SECURING THE FUTURE

The Cyber Security Climate in Ireland

An Amárach report for Microsoft

JANUARY 2019

Microsoft

amárach research

Des Ryan
Solutions Director, Microsoft Ireland

foreword

New Threats and Same Bad Habits Pose Serious Risk to Your Organisation.

Last year, new revelations and regulations underscored how critical data protection has become to all levels within any organisation. Over the last two years, we have seen the devastating WannaCry attack over 200,000 computers in 150 countries and last March 2018, an attack on the municipal government of Atlanta nearly grounded the city to a halt.

Now, the General Data Protection Regulation is fully in effect, with a package of financial penalties for organisations who do not comply. Irish organisations now face severe consequences for data loss or breach, due to a simple human error, a failure of process or falling victim to a cybercriminal. While organisations can invest in more robust data protection and security measures, it is their employees who can cause a potential disaster for their organisation.

Our research into large and medium Irish organisations reveals that poor, inconsistent security policies, processes or procedures, create bad habits amongst employees, which could compromise critical data and cause disruption with serious consequences.

foreword

Nearly half of organisations don’t continuously update policies, or train staff, or upgrade devices on a regular basis. Without proper training and oversight, expecting employees to always be vigilant is unrealistic. Our research shows employees make potentially dangerous assumptions and fall into bad habits when it comes to protecting data when at the office or working from home.

The most common and least detected sources of data breaches, however are compromised identities. Passwords can be hacked, guessed, leaked, or lost. New technologies like biometrics can deliver the robust security needed, and accompanied by consistent training, enforced policies, and better device upgrades, employees can deliver the productivity needed for successful transformation with a minimum of risk to the organisation.

Our experience (and this research) shows us that, organisations must now ensure they are taking a considered approach to data security. It is time to embrace new security procedures and technologies. Microsoft invests more than $1 billion every year in security to help build, protect and preserve critical data. As part of that investment, we pioneer innovative solutions and develop smart policies and strategic partnerships to help ensure that protections are in place to guard people from today’s threats while preparing for tomorrow’s.

We cannot protect ourselves with tools and tactics of the past. Whether you’re talking about products, businesses, elections, or even national public-sector operations – the only way to guard against today’s invisible weapons and risks is through intelligent and well-integrated technologies, practices and policies.

Des Ryan
Solutions Director,
Microsoft Ireland

Introduction

As the world becomes more and more connected and dependent on digital systems, the issue of cyber security has become more important for both individuals and organisations. With many high-profile security and data breaches occurring in recent years, cyber security has been thrust into the centre of media and public scrutiny; such as the 87 million Facebook users that were notified of having their data breached in April 2018, to the Equifax breach in the summer of 2017 leading to 143 million Americans having highly sensitive personal and financial information stolen.

In this atmosphere, Microsoft is seeking to conduct research into the current cyber security climate in Ireland. This research in particular focuses on the security of medium and large organisations, and the behaviour and attitudes of employees of these organisations in regard to technology and cyber security.

Securing the Future Executive Summary

Commissioned by Microsoft, we conducted the first ever survey of employees across the island of Ireland: interviewing over 700 employees, split between Republic of Ireland (500) and Northern Ireland (200) in large organisations of 100 or more staff. The research reveals that:

User Behaviour

- **Using the same password across different technology and services at work is commonplace (43%)**, as is recycling of old work passwords (38%).
- Those working from home are much more likely to engage in activities that may be a security concern compared to the average. For example:
    - 49% have used their personal email account/services for saving, editing, sending, or sharing work related documents (vs 32% overall).
    - 24% have accidentally shared work-related material with friends/family (vs 10% overall).
    - 73% use free WIFI for work purposes while away from work/home (vs 56% overall).

Security Conscious

- 30% of employees have been notified of a data breach and that their personal data had been accessed.
- **44% have experienced problems with phishing, hacking, cyberfraud or other cyberattacks**, with 31% reporting a problem happening in their personal life and 18% reporting problems at work.
- 54% say they receive cyber security training at least once a year, and those that work from home at least once a week more likely to regularly receive cyber security training.
- Biometric verification was broadly well received, with 62% of respondents saying they would welcome it; and half of respondents would welcome geo location verification. Dual access verification was received less positively, with 40% saying they would welcome it.

Legacy Devices

Legacy technology and devices can increase vulnerability.

- 34% of employees say their employer ensures technology is up-to-date and the best available, 18% say technology is upgraded regularly but they are not shown how to use it, while 47% say their technology is upgraded only occasionally or rarely.
- 26% say having the latest technology influences their decision to either accept a job offer or remain in their job.
- 11% say their laptop is old, and 7% that their laptop looks cheap/unstylish.
- 14% admit to secretly judging others on their laptops/devices.
- 25% admit to getting jealous when a colleague gets a new laptop.

Methodology

To conduct the research, we ran the first ever survey of employees across the island of Ireland: interviewing online a total sample of 700 employees, split between Republic of Ireland (500) and Northern Ireland (200). All respondents were employees of an organisation with *100 or more employees*. All respondents were required to use some form of device in the course of their normal working day, such as a desktop/PC, laptop, work smartphone, or work tablet. Fieldwork for the research took place in November 2018.

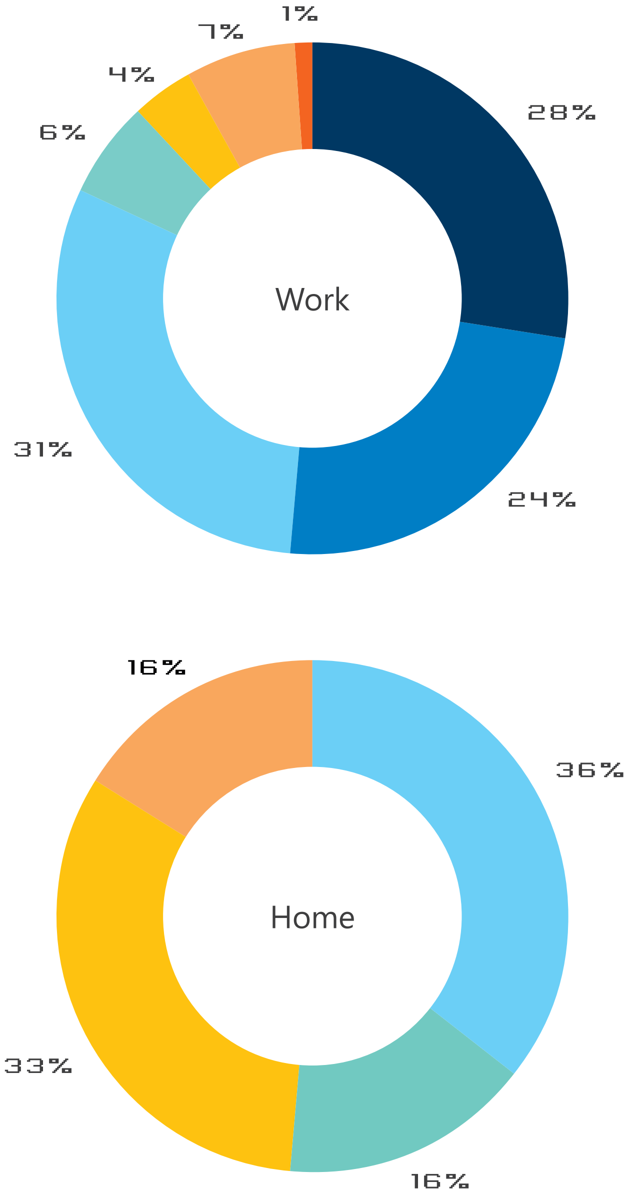
The research was broken down into three different sections, in order to help explore each of the key themes more thoroughly:

01 User Behaviour
02 Security Conscious
03 Legacy Devices

User Behaviour

In their work devices, respondents made use of a variety of security measures to keep them secure; 29% had a pin, 11% had fingerprint recognition, and 2% had facial recognition. However, passwords were predictably the most common, with 88% of respondents using one to secure their work device(s). Notably, 2% answered “None of the Above” for this question, suggesting they do not have any security on their device.

Conventional wisdom (though this is beginning to see changes) recommends changing your password regularly to ensure security. As can be seen in fig 1, 52% of respondents are required to change their work passwords at least every three months – however no respondents reported that they change their personal passwords this regularly.



🟦	Monthly
🟦	Quaterly
🟦	Several times a year
🟩	Once a year
🟨	Less often
🟧	Never
🟥	Don’t use passwords

Fig 1.

How often do you change your passwords?
Circa half of all respondents are required to change their work passwords at least every three months, respondents change their personal passwords more infrequently.
(Base: All respondents - 700)

> 43% of public and private sector employees in Ireland using the same password across different technology.

To remember their passwords, respondents typically relied on their memories for both work (77%) and personal (78%) passwords. **14% of respondents physically write down their work passwords**, and 8% keep them in a document on their computer.

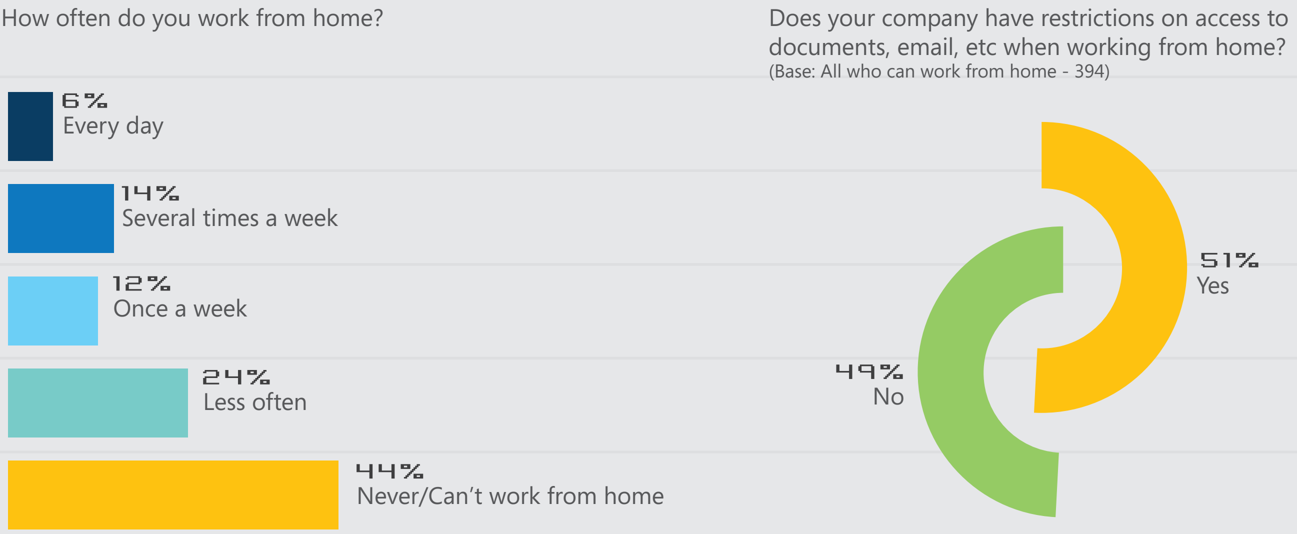
The reliance on memory to remember passwords could be detrimental to security, as human memory is a very finite thing. **When asked whether they use the same password across different technology and services at work, 43% of respondents admitted to doing so** (50% did so at home). The potential security risk this poses is exacerbated due to potential password recycling – to which 38% of respondents admitted to doing so with work passwords (44% with personal). Combining these issues suggests that quarterly password changes may only have minimal effects on improving security, as employees just cycle through old passwords or use increments of current ones – and their old passwords may still work on some legacy devices, or software that didn't synchronise it's password change.

Working from home

Working from home has become a much more viable component of the modern workplace, as technology has increasingly enabled a greater number of tasks to be completed remotely. To reflect this, 56% of respondents claim that they can work from home (at least sometimes), with 32% doing so at least once a week (fig 2). However, this evolution comes with some drawbacks, particularly in terms of security. 49% of respondents that can work from home at least once a week claim that their company has now restrictions on access to documents, emails, or other information relating to work at home (fig 2). This cohort that works from home, particularly those that work from home at least once a week, were found to be much more likely to engage in risky security behaviour.

Fig 2

56% of respondents work from home, and almost half of these have no restrictions on access to documents when working from home.
(Base: All respondents - 700)



01

User Behaviour Insights

Close to one third (32%) of respondents admitted to using their personal email account or services (Google Drive, iCloud, Dropbox) in relation to saving, editing, sending or sharing work related documents, and this rose to 49% amongst those that work from home at least once a week. 10% admitted to sharing work-related material with a friend or family member using their mobile or social media (increasing to 24% of those that work from home at least once a week); and 11% have had their friends or family access to their work devices (intentionally or unintentionally), rising to 25% of those that work from home at least once a week. While working from home is an important option to empower employees to be more flexible in their roles, it is also important to acknowledge that it exposes them and the organisation to more cyber security risks. Better security training and measures need to be implemented when considering enabling employees to take advantage of remote working.

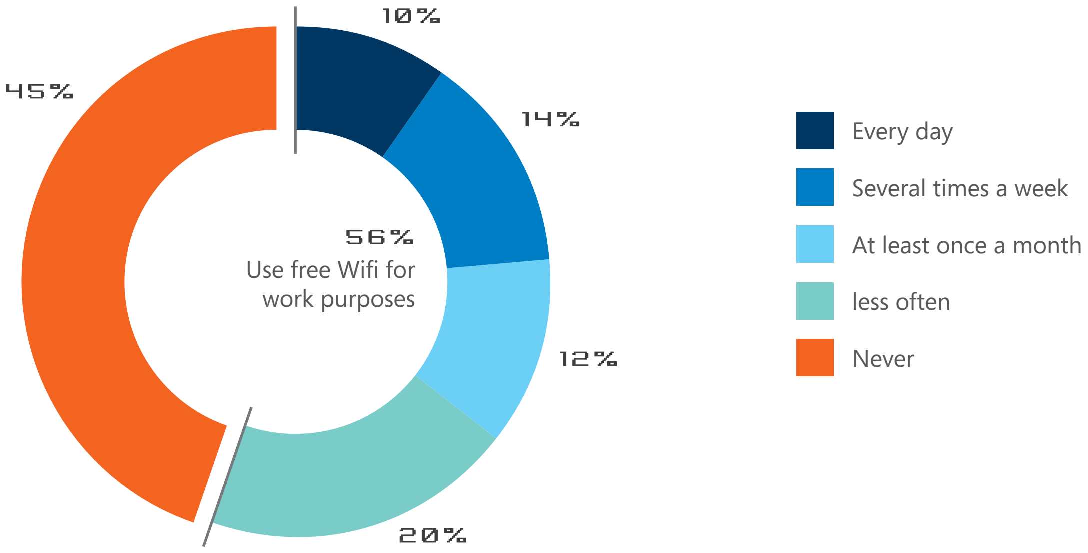
31% of respondents say their workplace allows them access to music/video streaming services for which they have a personal account while at work. While potentially not a priority concern, it is important that these sites are vetted first. Common sites such as Spotify and YouTube have an excellent reputation, however these are not the only streaming sites that exist, and concerns can arise from bespoke plugins being "necessary" to use the site, only for those plugins to contain malware, to potential hacking of the website itself and tracking user data through the browser.

Of greater concern is perhaps that 56% of respondents admitted to using free or public WIFI for work related purposes when they are away from work or from home (fig 3). Perhaps unsurprisingly, this figure increases for those that work from home at least once a week, with 73% of these respondents admitting to using free or public WIFI. This figure does not necessarily suggest that those who work from home are more likely to engage in risky behaviour, but is probably more reflective of the fact that they are exposed to riskier situations more often.

Fig 3

How often do you use free or public WIFI for work related purposes when you are away from work or from home?

(Base: All respondents - 700)



56% of respondents have used free or public WIFI for work related purposes when away from work/home, rising to almost 3 in 4 if those working from home at least once a week.

(Base: All respondents - 700)

	At least once a week (Base: 228)	Less often (Base: 166)	Never (Base: 306)
Every day	16%	9%	7%
Several times a week	25%	11%	6%
At least once a month	14%	13%	9%
Less often	18%	25%	18%
Never	27%	42%	60%

KEY TAKE AWAY

As more and more companies adopt smart working/flexible working practices with their staff, there is a growing risk that the behaviours of employees will have the unintended consequence of making their employers more vulnerable.

Passwords are a liability, pure and simple. They have become too easy to guess or steal. People today use a variety of devices, applications, and websites. Trying to remember a long list of strong passwords is becoming impossible. Our research has shown that most people use the same weak password across dozens of different accounts, services and devices, making a stolen password even more lucrative to criminals. Organisations need to enforce stricter password policies ensuring that they are complex enough to avoid being guessed. In the longer term, move towards alternative biometric verification as most employees would be in favour of it.

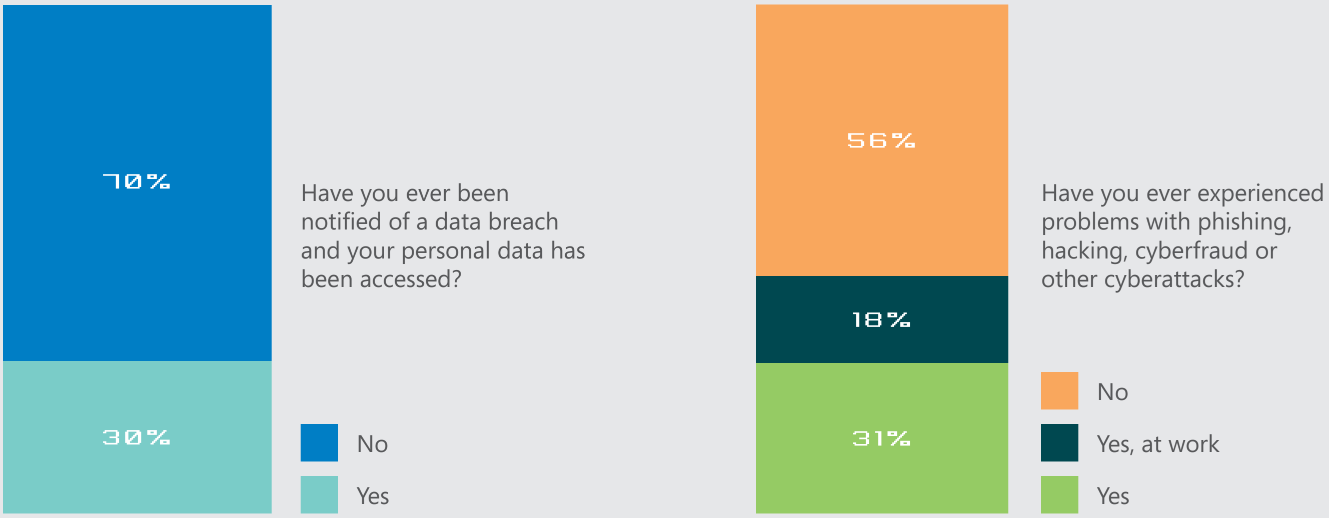
Security Conscious

Cyberattacks have become very common in today's world, and this is reflected in the research. 30% of respondents reported that they have been notified in the past of a data breach and that their personal data had been accessed (fig 6).

Furthermore, 44% have experienced problems with phishing, hacking, cyberfraud or other cyberattacks. 56% of those interviewed have accessed public Wi-Fi. If these devices do not have a secure Virtual Private Network (VPN) channel, they are left wide open to a hacking attack.

3 in 10 have been notified about a breach of their personal data, and 44% have experience problems with phishing, hacking, cyber fraud or other cyber attacks.
(Base: All respondents - 700)

Fig 6

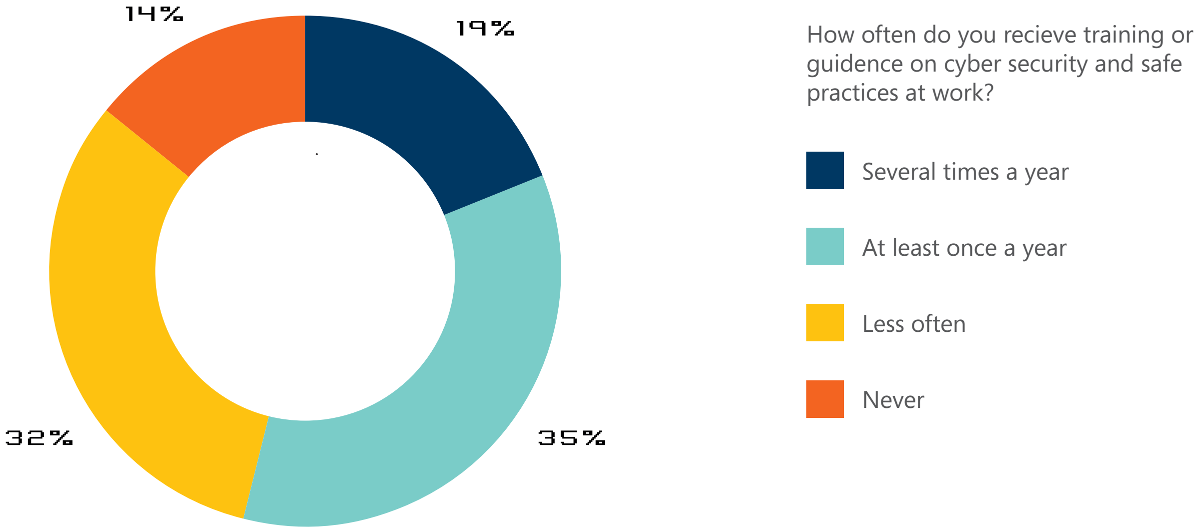


IT and security professionals may be shocked to see that "low" number – as many large organisations see daily attacks on their system. These statistics highlight that IT are performing their role quite well, sheltering the employees from the brunt of the attacks, however the fact that some get through highlights the need for consistent training among all levels of the organisation.

> 46% of public and private sector employees in Ireland have had no training in last 12 months on combatting cyberattacks.

Fig 7

54% of respondents receive cyber security training at least once a year.
(Base: All respondents - 700)



	At least once a week (Base: 228)	Less often (Base: 166)	Never (Base: 306)
Several times a year	27%	16%	15%
At least once a year	39%	37%	30%
Less often	27%	35%	34%
Never	7%	11%	21%

54% of respondents reported that they receive training or guidance on cyber security at least once a year (fig 7), rising to two thirds (66%) of respondents who work at home at least once a week. This cohort were identified as part of this research as being particularly susceptible to risky behaviour. Focus should be placed on this cohort to improve their understanding of security best practices; however, it appears that the current training regimen is insufficient and could be revised.

In addition to improving training, new verification techniques can be introduced to overcome some of the shortcomings of passwords.

> 44% of public and private sector employees in Ireland have been victims of cyberattacks.

Fig 8

Circa 3 in 5 would welcome biometric verification, and half would welcome geolocation as security alternatives to passwords in the future.
(Base: All respondents - 700)

	Would not welcome	Would not welcome at all	Would welcome completely	Would welcome	Neither/Nor
Biometric verification	8%	7%	32%	30%	23%
Geo location verification	10%	11%	27%	23%	30%
Dual device access	15%	12%	21%	19%	32%

Fig 8 highlights that employees are open to the introduction of more secure alternatives, with 62% of respondents saying they would welcome biometric verification, half (50%) saying they would welcome geolocations, and 40% would welcome dual device access.

However, just 15% would not welcome biometric verification, 21% wouldn't welcome geolocation, and 27% wouldn't welcome dual device access – highlighting that there is relatively low resistance to their introduction.

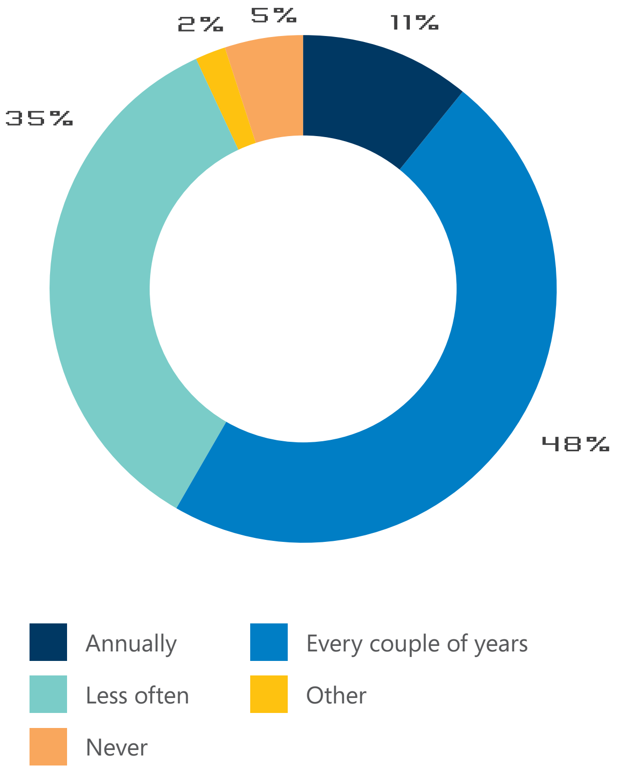
KEY TAKE AWAY

We are at the early stages of a security revolution in our organisations, and a key finding from our study is that Irish employees are enthusiastic about the potential to move away from dated and risky password practices as they face an ever evolving threat from sophisticated hackers and a changing regulatory landscape.

Legacy Devices

Fig 4

How often are laptops/PCs/tablets upgraded/replaced at work?



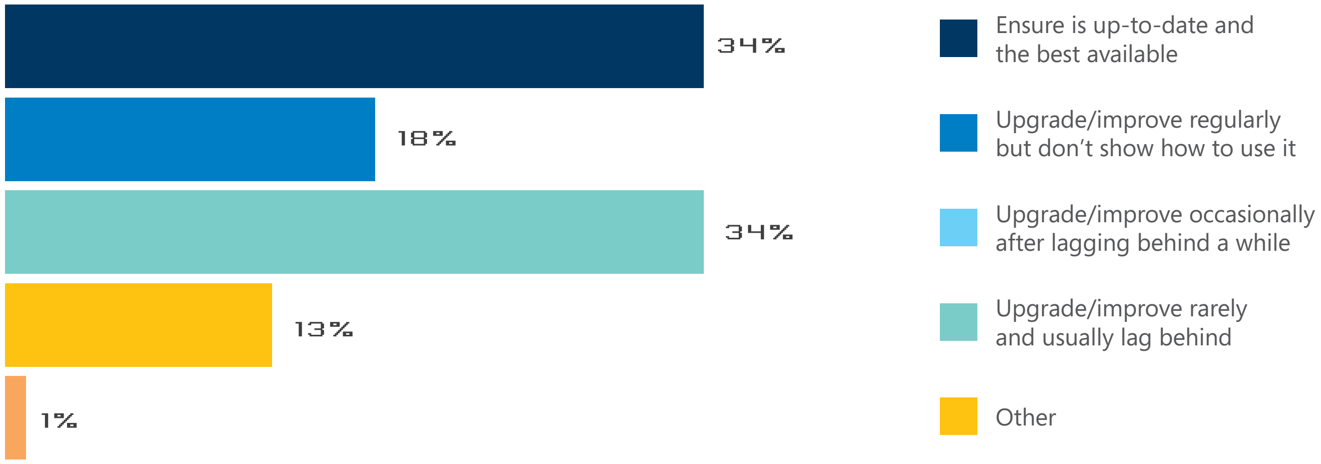
1 in 3 claim their workplace ensures technology is up-to-date and the best available, and 1 in 5 claim technology is updated regularly, however they aren't shown how to use it.

(Base: All respondents - 700)

Legacy devices can be of great concern to security advisors. As technology ages, new vulnerabilities are identified and can be exploited. To avoid this, it is often a priority to ensure all software and hardware are as up to date as possible, so that these vulnerabilities can be fixed once discovered.

Fig 4 asked respondents about how often their work devices (PCs, laptops, tablets) are upgraded. 11% of respondents claimed they were upgraded annually, however the majority (48%) reported that their devices were upgraded every couple of years. When considering their employer's attitude towards upgrading, 47% of respondents described their attitude as upgrading occasionally or rarely after lagging behind. 18% described their employer's attitude as wanting to upgrade regularly, however they don't show employees how to use the new technology.

47% of respondents described their attitude as upgrading occasionally or upgrading rarely after lagging behind.



In addition to their work devices, many employees will also have equivalent devices available at home. When asked whether their personal devices at home are better than their work devices, 50% of respondents reported their home device was superior. Of those with a superior device at home, **28% used this device to work on sensitive files or projects by sending the file from their work device to their home device.** However, 35% of respondents reported that their workplaces allow them to use their personal device for work purposes.

When asked whether they plugged devices into their work device that were not from their company, **25% of respondents admitted to connecting USB thumb drives, 12% connected back-up drives**, and 5% connected a smartphone that didn't belong to them. Additionally, 40% of respondents store client files/work on the desktop of their work device.

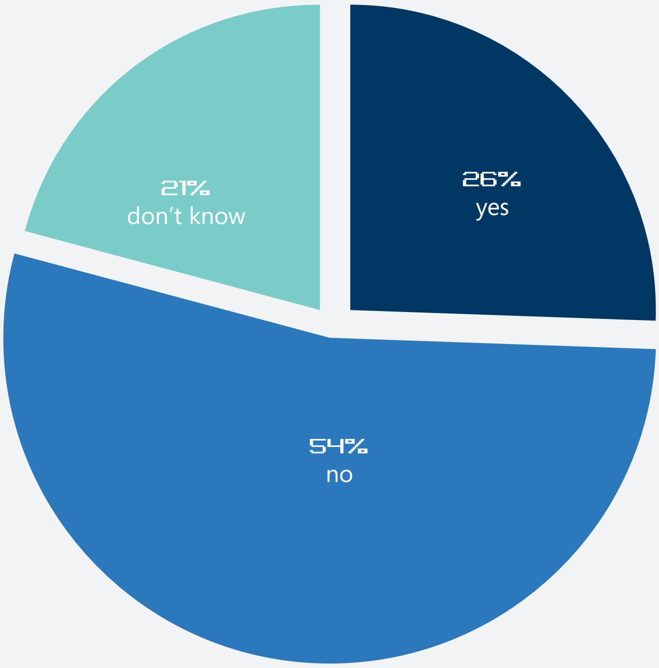
Without a clear and enforced security policy in place that is clearly communicated to employees, the research shows there is a significant risk to breaching the General Data Protection Regulation (GDPR). This could have potentially severe implications for organisations found to have flouted these regulations. Remember, the fines for non-compliance can be up to four percent of your organisation's annual global revenue or up to €20 million in fines.

Technology nowadays is often seen as a fashion statement, with people taking pride in showing off their latest devices. However, when it comes to work devices, employees are not overly concerned with this. 11% said that they have been embarrassed about their laptop in meetings as it is old, and 7% because it looks cheap/not stylish. 14% said they judge others on their laptop or devices, and 25% get envious when a colleague gets a new laptop.

> Half of of public and private sector employees in Ireland claim their personal device is better than their work device.

Fig 5

Would having the latest technology influence your decision to either accept a job offer or remain in your job?



A quarter of respondents say that having the latest technology would influence their decision on accepting job offers
(Base: All respondents - 700)

Technology also plays a role in job decisions taken by employees. 26% of respondents (fig 5), a not insignificant amount, report that having the latest technology would influence their decision to either accept a job offer, or remain in their current job, with 21% saying "don't know".

KEY TAKE AWAY

As Digital Culture within organisations grows to enable successful transformation or organisations, the boundaries between home and work lives and devices blurs. It will be crucial to enable employees to be more productive on the go and support them with both training and policies that will protect them against data loss.

It will be increasingly important that employers upgrade their hardware and software to ensure optimum levels of security but also to demonstrate a commitment to current and prospective employees that they are willing to invest in the best and ensure that all steps are taken to guarantee device security, facilitate the development of a productive Digital Culture.

Conclusions

We began by noting the growing threat posed by cybersecurity breaches on a global scale. Our research shows that the weakest link in the battle against hackers and other digital threats is not software or hardware but people.

Habits can be good or bad, and too many employees have bad habits when it comes to passwords, the inappropriate use of personal tech and risky behaviour on networks outside the workplace. If anything, our research highlights the need for greater involvement by the HR department alongside the IT department in Irish organisations in order to avoid ‘bad habits’ by improving security for employers and equip employees with the skills and resources that help form good habits.

The good news from our study is that employees are aware of the risks some of them take and open to alternative practices and procedures that will reduce risk. The task for senior management is to use this awareness and goodwill to secure their future against a growing menace.