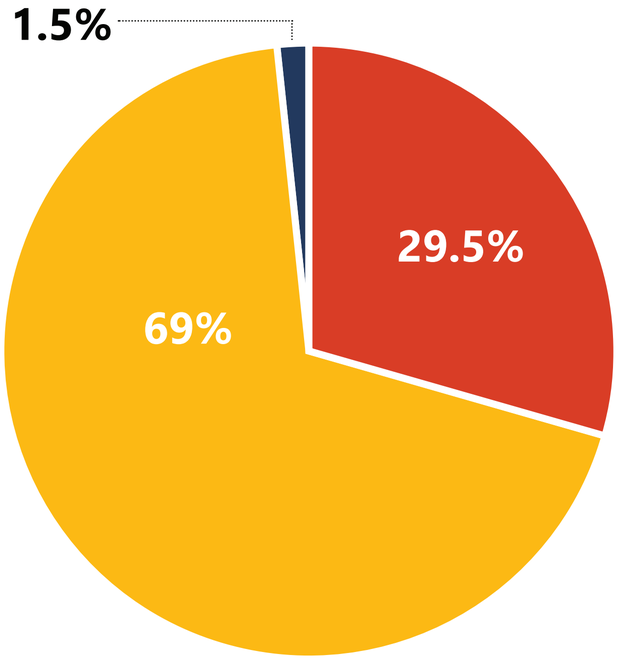
Experienced one or more cyber incidents* in the last 3 years



Reported 1 or more cyber incidents to NCSC or DPC in last 3 years



Ever experienced a data breach



Yes

No

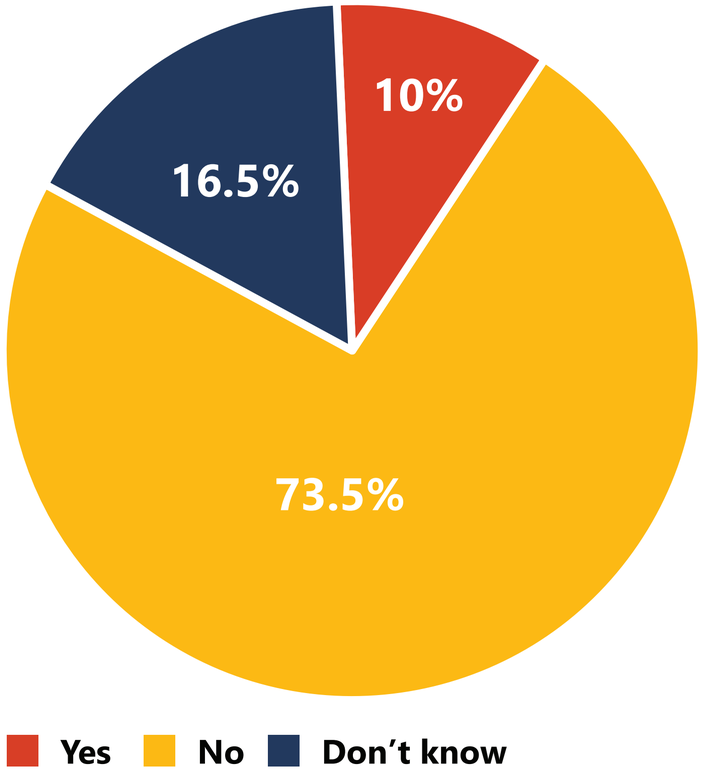
Don't know

*For the purposes of this report, a cyber incident is defined as an event that could jeopardise the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents can take many forms, such as denial of service, malware, ransomware or phishing attacks.

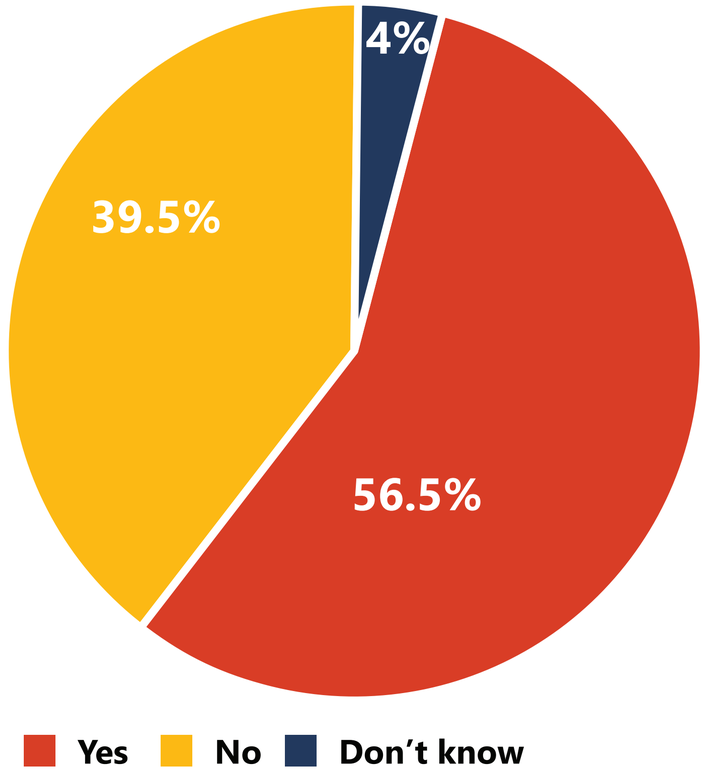
Recent cybersecurity investment and training

While 20% of organisations say that they have suffered financial loss as a result of a cyber incident, almost three quarters of organisations have maintained their spend on IT security, and more than half indicate they have adequate training and security resilience.

Spend on cybersecurity reduced in the last 3 years

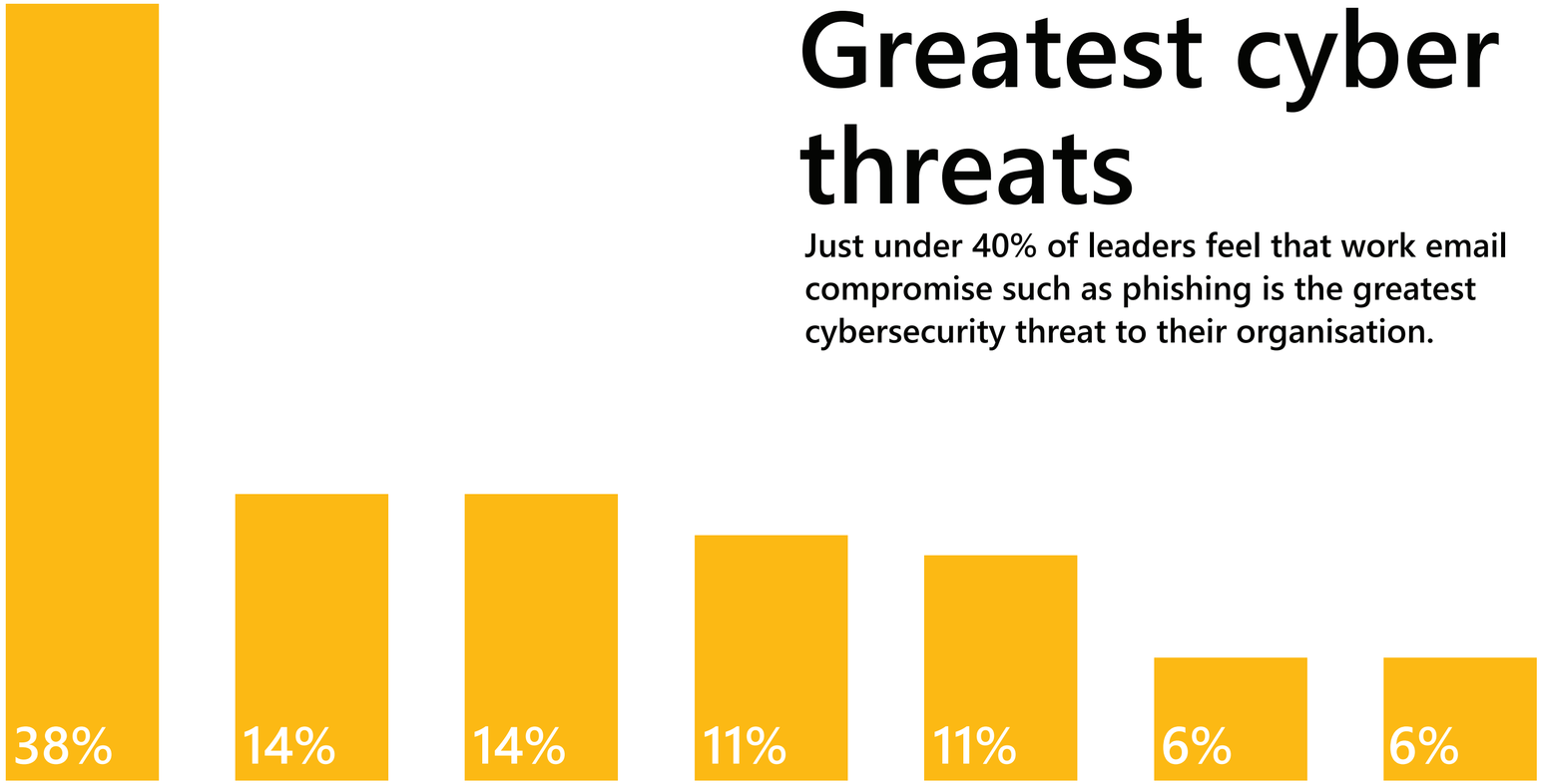


Regular cybersecurity training



Greatest cyber threats

Just under 40% of leaders feel that work email compromise such as phishing is the greatest cybersecurity threat to their organisation.



*Definitions used:

- Work email compromise - phishing, social engineering to trick employees into revealing confidential data
- Increased sophistication of attacks, for example attackers using BOTS to broadsweep attack customers
- Ransomware - malware that encrypts the victim's data and demands a ransom
- Insider threats - employees/contractors intentionally or unintentionally compromising the organisation's security
- Systems misconfigurations - exposing data or resources to unauthorised access due to errors in setting up or managing data
- Supply chain attacks - targeting vendors, partners, or service providers to gain access to systems or data

Create a cybersecurity awareness culture

Make it relatable and human centric
Understand your behaviours and challenges. Focus on a collaborative and positive message to create a security culture. Make security education engaging easy and fun. Use comprehensible content for all types of roles.

Engage your leadership team
Explain benefits and importance of cybersecurity practices to all business areas. Have support from your leadership team to encourage all teams to complete trainings and consume content.

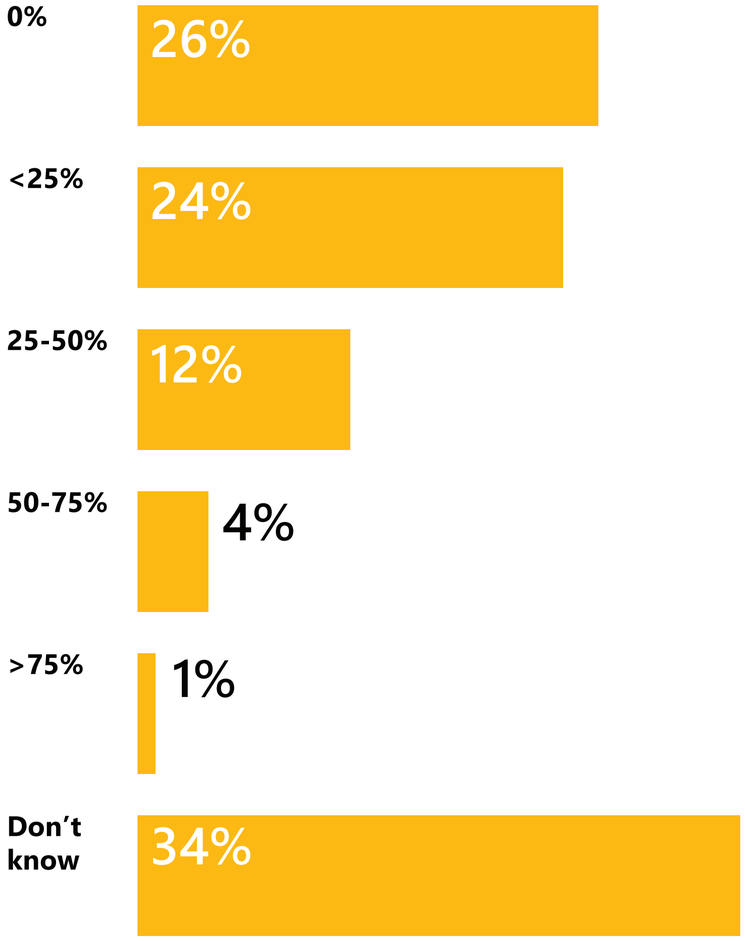
Strategic cyber defences

More than half of organisations lack the strategic infrastructure requirements of an adequate cyber defence strategy.

Future cyber security investment

More than a quarter of organisations are not planning to invest in their IT infrastructure over the coming year. Another quarter are planning to invest less than 25% of their overall IT budgets on cybersecurity measures, 12% are planning to invest between 25% and 50%, and 4% are planning to invest between 50% and 75% of their budgets.

% of IT budget to be spent on cybersecurity in the coming year



2. Artificial intelligence and cybersecurity

The study shows that Irish executives are increasingly fearful of the changing cyber threat landscape due to technological innovation. Additionally, adoption of AI technologies to support defensive strategies is slow.

All forms of new and emerging technology have an impact on the nature of cyberattacks as cybercriminals readily adopt these tools to create more sophisticated forms of breaching defences. The increasing sophistication of generative AI is no different, so it is important to be vigilant and evolve cyber defences accordingly.

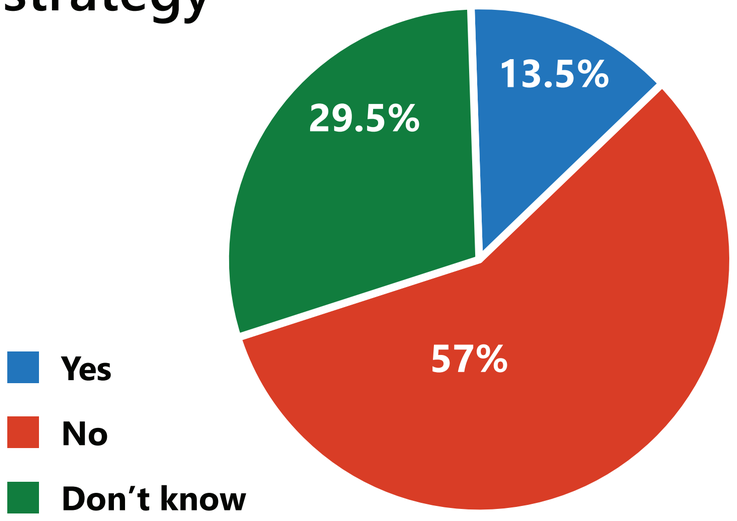
As we are seeing, Artificial Intelligence (AI) technologies are set to become a major focus of regulators and industry. We will undoubtedly see AI exploited by malicious actors to launch cyberattacks, such as automated phishing campaigns, data breaches, and malware that can adapt and evolve to evade detection. This could pose significant threats to businesses, organisations, and individuals.

However, when leveraged as a form of defence, AI can be a powerful tool for enhancing cybersecurity and defending against cyber threats. It can analyse vast amounts of data in real-time to detect and respond to threats more quickly than traditional methods. For example, in Ukraine, we saw the first successful use of AI technology to help defend against Russian cyberattacks. In the coming years, innovation in AI powered cyber defence will help reverse the tide of cyberattacks.

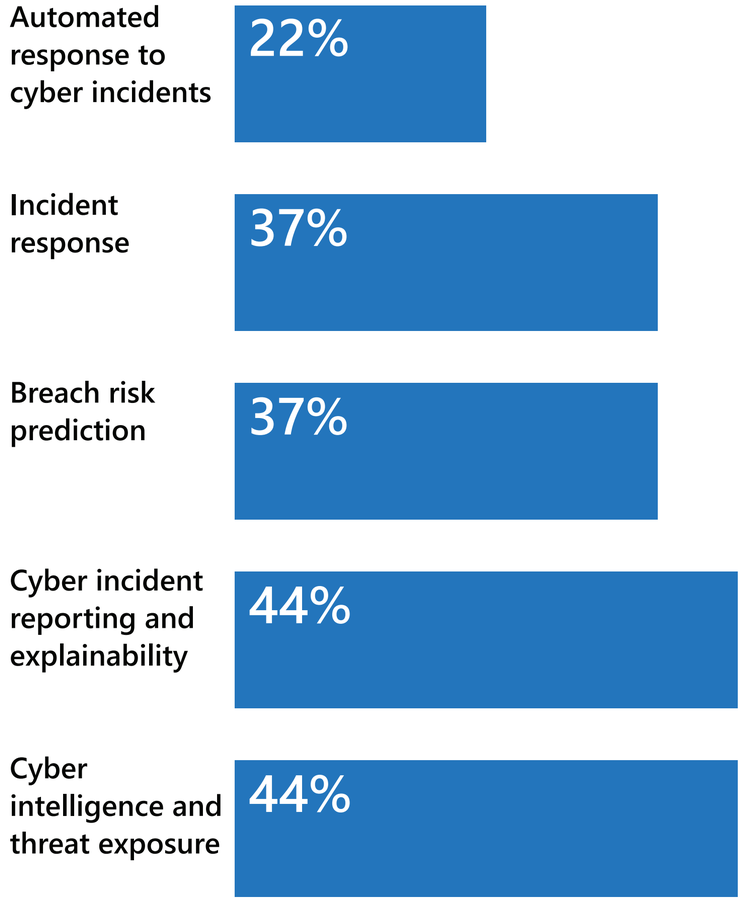
AI in cybersecurity

Just 14% of organisations are currently using AI technology as part of their cybersecurity strategy –although 30% of leaders are unsure if they are in fact using AI technologies.

Using AI-enabled technology in security strategy



Uses of AI solutions within cyber defence



Leveraging AI and large language models in cyber defence

One way that Microsoft is confronting cybercrime is by leveraging AI and large language models (LLMs). LLMs can automate and augment many aspects of cybersecurity, including: threat intelligence; incident response and recovery; monitoring and detection; testing and validation; education; and security governance, risk, and compliance.

Our approach for the next year will focus on bringing to bear AI in combating threats while also embracing the three Security Development Lifecycle (SDL) principles of Secure by Design, Secure by Default, and Secure in Deployment (SD3).

Many modern apps will become LLM based in time. This will increase the threat surface, making them vulnerable to both inadvertent and deliberate misalignments. As LLM-based apps bring new and unique threats, we adapt our security measures and protocols to address them.

Additional information: Governing AI: A Blueprint for the Future (microsoft.com)

Defending against social engineering and identity threats

Joy Chik, President of Identity and Network Access, Microsoft

Social engineering and phishing attacks involve perpetrators who adeptly exploit human vulnerabilities and security gaps, capitalising on trust to gain unauthorised access to sensitive information and systems. Understanding the intricacies of these techniques is critical to defending against them. Emerging technology, such as generative artificial intelligence (GenAI), is accelerating the innovation curve of modern social engineering, particularly phishing techniques, and escalating its threat to our digital society. Social engineering can make end users vulnerable to these schemes, but there are technologies and behaviours they can employ to create a safer online experience for all.

Most breaches begin with an identity compromise, which is why bad actors attempt to steal credentials. Passwords attacks are the most common attack vector. Although people try brute force or password spray attacks, phishing and social engineering are popular because they work, and they're relatively inexpensive to launch.

People are susceptible to phishing schemes and they can be hard to identify. However, the insidious nature of these attacks can result in a significant chain of events from the attack on the individual, to an attack on a large organisation, that can affect the ability to do business or offer services. Alternatively it can be an attack on a community, state, or nation, that could result in interference with infrastructure operations.

To stay ahead of phishing and other types of cyberattacks, organisations must train their

people to recognise phishing and social engineering tactics, so they don't fall prey to them. They should also build AI-driven defences. Signal-driven detections that rely on machine learning and AI to recognise attack patterns and anomalies in user behaviour are already a de facto standard for enterprise-grade and government-grade security defences.

To build, deploy, and manage AI-driven security systems, organisations need to train defenders.

- Organisations need to train human teams on how to use AI tools effectively, e.g., prompt engineering.
- These teams need to customise and enhance AI engines to optimise them for securing their specific environments.

Attackers are adept at finding seams and gaps in security defences, especially in multicloud environments.

- Organisations need to ensure that security systems are interoperable based on standards and tightly coupled.
- Applying Zero Trust principles (verify explicitly, enforce least privilege access, assume breach) is critical.
- Apply Security Defaults

Organisations need strong security hygiene.

- Applying Zero Trust principles to non-human identities used in apps as well as human identities.
- Adhering to strong governance practices, such as removing unnecessary and unused permissions and privileges.

3. Regulation and legislation compliance and readiness

The majority of Irish executives are unaware of the upcoming legislation NIS2 or DORA which will require organisations to have a more robust cyber defence strategy. Additionally, the majority were unsure if their organisations had investment, or a roadmap earmarked to ensure compliance with NIS2 by October 2024.

In October 2024, the NIS2 Directive will come into effect across the EU, covering 18 sectors and more than 180,000 companies. The directive is an essential piece for strengthening the cybersecurity posture of organisations and reinforcing the trust of their stakeholders. Its purpose is to establish a baseline of minimum-security measures for digital service providers and operators of essential services, to mitigate the risk of cyberattacks and to improve the overall level of cybersecurity in the EU.

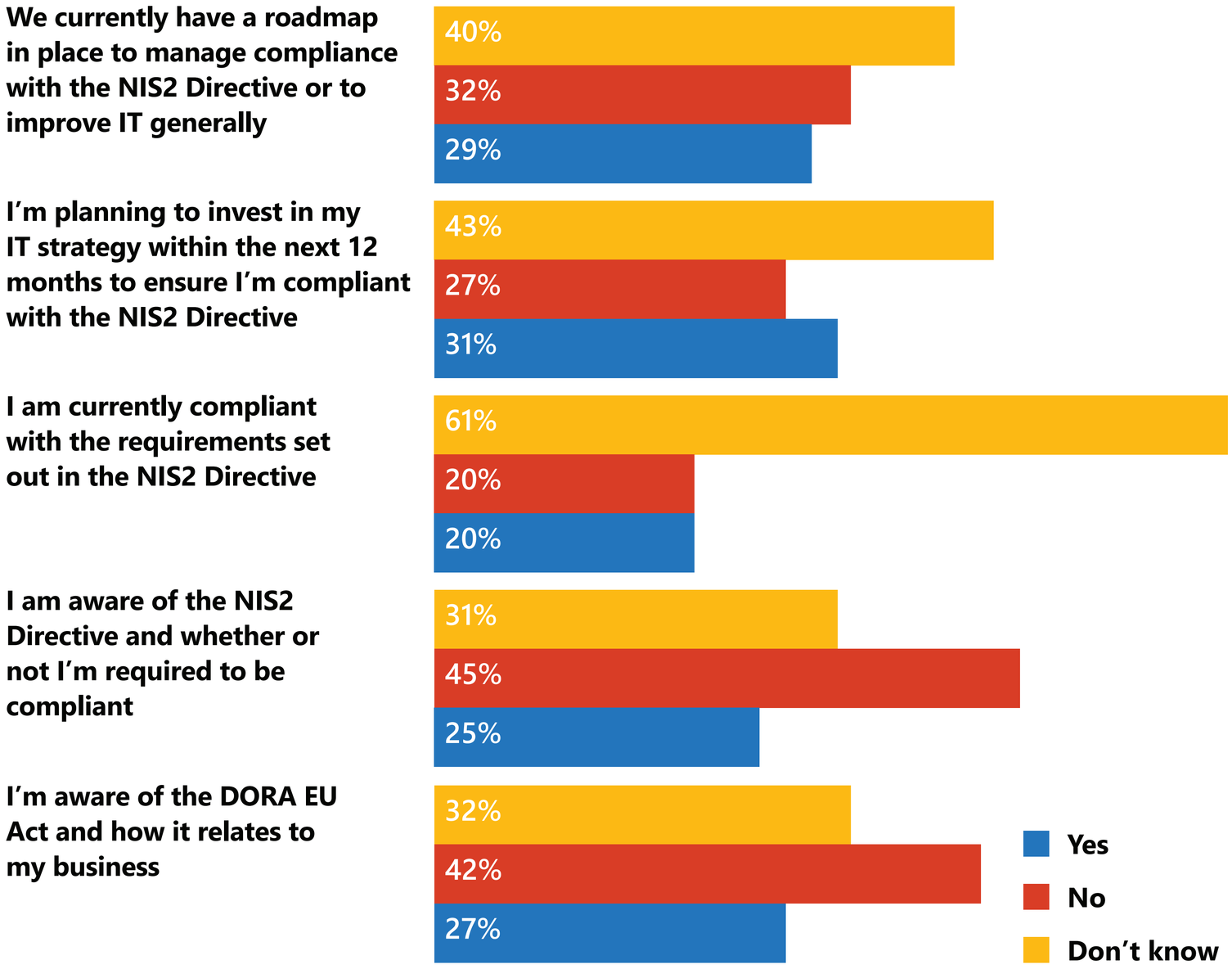
We can see from our research that more than 70% of leaders either are not aware of, or prepared for, compliance with the directive. The research also revealed that while organisations may have experienced a cyber incident (46%), not all (14%) felt they had to report it. However, under NIS2, organisations will have to report earlier and more often. It is imperative that Irish organisations are aware of, and planning for, this new legislation that will have a significant impact on their organisation's, and potentially their customers', cybersecurity policies and defences.

Compliance and readiness

Just under half of leaders are unaware of major upcoming legislative changes that will impact their cybersecurity strategy – specifically Network and Information Security Directive 2 (NIS2) (45%) which will be enforced by October 2024, and the Digital Operational Resilience Act (DORA) (42%).

Of those who are aware of NIS2, 20% feel they are currently compliant with the legislation and 20% believe they are not compliant. 60% of all respondents are unsure if they are or not.

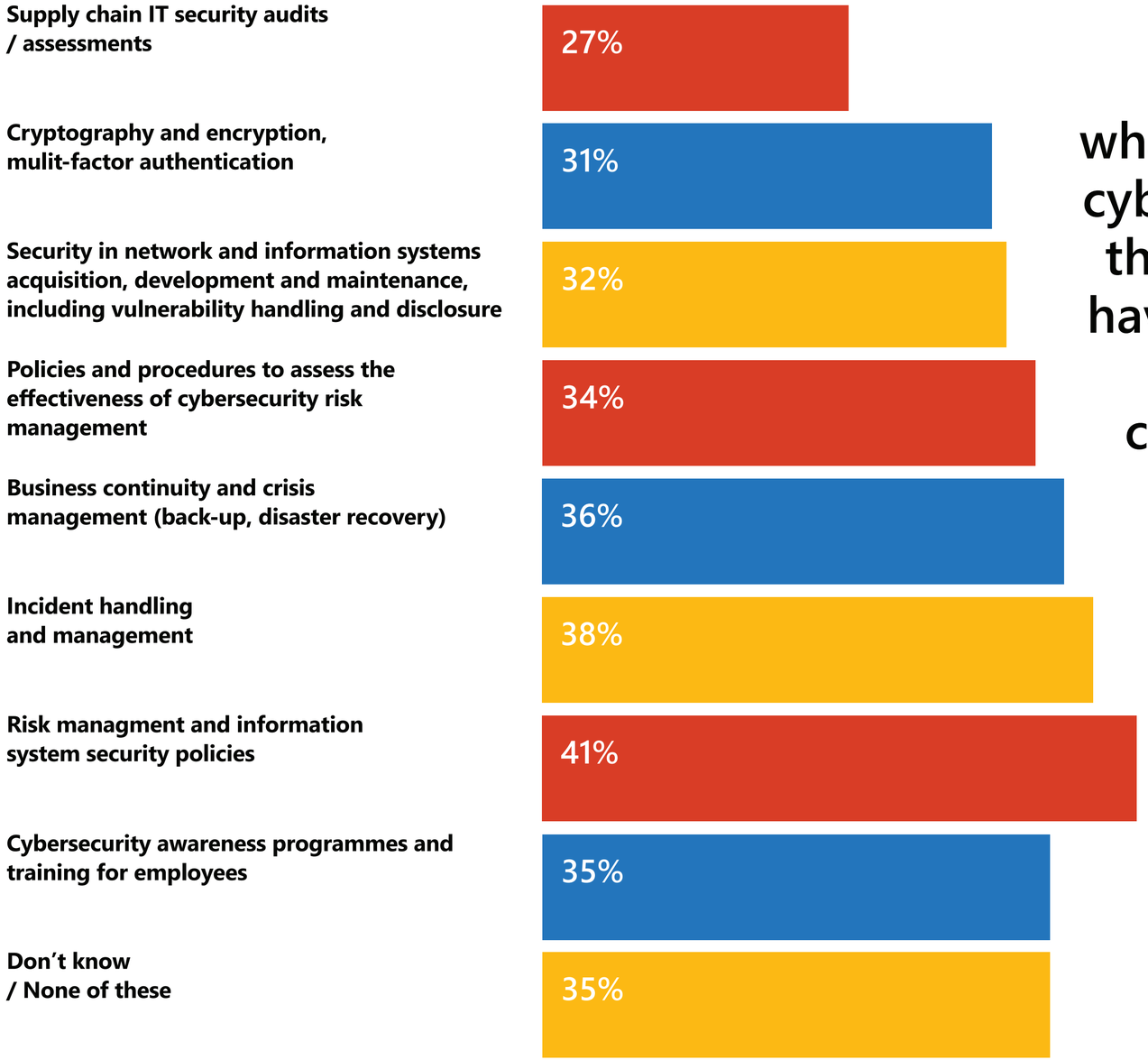
Positively, 31% of organisations are planning to invest in their strategy to achieve compliance with NIS2 and 29% have a roadmap in place to achieve this. That said, in the main, business leaders did not know if their organisations have investment (43%) or a roadmap in place (40%)



The challenges and opportunities of NIS2 and DORA

The new regulatory frameworks of NIS2 and DORA aim to enhance the security and resilience of critical digital infrastructure and services in the EU. They will impose stricter requirements and higher fines for non-compliance on services provided by critical and important sectors, as well as extending the scope of sectors and entities covered by the existing legislation. This means that many organisations will need to review and update their cybersecurity strategy, policies, and practices to align with the new standards and expectations.

Leaders indicate what areas of cybersecurity they already have in place for NIS2 compliance



Key features of NIS2

Sets a benchmark of minimum cybersecurity measures including risk assessments

Emphasises the need for cybersecurity in supply chains and the relationship between companies and direct suppliers

More than 180,000 companies are affected in Europe

Sets a benchmark ‘minimum measures’ including risk assessments, policies and procedures for cryptography, security procedures for employees with access to sensitive data, multi-factor authentication, and cybersecurity training

Provides guidelines on reporting security incidents and potential vulnerabilities

Aims to harmonise cybersecurity requirements and enforcement across Member States

Covers 18 sectors including: energy, food, finance, healthcare, transport, and manufacturing

Directs companies to create a plan for handling security incidents and managing business operations during and after a security incident

The evolving threat landscape globally

Insights from the Microsoft Digital Defense Report

Microsoft's Global Digital Defense Report 2023

The Microsoft Digital Defense Report details cyberattack trends throughout the year, how threats are evolving and what defenders must do to stay ahead. We've included the below key takeaways for your convenience.

- Russia and China are refocusing their influence operations to target diaspora communities.
- Iran and North Korea enhanced their offensive cyber capabilities.
- AI technology will be crucial for successful defence, automating and augmenting aspects of cybersecurity such as threat detection, response, analysis, and prediction. For example, Russia's use of cyberweapons as part of its hybrid war against Ukraine sparked sustained collaboration between Microsoft and Ukrainian officials to successfully defend against most of these cyberweapons.
- Cyberattacks are occurring more frequently than ever; Microsoft's built-in protections have blocked tens of billions of malware threats, thwarted brute-force password attack attempts, and mitigated distributed denial of service (DDoS) attacks.
- Partnerships between the public and private sector are critical in keeping us all safe. For example, 75% of eligible citizens in democratic nations have the opportunity to vote in the next year and a half. We must ensure that strong cyber defences keep elections safe.

Read the full report Microsoft Digital Defense Report 2023 (MDDR) | Microsoft Security Insider

The evolving threat landscape globally

At Microsoft, more than 10,000 security experts analyse over 65 trillion signals each day with the help of AI. The Microsoft Threat Intelligence Centre tracks hundreds of threat actor groups worldwide. The Microsoft security ecosystem includes more than 15,000 security partners with specialised solutions, while the global open community of security researchers and testers contribute to bug bounties and security challenges. This broad, deep, and diverse security ecosystem is driving some of the most influential insights in cybersecurity. Together, we can build cyber resilience through innovative action and collective defence.

Irish organisations can benefit from Microsoft's regular updates and analysis of the ever-evolving nature of cyber crime through our quarterly Cyber Signals Bulletins. These bulletins provide real-time advice to leaders to stay informed of ongoing global trends as well as helpful advice to responding to the threats.

65 trillion

Signals synthesized daily

That is over 750 billion signals per second, synthesized using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

300+

Threat actors tracked –Microsoft Threat

Intelligence has grown to track more than 300 unique threat actors, including 160 nation state actors, 50 ransomware groups, and hundreds of others.

10,000+

Security and threat intelligence experts

10,000+ engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

100,000+

Domains removed

100,000+ domains utilised by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

4,000

4,000 identity attacks blocked per second

4,000 identity authentication threats blocked per second.

15,000+

Partners in our security ecosystem

15,000+ partners with specialized solutions in our security ecosystem, who increase cyber resilience for our customers.

135 million

Managed devices

135 million managed devices providing security and threat landscape insights.

Microsoft Digital Defense Report 2023

How can we protect against 99% of attacks?

1. **Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.

2. **Apply zero trust principles:**
   - **Explicitly verify**. Ensure users and devices are in a good state before allowing access to resources.
   - **Use least privilege access.** Allow only the privilege that is needed for access to a resource and no more.
   - **Assume breach**. Assume system defences have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.

3. **Use extended detection and response (XDR) and anti-malware:** Implement software to detect and automatically block attacks and provide insights to the security operations software.

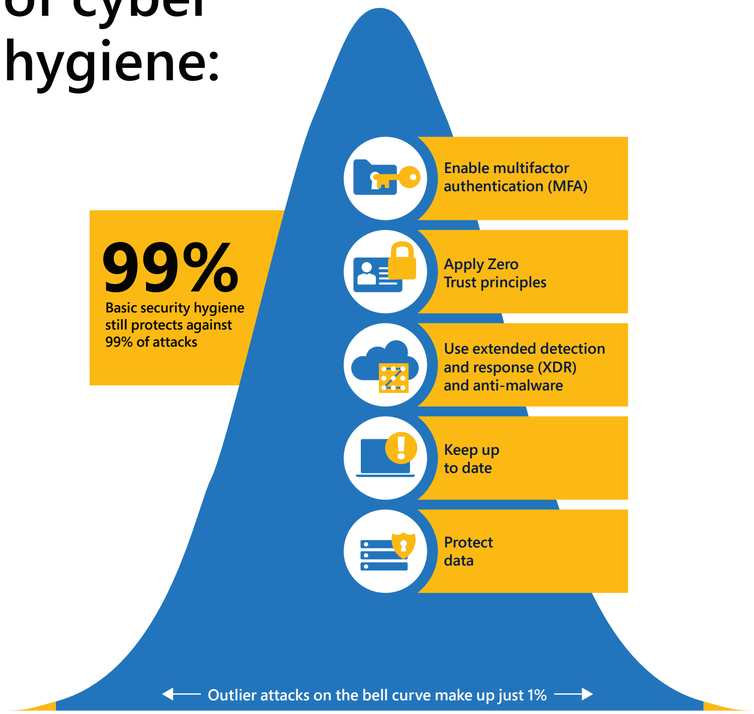
4. **Keep up to date:** Unpatched and out-of-date systems are a key reason many organisations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.

5. **Protect data:** Knowing your important data, where it is located, and whether the right defences are implemented is crucial to implementing the appropriate protection.

Hyperscale cloud makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With software as a service (SaaS) and platform as a service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management.

Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud enabled capabilities like XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.

Fundamentals of cyber hygiene:

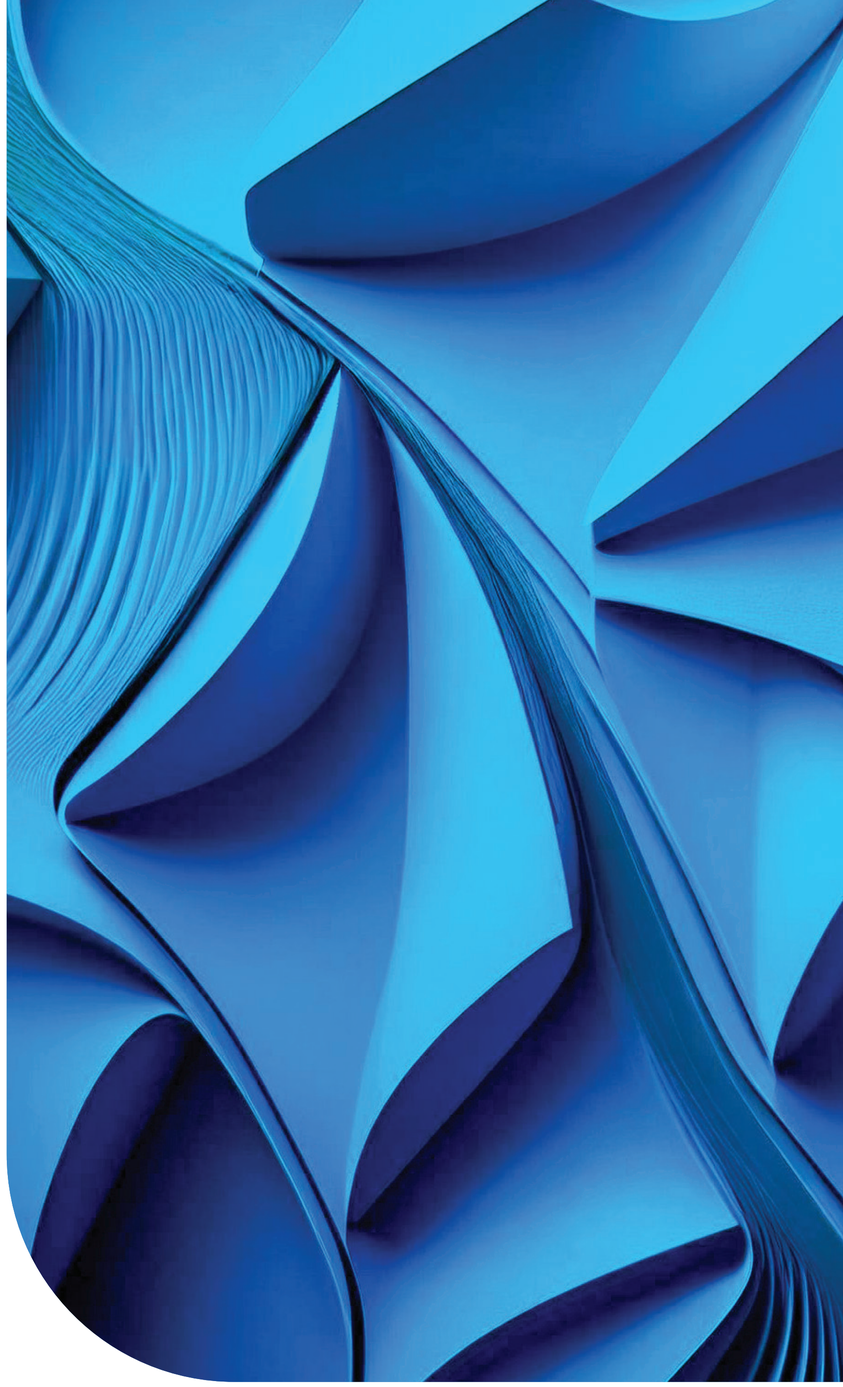


How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.

Microsoft Digital Defense Report 2023

Microsoft Security

Cybersecurity trends **in Ireland 2023**



Cybersecurity: resources for effective defence

- Learn more: https://aka.ms/cybersecurity-awareness
- For news and updates: https://www.microsoft.com/en-us/security/blog/
- For NIS2 Directive guidance for leaders: NIS2: Guiding Principles for Leaders
- Latest cybersecurity insights and best practices: Be Cyber Smart Kit | Microsoft Security