amárach research

Microsoft

Securing the Future 2020

THE STATE OF CYBERSECURITY IN IRELAND
AN AMÁRACH REPORT FOR MICROSOFT IRELAND
JANUARY 2020

Contents

Foreword

Every day, organisations in Ireland take precious time and resources away from their core business to defend against and recover from cyberattacks. They struggle to operate dozens of complex disconnected tools, yet the gaps between those tools remain, and threats get through. As a result, organisations can investigate only 56% of the security alerts they receive on any given day.

Microsoft invests heavily to secure its one billion customers across enterprise and consumer segments globally and in 2018, blocked over five billion malicious and suspicious phishing emails.

In February 2019, Microsoft Ireland looked at how poor employee security habits within large public sector and private organisations across Ireland threatened data loss and cyber breaches. We found that 44% of employees have experienced problems with hacking, phishing and cyber fraud. When we looked more closely, this was a combination of poor security behaviour amongst employees, coupled with a lack of consistent security training.

"We found that 44% of employees have experienced problems with hacking, phishing and cyber fraud."

However, the issues highlighted are not just the sole responsibility of the employee. As cyber threat risks grow and become more sophisticated, we need a broader view of the security landscape in Irish organisations.

Nearly a year on, we are now looking at employers in Ireland in these same sectors and examined their security habits. Overall we see a lack of confidence amongst Irish companies regarding their approach to digital security and access management. A gap exists between an organisations' view of how secure they are, versus the reality where their organisational security habits are leaving them open to data loss or hacking. Iterative security policies, and poorly implemented planning have spawned some bad employee habits that opened up specific areas of potential risk that this report will talk about in more depth.

Enterprise security is as much a reputational priority as cash flow or quarterly earnings. It needs to be a foundational element of any major organisation, reinforced with a consistent set of policies, practices and training across the four key areas of security outlined in this report.

In addition, what's needed is a pivot to "boundaryless" security, known more commonly as Zero Trust. In a Zero Trust model, all users and devices—both inside and outside the corporate network—are deemed untrustworthy. Access is granted based on a dynamic evaluation of the risk associated with each request. The same security checks are applied to all users, devices, applications, and data every time. If companies take this approach they can't lose.

While we are all on a digital transformation journey, now is the time to get the building blocks right, including having an agile security strategy, to be set up for future digital success.

Des Ryan
Solutions Director, Microsoft Ireland

Introduction

With breaches on the rise, it's time to dispel the myth that security is an add-on, and start talking about security as a differentiator, money-saver, and foundational element in every enterprise strategy.

However, this is not simply another report about the importance of cybersecurity but more of a business case for prioritising security. For example, productivity is paramount for today's enterprise, but productivity grinds nearly to a halt when security lapses occur. In fact, a quarter of a company's attack costs are attributable to downtime, according to recent Microsoft research.

In 2019 Microsoft published a report on cybersecurity in Ireland, based on a survey of 900 employees' perspectives throughout the island of Ireland. The research was conducted by Amárach Research on behalf of Microsoft Ireland. We have now revisited the topic again, but from an employer's perspective, by surveying 200 senior decision makers in organisations employing over 250 staff throughout the Republic of Ireland.

"Our 2020 report shows that Irish businesses face critical vulnerabilities due to the behaviour of some of their employees."

Since our last report on cybersecurity in Ireland there have been several high-profile media stories about the damage done by security breaches around the world. However, this is not a problem happening 'elsewhere': our 2020 report shows that Irish businesses face critical vulnerabilities due to the behaviour of some of their employees. This report explores the employer perspective of the cybersecurity agenda and gives us a chance to examine some of the key perceptual gaps between employees and employers about emerging security threats.

We have used a unique Microsoft framework to guide our 2020 research, focusing on four key areas of cyber vulnerability:

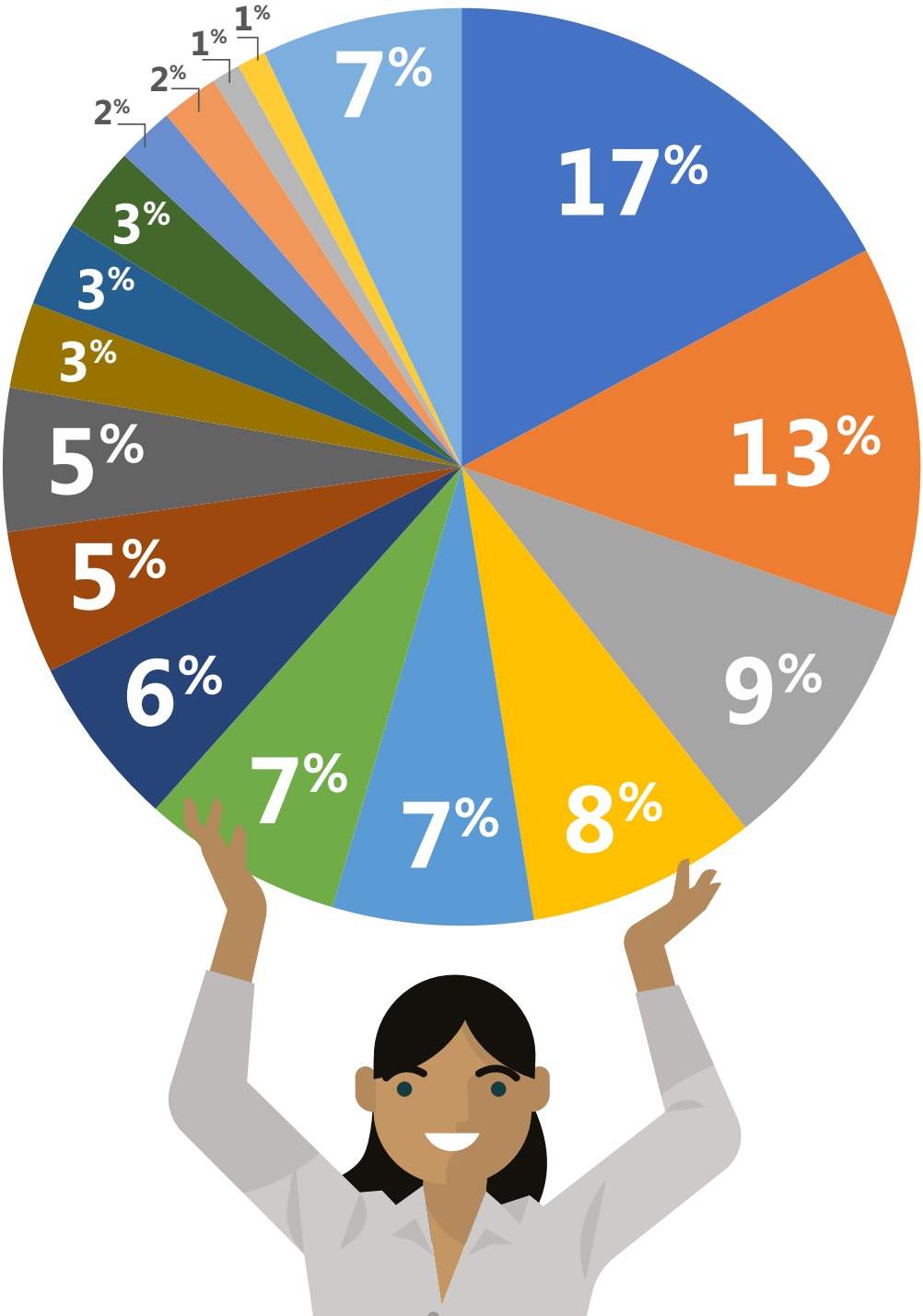
- **Identity and Access Management**
- **Threat Protection**
- **Security Management**
- **Information Protection**

We polled 200 IT decision makers in the Republic of Ireland using this framework, all working in corporate organisations employing over 250 staff. We drew on similar themes to that in the previous survey of 900 employees. We have compared and contrasted their opinions where relevant throughout this report.

Respondents Industry Breakdown:

Industry

- Manufacturing
- Health and social care
- Banking, insurance and other financial services
- Central or Local Government
- Education and Training
- ICT and Telco products or services
- Hospitality and recreation
- Consulting or other professional or advisory services
- Construction
- Charity, social enterprise or non-profit
- Transport, logistics and storage
- Other service industry
- Utilities
- Technical and scientific services
- Retail or wholesale
- Agriculture, forestry and fishing
- Other



01

Identity and Access Management

Identity is at the centre of how organisations connect people, devices, apps, and data. Taking a comprehensive approach to identity management, organisations can better manage and secure partners, employees, and customers across on-premise and cloud infrastructure.

IAM is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons, and it's more challenging than ever to manage for today's IT.

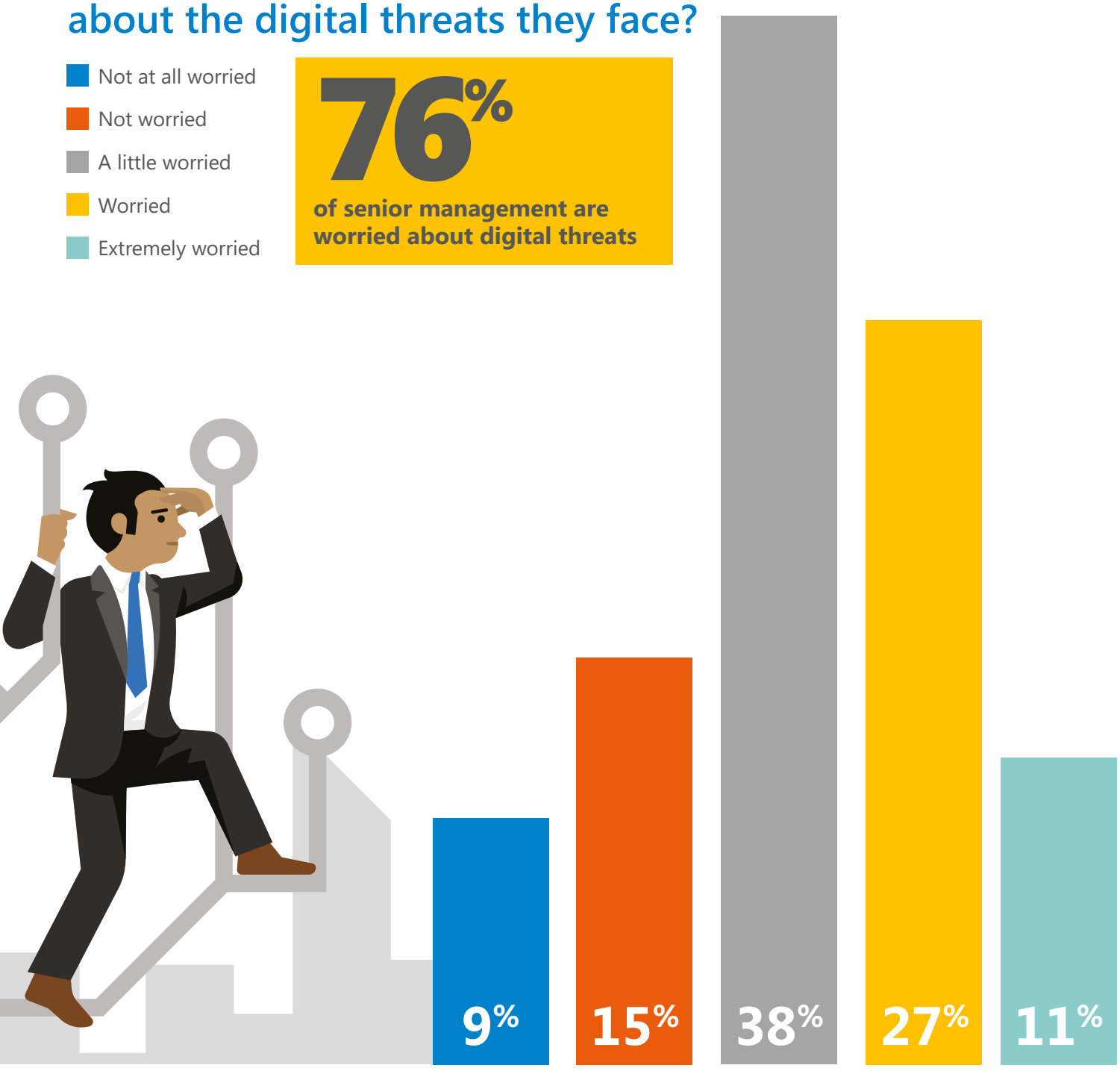
In our 2019 survey of employees in Ireland, 44% of employees said they use the same password across multiple devices, and 38% recycle their passwords at work.

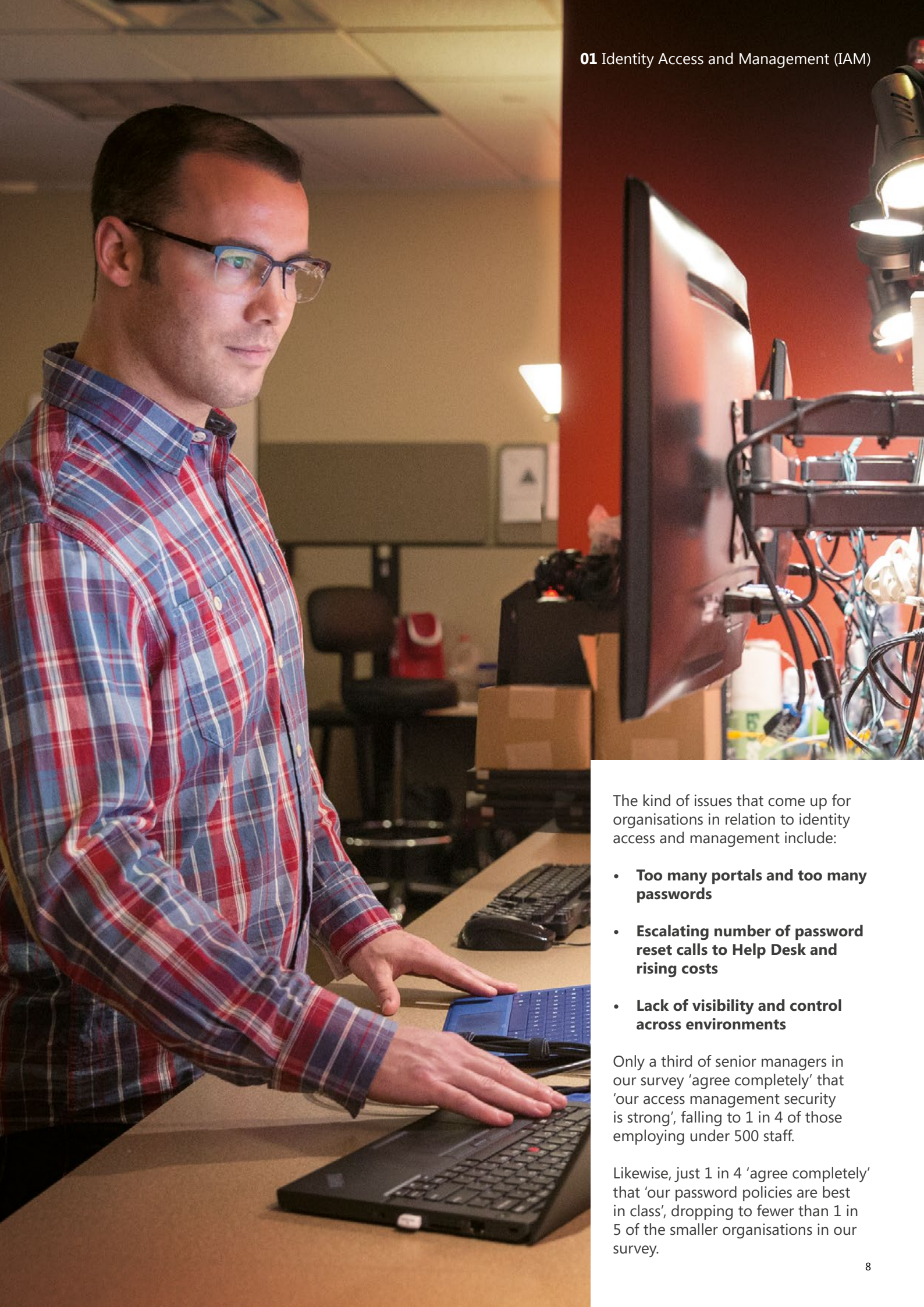
Considering last year's research demonstrated the concerning attitude towards access management amongst employees, we wondered how worried are senior management in Irish businesses about the digital threats they face?

Our 2020 survey reveals that only 1 in 5 Irish IT decision makers are not worried for their company, while nearly 76% said they were worried (1 in 10 are extremely worried).

Interestingly, it is the larger firms in our survey – employing more than 500 people – who are the most worried, as are those who have previously experienced problems with phishing, hacking etc. (see Section 2).

How worried are senior management in Irish businesses about the digital threats they face?





The kind of issues that come up for organisations in relation to identity access and management include:

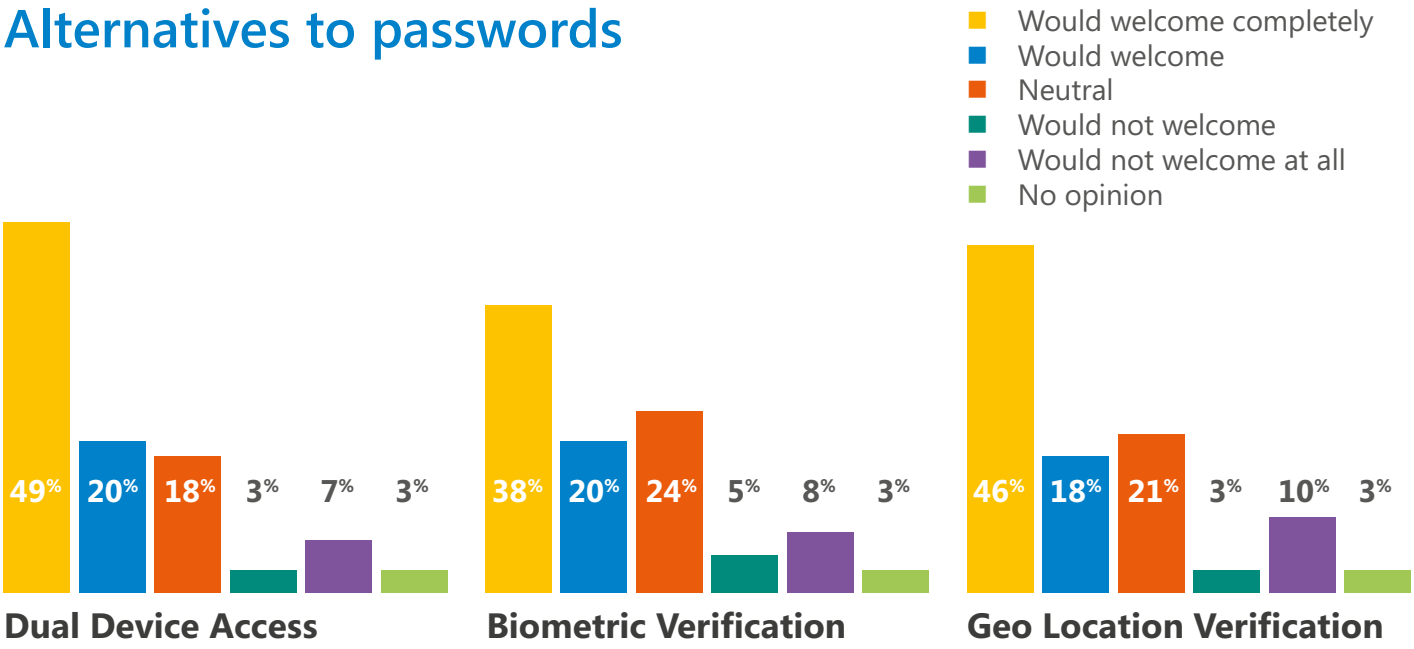
- **Too many portals and too many passwords**
- **Escalating number of password reset calls to Help Desk and rising costs**
- **Lack of visibility and control across environments**

Only a third of senior managers in our survey 'agree completely' that 'our access management security is strong', falling to 1 in 4 of those employing under 500 staff.

Likewise, just 1 in 4 'agree completely' that 'our password policies are best in class', dropping to fewer than 1 in 5 of the smaller organisations in our survey.

We asked employers whether they would welcome secure alternatives to passwords in the future (some of which are already in place in some organisations).

Alternatives to passwords



Definitions:

Dual device access - using an app or code in a text message on your mobile to access a service via your laptop/PC.

Biometric verification - laptop or phone reads your fingerprint or scans your face via the inbuilt camera to access a service.

Geo location verification - receiving a text message or email to verify you are the person making a purchase in, say, a shop or restaurant while abroad.

63% **would welcome alternatives to passwords and 25% would welcome alternatives to passwords in governement organisations.**

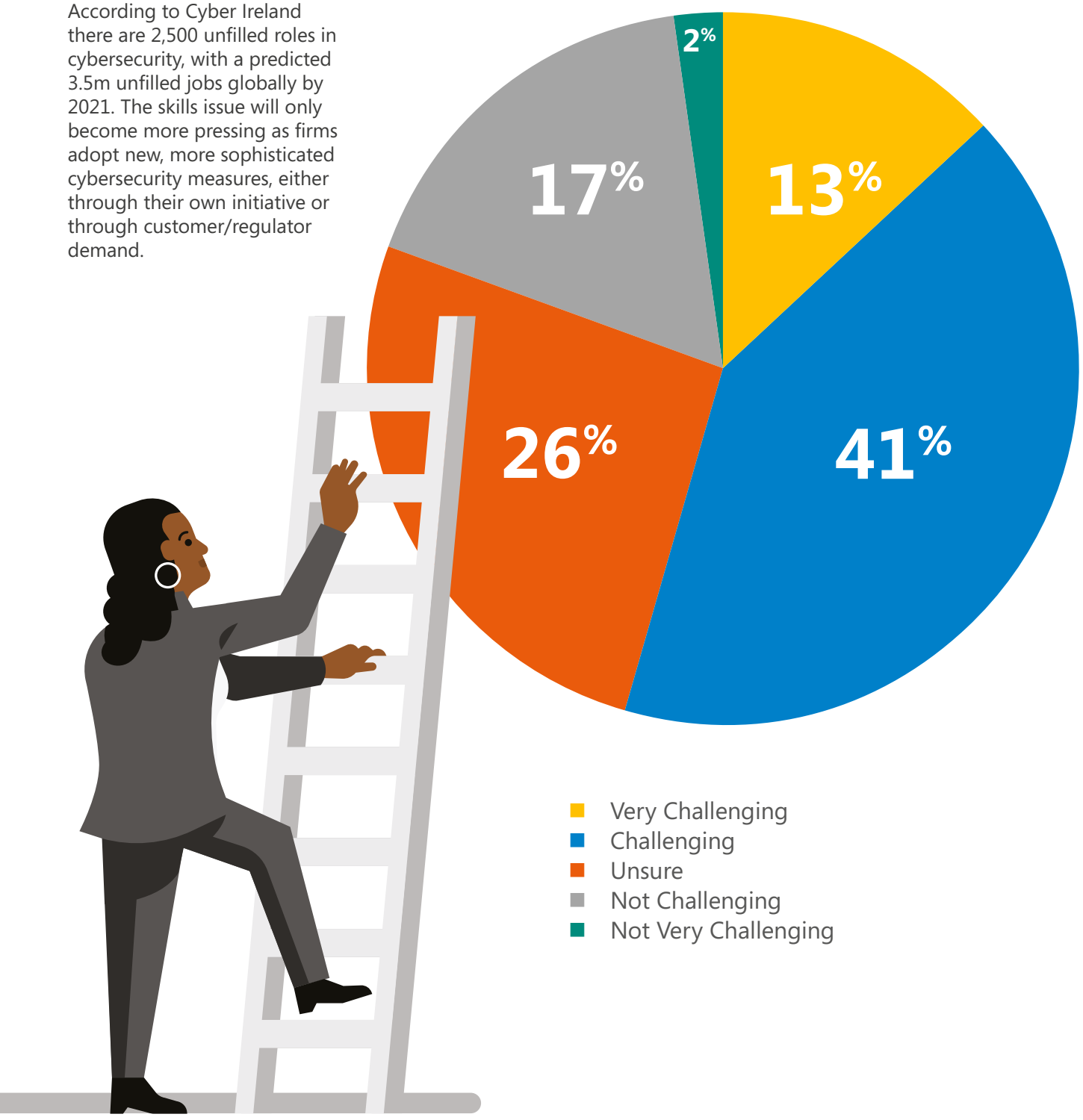
We asked a similar question of employees in Ireland in 2019 last year, and their responses are included for comparison:

% Would welcome each alternative solution:	% of Employers In 2020	% of Employees In 2019
Dual device access	69%	41%
Biometric verification	58%	62%
Geo location verification	64%	49%

Cybersecurity Skills Gap:

According to Cyber Ireland there are 2,500 unfilled roles in cybersecurity, with a predicted 3.5m unfilled jobs globally by 2021. The skills issue will only become more pressing as firms adopt new, more sophisticated cybersecurity measures, either through their own initiative or through customer/regulator demand.

How challenging are you finding it to find someone with cybersecurity skills



KEY TAKE AWAY:

Most large firms are worried about the management of identity and access in their organisations. Only a minority feel they have a strong access management security or that their password policies are best in class. So they recognise they have room for improvement. Moreover, it is those organisations that have experienced significant cyberattacks in the past who are consistently more likely to be modest about their current security performance – and more willing to admit they can do better.

10

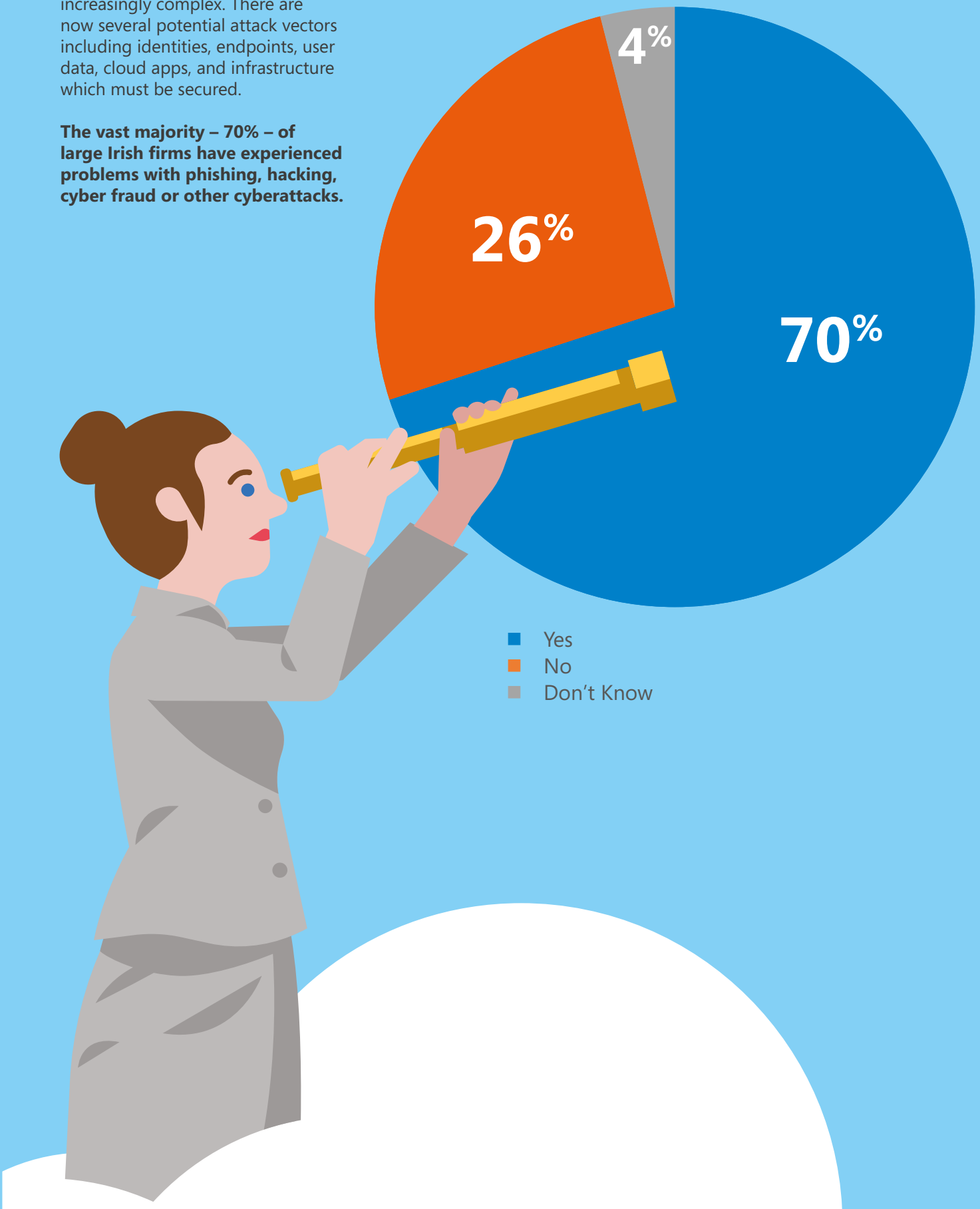
02

Threat Protection

Cybercriminals are finding more advanced methods to attack organisations. Therefore, built-in cybersecurity services need to be seamlessly integrated and powered with automation to help protect, detect, and respond to the latest threats. The threat landscape is increasingly complex. There are now several potential attack vectors including identities, endpoints, user data, cloud apps, and infrastructure which must be secured.

The vast majority – 70% – of large Irish firms have experienced problems with phishing, hacking, cyber fraud or other cyberattacks.

Has your organisation ever experienced problems with phishing, hacking, cyberfraud or other cyberattacks?



For organisations dealing with threat protection, typical issues include:

- **Growing sophistication/volume of advanced threats**
- **Expanding digital estate and multiple attack vectors**
- **Difficulty correlating disparate data points and threat signals**

In our survey, we asked respondents to pick the threats that they are most worried about and a clear hierarchy of concerns emerged:

1 in 4

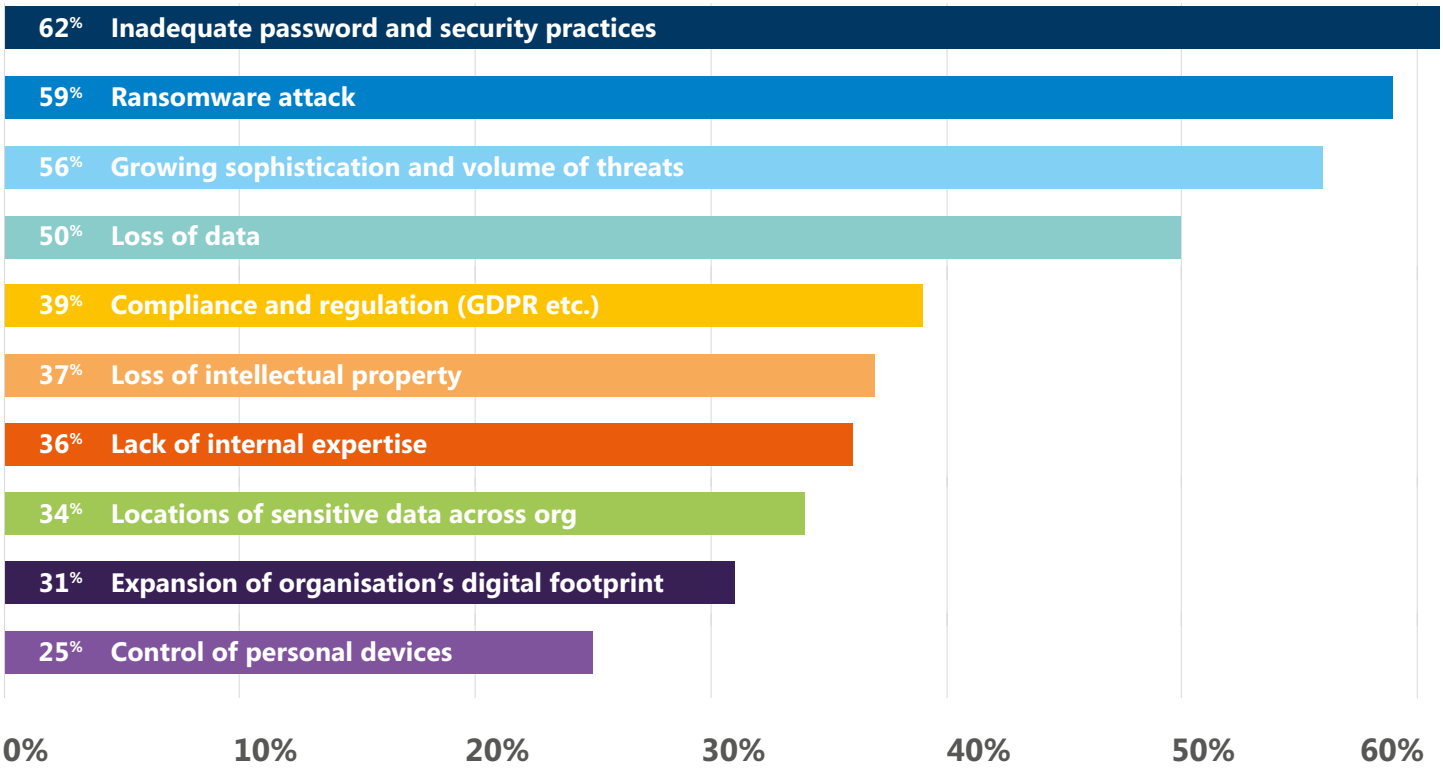
companies are confident they can respond to any security incident effectively.

33%

of government organisations agree that they can respond to any security incident effectively.

Main security threat concerns for organisations in Ireland:

% WORRIED



Passwords, ransomware, threat sophistication, and data loss are the top concerns, regardless of size of organisation. Despite passwords being the top threat, only 65% believe their password policies are best in class.

Perhaps, not surprisingly, just one in four companies 'completely agrees' with the statement 'we are confident we can respond to any security incident effectively'; falling to below 1 in 5 of those that have experienced cyberattacks.

65%

of senior decision makers in organisations in Ireland believe their password policies are best in class.

KEY TAKE AWAY:

While Irish decision makers are now confident about their ability to comply with GDPR and the wider data regulatory agenda, the majority feel vulnerable to the type of hostile threat such as ransomware that features in the headlines with increasing frequency.
Experience of past attacks certainly makes businesses less sanguine about their vulnerability to future attacks and appears to be a catalyst encouraging them to do more to protect themselves from growing hostility.

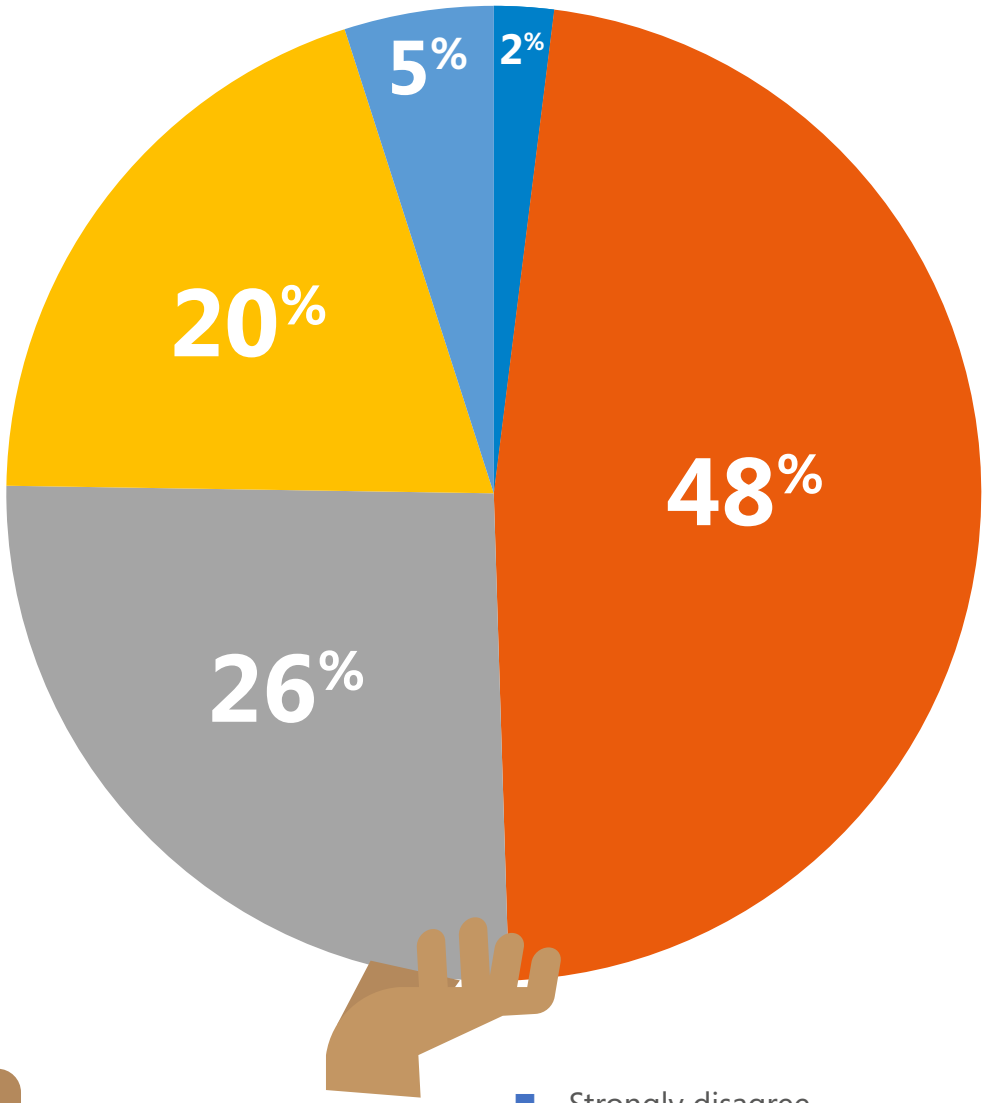
03

Security Management

As the complexity and number of attacks increase, organisations often have many security solutions in place. Given the pace of change and acceleration in the cybersecurity landscape, IT teams are operating at more than 100% capacity. The result is poor security health and posture, which manifests in episodes that have compromised scores of organisations and millions of customers.

Just one in four firms in our survey 'completely agree' with the statement 'our organisation is well secured against advanced cyber threats' – rising to 4 in 10 of those that haven't been subject to a cyberattack. When it comes to security management, only 3 in 10 strongly agree that 'we have a clear strategy for protecting and managing sensitive information' whereas half of government organisations agree they have a clear strategy for protecting and managing sensitive information. Even fewer – 1 in 4 – completely agree that 'we have enough capabilities in-house to deal with all our security requirements'. Only 25% of government organisations agreed to this statement with none strongly agreeing.

Our organisation is well secured against advanced cyber-threats

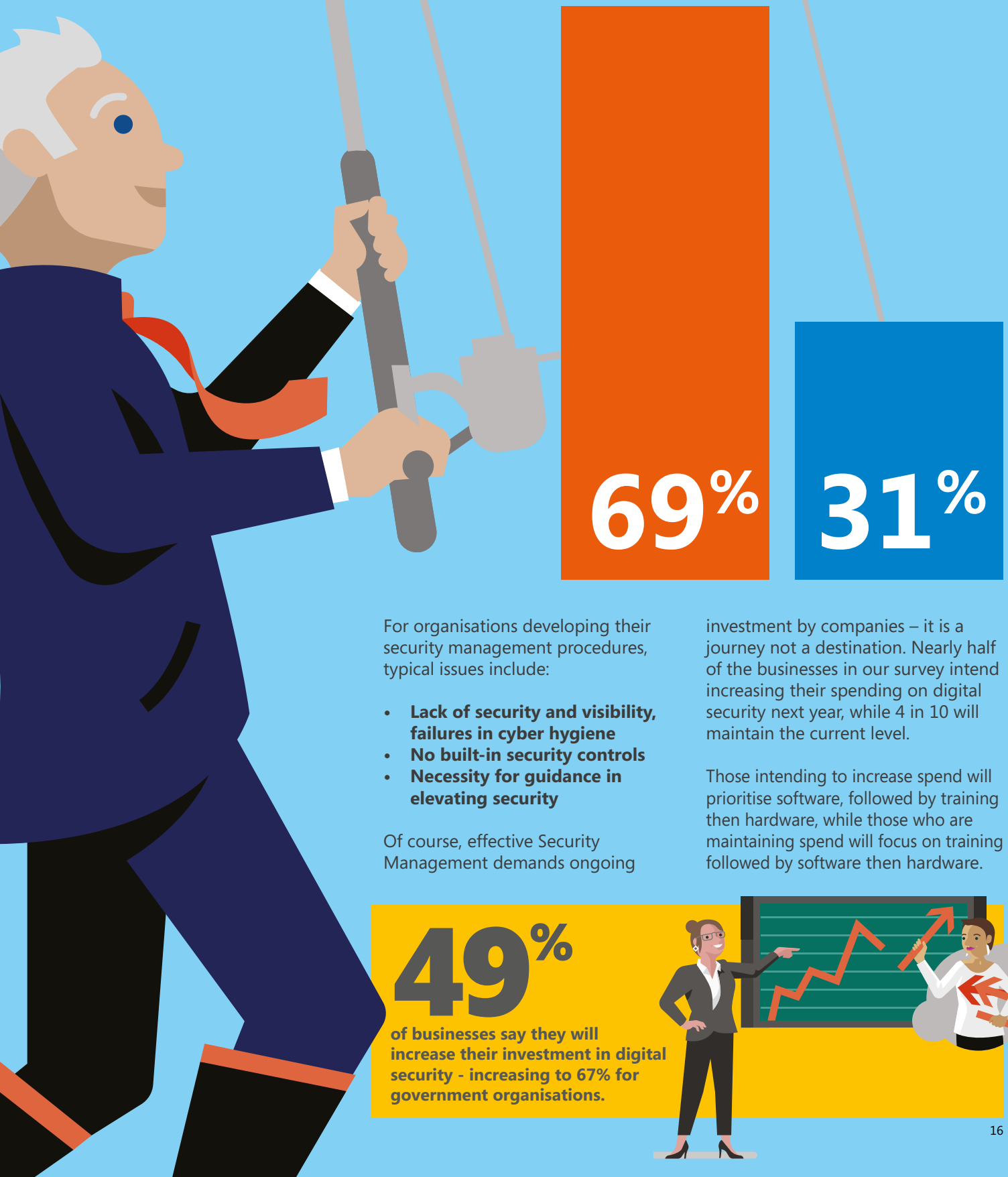


59%

of government organisations agree they are well secured against advanced cyber threats.

Are you planning to hire someone with cybersecurity expertise into your organisation?

Perhaps not surprisingly, many organisations intend beefing up their cybersecurity expertise through recruitment in future, but they also recognise just how challenging this will be:



For organisations developing their security management procedures, typical issues include:

- **Lack of security and visibility, failures in cyber hygiene**
- **No built-in security controls**
- **Necessity for guidance in elevating security**

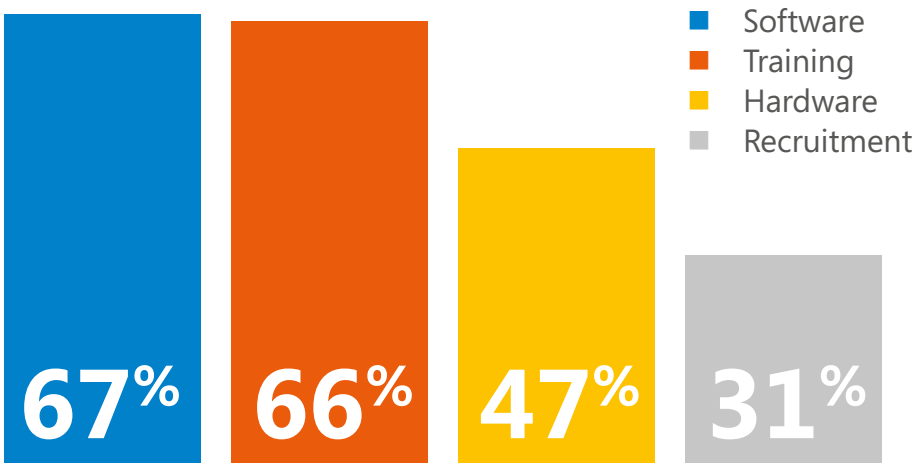
Of course, effective Security Management demands ongoing investment by companies – it is a journey not a destination. Nearly half of the businesses in our survey intend increasing their spending on digital security next year, while 4 in 10 will maintain the current level.

Those intending to increase spend will prioritise software, followed by training then hardware, while those who are maintaining spend will focus on training followed by software then hardware.

49%

of businesses say they will increase their investment in digital security - increasing to 67% for government organisations.

What investments if any will you make in digital security next year?



This planned investment marks a change since our 2019 survey of employees, 39% said the hardware they use at work is only updated every few years or less often, while 48% said they receive training or guidance on security less than once a year or never.

KEY TAKE AWAY:

As cybersecurity threats increase in scale and sophistication, IT decision makers in Ireland's largest firms are looking at new ways of responding to these threats and are prepared to invest in the means to secure their business operations in future.

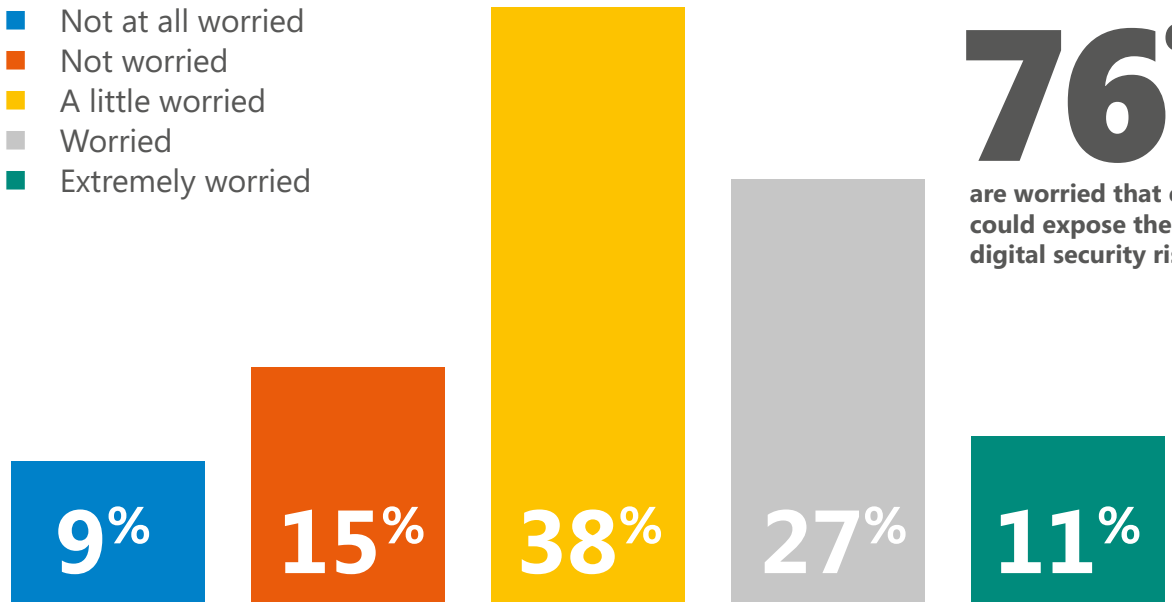
04

Information Protection

Today, protection of sensitive information must be comprehensive. It applies to how we discover, classify, protect, and monitor sensitive data – wherever it lives or travels – across devices, apps, cloud services and on-premises. Information protection focuses on ensuring that only the right people can access sensitive information – and preventing the accidental leakage or over-sharing of critical information. It's about implementing the right policies and controls without inhibiting user productivity – a hard balance to maintain for today's complex and data-heavy enterprises.

Given that employees pose potential security risks, we asked respondents how worried they were that employees could expose the company to digital security risks, whether unintentional or not.

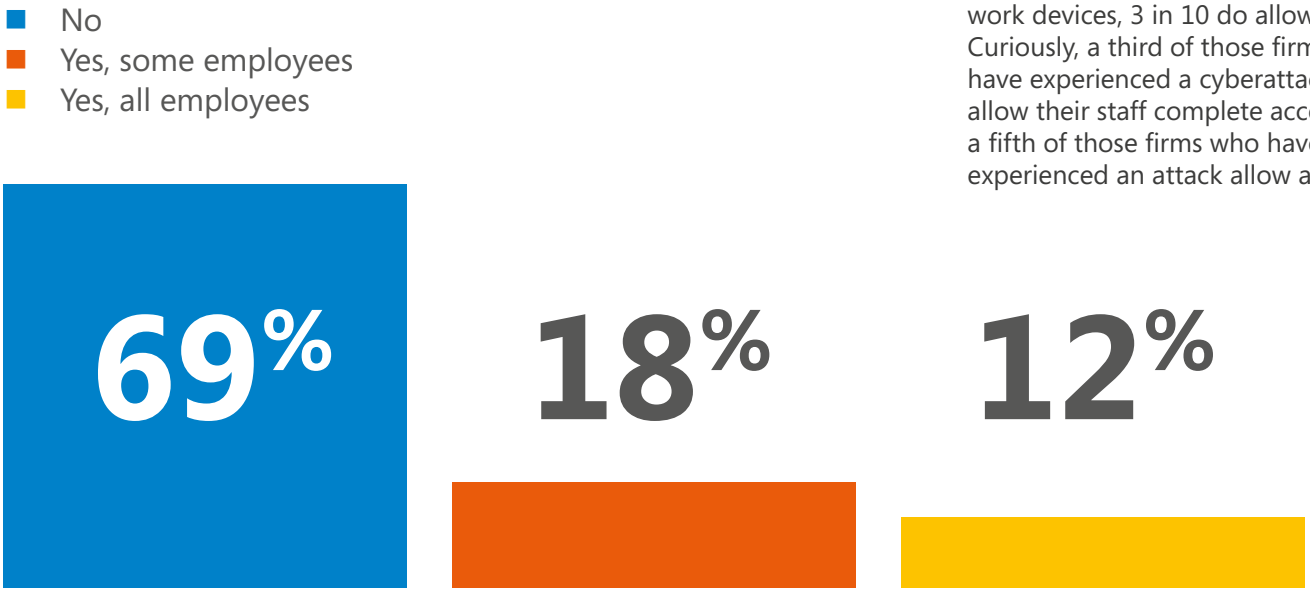
How worried are you that your employees could expose your company to digital secruity risks?



76%

are worried that employees could expose their company to digital security risks

Organisations allowing complete network access from personal/non-work devices

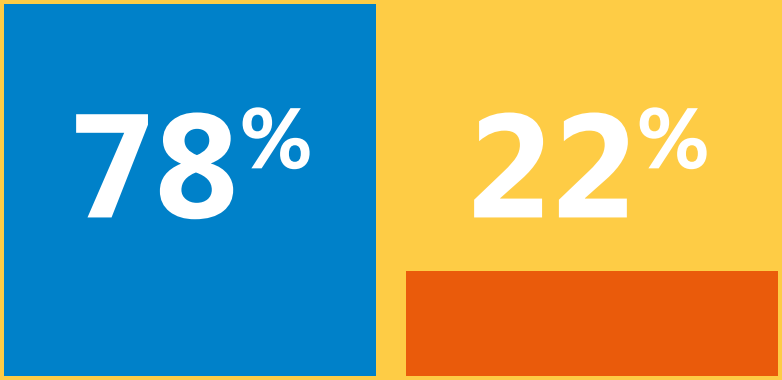


One area of cyber vulnerability identified in our previous research was the issue of personal devices in the workplace. While 7 in 10 firms do not allow employees complete access to their network from employees' personal or non-work devices, 3 in 10 do allow it. Curiously, a third of those firms who have experienced a cyberattack allow their staff complete access, but a fifth of those firms who have not experienced an attack allow access.

A related issue is working from home. The vast majority of firms (78%) have restrictions on employees' access to documents, email and other information relating to work when they work from home. But more than a fifth have no restrictions: rising to a quarter of those employing over 500 staff.

Does your organisation have restrictions on access to documents, email or other imformation relating to work when working from home?

- Yes
- No



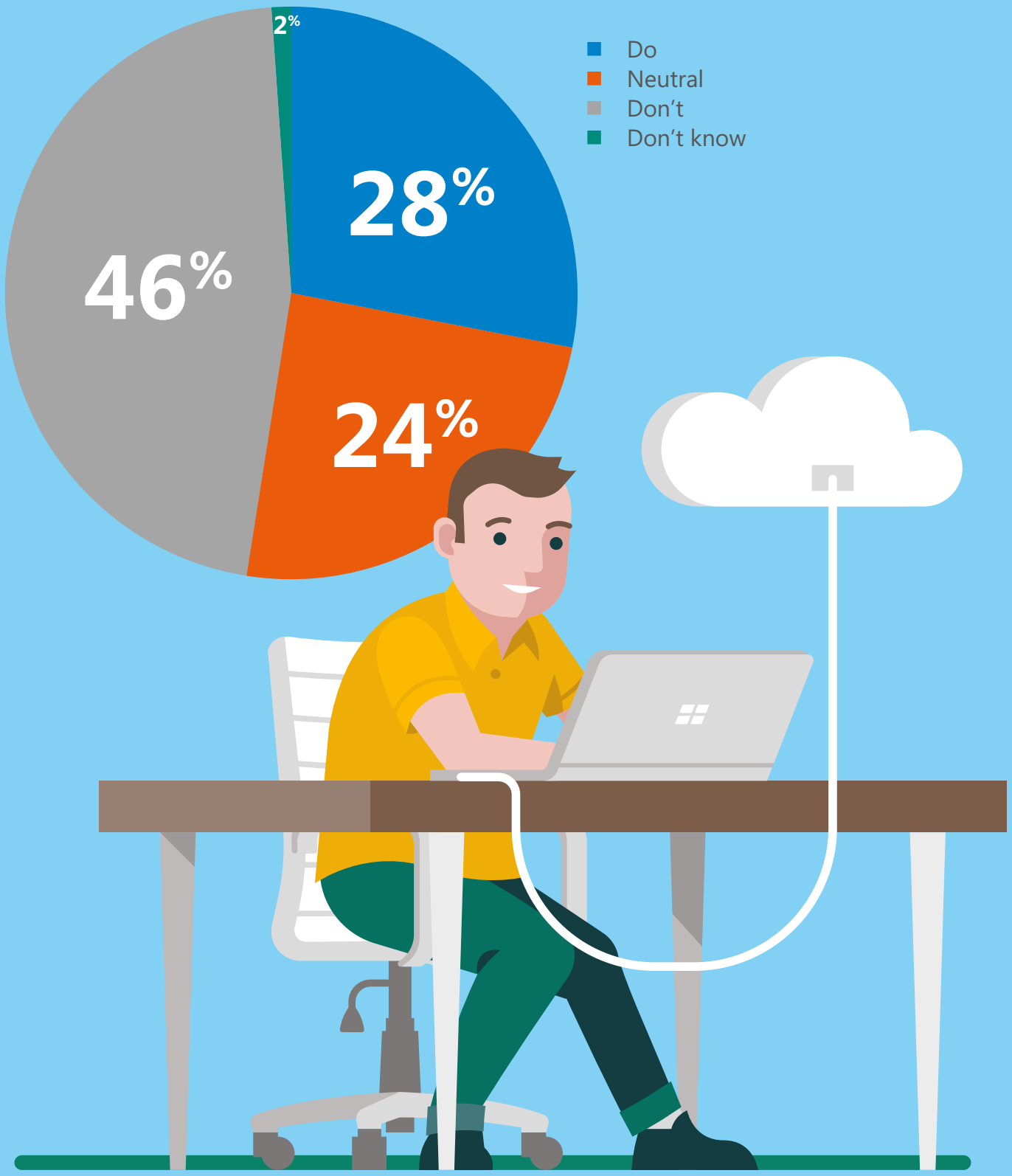
In our 2019 survey of employees in Ireland, 6 in 10 claimed to work from home, and half of these claimed to have no restrictions on access to work-related content from home.

For organisations responding to the need for information protection, typical issues include:

- **Data sprawl across devices, apps, cloud, and on-premises**
- **Lack of visibility into where sensitive data lives across the organisation**
- **Struggles conforming to new compliance regulations**

Many organisations are embracing cloud computing as a solution to many of their IT issues. But this can also be a source of worry for senior decision makers: only 16% agree strongly that 'we don't have any security concerns about running/ moving our data and systems in/ to the cloud': only 9% of those who have experienced a cyberattack are inclined to 'agree strongly' with this statement.

Companies with concerns moving data and systems to the cloud



KEY TAKE AWAY:

As firms seek to embrace flexible working patterns to meet changing employee preferences, the issues of personal devices, remote access and cloud computing will challenge even the most sophisticated organisations to balance flexibility with security.

Conclusions

We began by noting the growing threat posed by cybersecurity breaches on a global scale. But we also noted that cybersecurity isn't just an IT issue: it's a business issue.

Those firms that make the right investments in cybersecurity – for their employees as well as for their customers – will not only enjoy greater security in terms of day-to-day business operations, but they will also enjoy higher levels of staff and customer satisfaction as services remain secure, flexible and easy-to-use.

But we should also note the gaps that exist between employees' experiences of security in their firms and what employers say. Unless that gap is closed – and employees feel that their own cybersecurity resources and skills are properly developed – then the investments made in cybersecurity in the years ahead will not deliver their full potential to either the organisation, nor the employee.

Further Information

Enabling zero trust security

The widespread adoption of public cloud services and the growth of the mobile workforce have rendered perimeter-based security models obsolete. An organisation's applications and data are likely to exist both inside the traditional firewall and beyond it. Security and IT teams can no longer assume that users and their devices (both personal and corporate) on the network are any safer than those on the outside.

What's needed is a pivot to Zero Trust security where all users and devices—both inside and outside the corporate network—are deemed untrustworthy. Access is granted based on a dynamic evaluation of the risk associated with each request. The same security checks are applied to all users, devices, applications, and data every time.

Building Zero Trust into your organisation

A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements: identities, devices, applications, data, infrastructure, and networks. Each of these six foundational elements is a source of signal, a control plane for enforcement, and a critical resource to be defended. This makes each an important area to focus investments.

1. Identities – whether they represent people, services, or IOT devices – define the Zero Trust control plane. When an identity attempts to access a resource, we need to verify that identity with strong authentication, ensure access is compliant and typical for that identity, and follows least privilege access principles.

2. Devices - Once an identity has been granted access to a resource, data can flow to a variety of different devices—from IoT devices to smartphones, BYOD to partner managed devices, and on-premises workloads to cloud hosted servers. This diversity creates a massive attack surface area, requiring we monitor and enforce device health and compliance for secure access.

3. Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lift-and-shifted to cloud workloads, or modern SaaS applications. Controls and technologies should be applied to discover Shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behaviour, control of user actions, and validate secure configuration options.

4. Data - Ultimately, security teams are focused on protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organisation controls. Data should be classified, labelled, and encrypted, and access restricted based on those attributes.

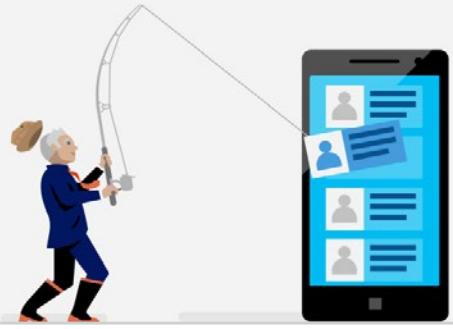
5. Infrastructure (whether on-premises servers, cloud-based VMs, containers, or micro-services) represents a critical threat vector. Assess for version, configuration, and JIT access to harden defence, use telemetry to detect attacks and anomalies, and automatically block and flag risky behaviour and take protective actions.

6. Networks - All data is ultimately accessed over network infrastructure. Networking controls can provide critical "in pipe" controls to enhance visibility and help prevent attackers from moving laterally across the network. Networks should be segmented (including deeper in-network micro segmentation) and real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

6 TECH TIPS TO STAY SAFE

Microsoft

We recommend these simple tips to keep your information safe and sound:



Avoid phishing scams.

If you don't recognise a link, don't click on it. Pay close attention to messages from supposed banks or credit companies, especially if they urge you to act immediately.

If you're the slightest bit suspicious, go directly to the official website to check the status, even if the mail is "personalised" with your name included.

Back up your data.

Protect your files from the bad guys using an encrypted cloud storage source like Microsoft's One Drive. If something happens to your device, you don't have to worry about losing your files or photos – they're all happily waiting in your OneDrive.

Looking for a new PC?

Make sure to purchase a modern device with a secure operating system like Windows 10 that has the latest security and feature updates, in tandem with built-in anti-virus protection, such as Windows Defender Antivirus. For more information, visit the Microsoft Store.

Be careful when using public networks.

1 in 5 people make online purchases over insecure Wi-Fi networks

Don't be that person!

If you are using public WiFi, make sure:

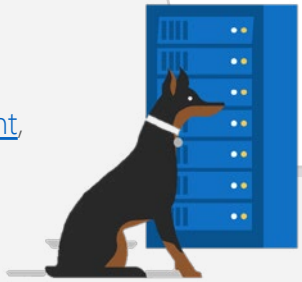
1. Your connection is encrypted and secure by looking for the lock icon in the top left of the address bar

2. You double check that the address you are navigating to is what you expected

Don't rely on passwords alone.

Use the Microsoft Authenticator app and Windows Hello for easy and secure sign in-to your Windows 10 device. Use your face or fingerprint to quickly log in across devices, apps and browsers without having to remember passwords.

Did you know? With a Microsoft Account, you can automatically sign in-to other Microsoft cloud-based applications like Bing, MSN, Xbox Live and Outlook.com



Further information

If you are looking for guidance on how to secure your business or to do a security assessment on your business, go to:

www.microsoft.com/en-us/security/security-fundamentals


Microsoft