REPORT

proofpoint®

PEOPLE-CENTRIC CYBERSECURITY:

A STUDY OF IT LEADERS IN THE UK & IRELAND

EXECUTIVE SUMMARY

With the global shift to remote working, the cyber threat landscape continues to evolve across Europe, and the UK&I is no exception. Employees have been working outside the usual security procedures they face in the office, and cybercriminals are all too aware of this.

Whether it's from email-based threats, such as Business Email Compromise attacks (BEC), compromised cloud accounts or debilitating ransomware attacks, cybercriminals are aware that employees can be easily tricked. Using social engineering techniques, attackers can steal credentials, siphon sensitive data, and fraudulently transfer funds. Employees across all job levels and functions can put your business at risk in numerous ways, from using weak passwords and sharing credentials to clicking on malicious links and downloading unauthorised applications.

To address this, organisations need total visibility into how often they are being targeted, the risks these attacks pose, and how prepared they – and more importantly, their workforce – are to defend against them.

To better understand how people-centric cyber attacks are impacting organisations in the current climate, Proofpoint commissioned a survey of 150 CISOs/CSOs across the UK and Ireland, from a range of industries in December 2020. The study, conducted by Censuswide, explored several key areas, including:

- The nature and frequency of cyber attacks
- The level of employee and organisational cyber preparedness
- The impact of the global shift to remote working on security teams
- How organisations are preparing for the future threat landscape

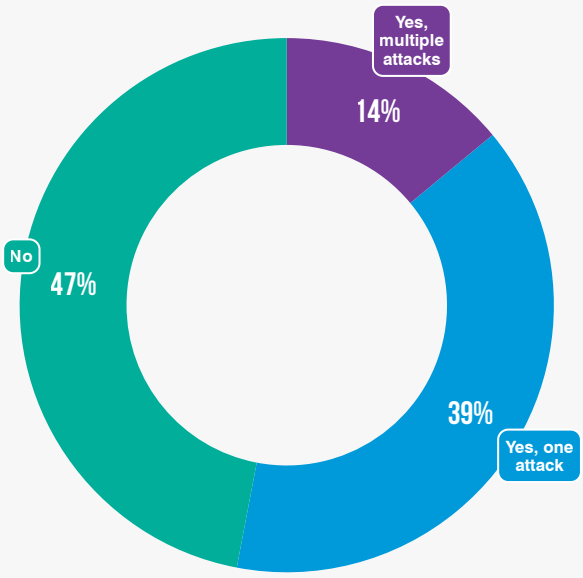
The study found that the need to protect people from imminent threats has never been greater, with a large share of organisations in the UK&I experiencing more than one significant cyber attack last year. It also highlights, among other key insights, that from board-level buy-in to upping cybersecurity awareness training, UK&I businesses are taking steps to shore up their cyber defences.

FINDING 1: ORGANISATIONS IN THE UK&I FACE A RANGE OF COMPLEX CYBER THREATS

Like their counterparts across the globe, organisations in the UK&I are under near-constant threat from cybercriminals.

Our survey revealed that **53%** of organisations in the UK&I suffered at least one significant cyber attack in the last 12 months. **14%** reported multiple incidents with over a third (**39%**) only experiencing one.

Has your organisation been victim of a significant cyberattack in the past 12 months?

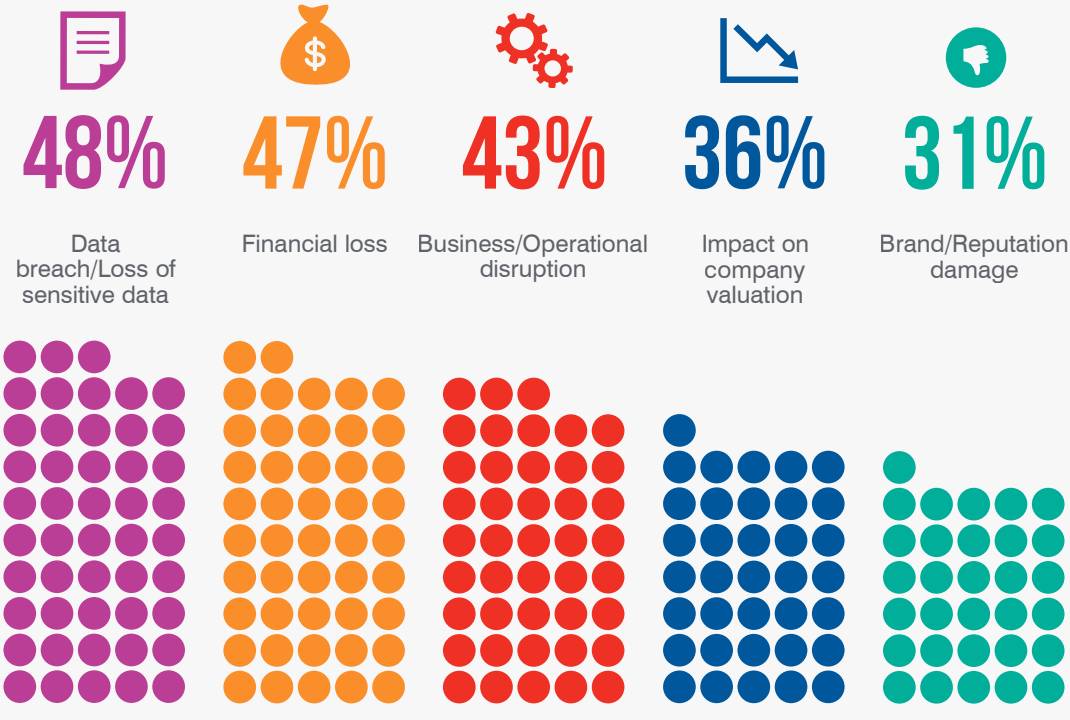


Data breach and financial loss are the primary consequences of successful cyber attacks in the UK&I

Cyber attacks can have devastating consequences for the organisations involved. The World Economic Forum estimates that between 2019 and 2023, $5.2tr in global value will be at risk from malicious actors. These losses arise for several reasons, from revenue disruption, downtime, legal fees, compensation and remediation, damage to brand valuation, and more.

CSOs and CISOs in the UK&I see a data breach (**48%**), financial loss (**47%**) and business disruption (**43%**) as the biggest consequences of a cyber attack. Over a third of CISOs (**36%**) cited an impact on company valuation as a consequence to a cyber attack.

What were the consequences, if any, for your business after suffering a cyber attack? (Tick all that apply)



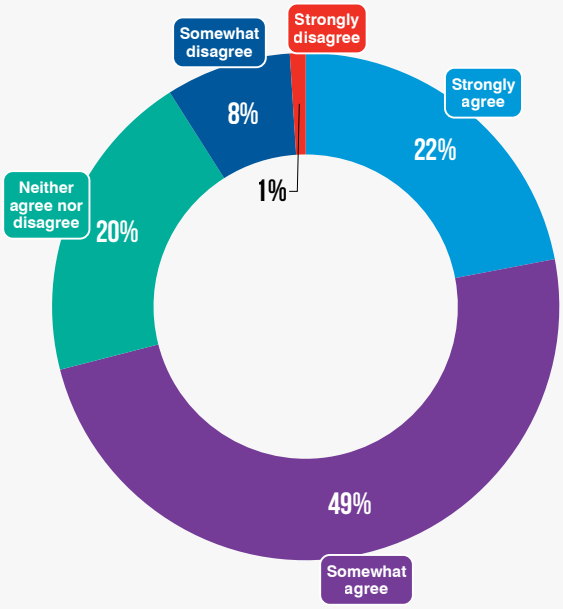
FINDING 2: ENFORCED REMOTE WORKING BRINGS NEW CHALLENGES FOR CYBERSECURITY TEAMS

Mass migration to remote working in reaction to the global COVID-19 pandemic has increased pressure on cybersecurity teams. Tasked with defending a larger and more complex attack surface, many admit they are struggling to make the transition.

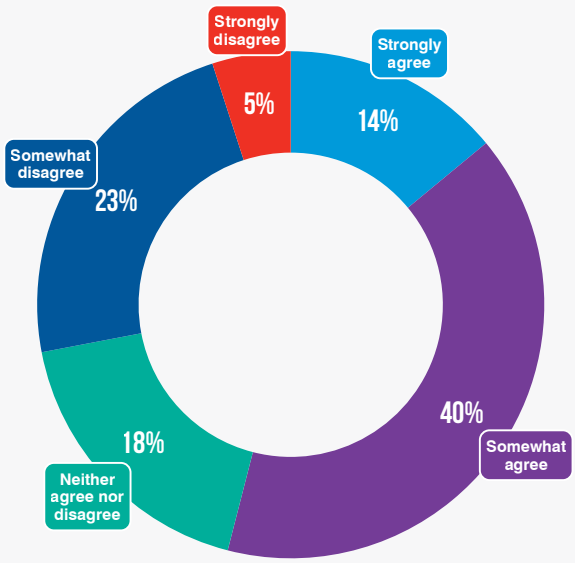
Just over one-fifth (**22%**) of CSOs/CISOs in the UK&I strongly agree that employees are well-equipped to work remotely, with almost half (**49%**) somewhat in agreement.

The new, distributed workforce has also brought poorly secured systems and applications to light. Over half of CSOs and CISOs in the UK&I (**54%**) agree that the switch to remote working has rendered systems and applications outdated when attempting to defend against today's cyber threats.

Our employees are correctly equipped to work remotely



The shift to remote working has made our systems and applications outdated to defend against today's cyber threats



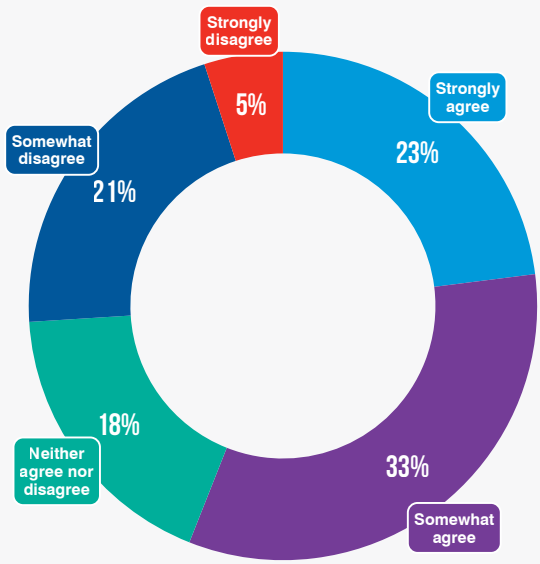
Cybercriminals are exploiting increasingly vulnerable remote workforces

The struggle to maintain comprehensive cyber defences with a larger remote workforce has not gone unnoticed by cybercriminals. Many are also actively using coronavirus-related lures (initially related to infection, now often relating to the vaccine) to phish credentials and other sensitive information from unsuspecting victims.

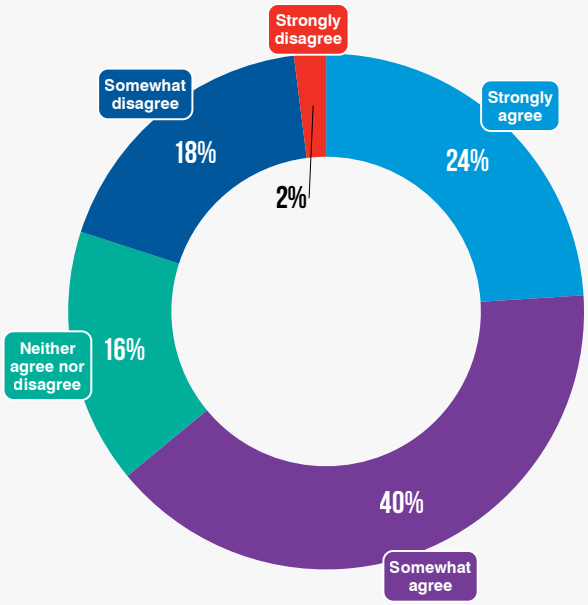
When asked if they have seen an increase in attempted phishing attacks since implementing a policy of home working, over half of CSOs/CISOs (**56%**) agreed. Only **5%** strongly disagreed.

An increased attack surface and rising numbers of attacks have left CSOs/CISOs in the UK&I feeling that their organisations are increasingly exposed. Two-thirds (**64%**) of CSOs and CISOs in the UK&I agree that implementing a remote working policy has left their business more vulnerable to cyber threats, with just **20%** in disagreement.

We have seen more targeted phishing attacks since implementing a policy of widespread remote working due to the Covid-19 pandemic



The shift to remote working has made our business more vulnerable to cyber threats



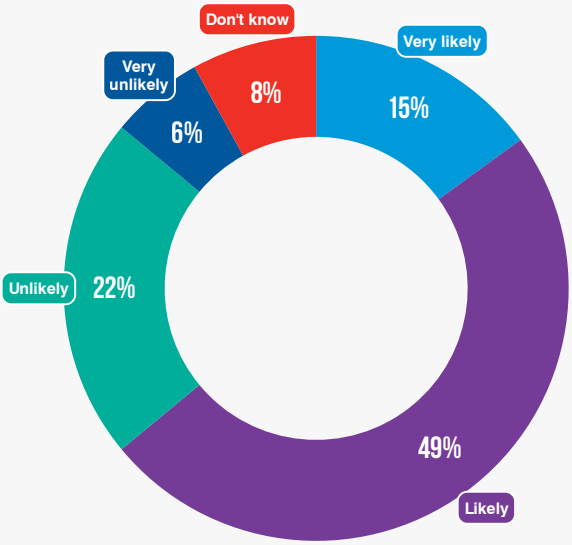
FINDING 3: ORGANISATIONS IN THE UK&I ARE AWARE OF THE RISK THEY FACE – BUT STILL FEEL UNDERPREPARED

Organisations in the UK&I are acutely aware of the risks they face from across the broad modern cybersecurity landscape and understand how cybercriminals are targeting their business.

Our study reveals that **64%** of CSOs and CISOs in the UK&I believe that their organisation is at risk of cyber attacks in the next 12 months. Interestingly, this jumped to **89%** amongst CSOs and CISOs from organisations over 2,500 employees and **83%** from organisations over 5,000 employees.

That said, the fact that over a quarter (**28%**) believe an attack is unlikely is cause for concern, especially when looking at the data across verticals: least worried of the likelihood of a cyber attack were manufacturing (**40%**), healthcare (**36%**) and public sector and education (**33%**), sectors that made headlines in 2020 for suffering devastating cyber attacks.

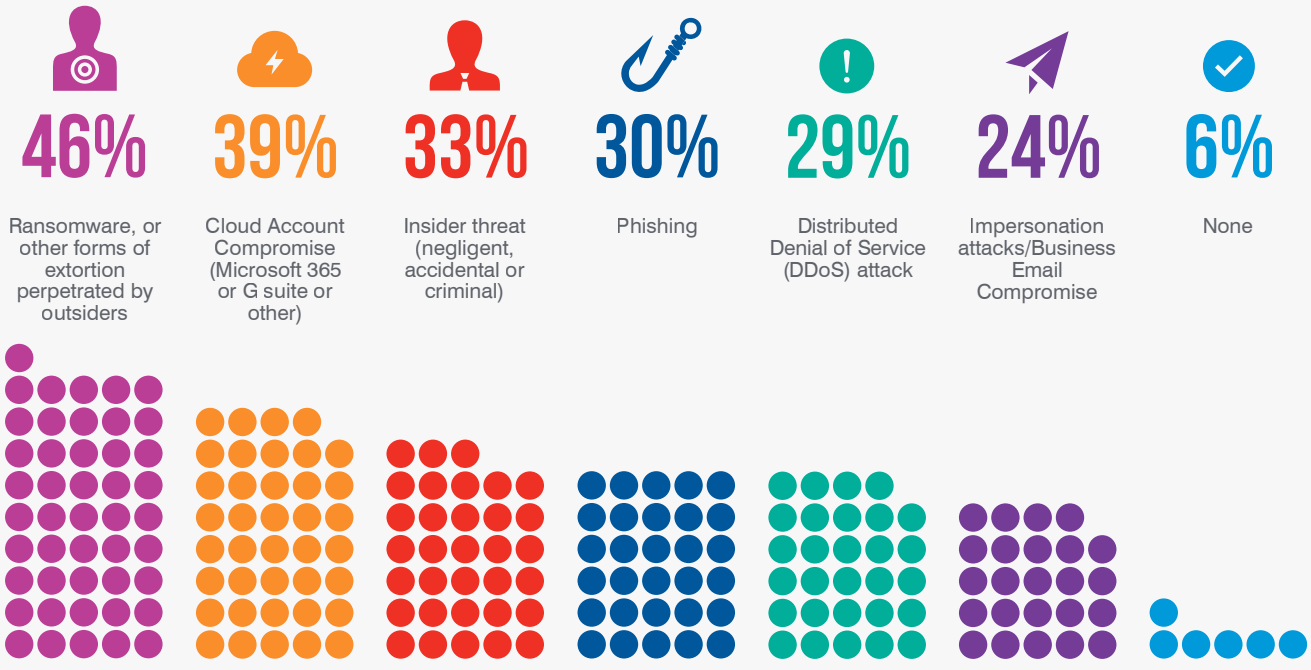
Do you feel at risk of being targeted by a cyberattack in the next 12 months?



Ransomware continues to cause concern

Ransomware remains the major threat keeping CISOs awake at night.

What, if anything, do you consider to be the biggest cybersecurity threats within your organisation in the next year? (Tick up to three)



Our research found that in the next 12 months, **46%** of CSOs and CISOs in the UK&I believe that ransomware, or other forms of extortion perpetrated by outsiders will be the biggest cybersecurity threat to their organisation. This was followed by cloud account compromise (**39%**), insider threats (**33%**), and phishing (**30%**).

These predictions align with current trends. Cybercriminals are increasingly using compromised credentials to access email accounts, sensitive information, and corporate systems. Credentials are often phished via email – a method of attack that remains alarmingly effective.

Proofpoint research has revealed that almost one in four people who receive a phishing email will open it, with over **10%** admitting to clicking on malicious links contained within.

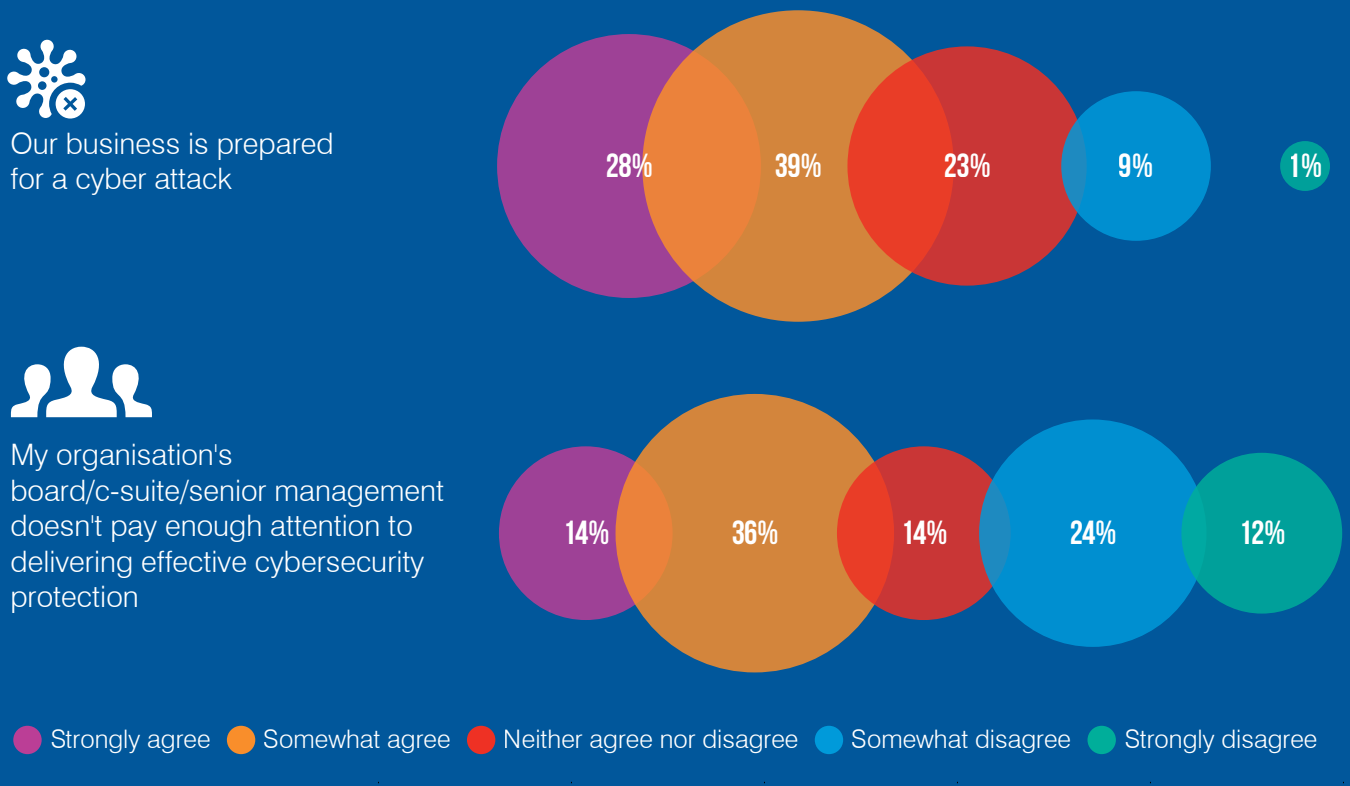
Worryingly, less than a quarter (**24%**) of CISOs/CSOs in the UK&I consider impersonation attacks and Business Email Compromise (BEC) attacks as the potential biggest cyber threat to their organisation in the next year. With attacks such as these quickly becoming one of the most expensive cyber threats globally – the FBI estimates the losses due to which at $26.5 billion over three years – this could indicate the IT leaders in the region are not correctly understanding the risk.

Cyber risk awareness and the C suite

While it's encouraging that the majority of IT leaders are showing such awareness of the risk and challenges they face, what is surprising is the perceived lack of concern shown by senior leaders across the organisation about their cybersecurity posture.

Half (**50%**) of CSOs/CISOs in the UK&I agree that their organisation's board and senior management do not pay enough attention to cybersecurity protection. Despite this, **28%** strongly agree that their business is prepared for a cyber attack.

To what extent do you agree or disagree with the following statements?

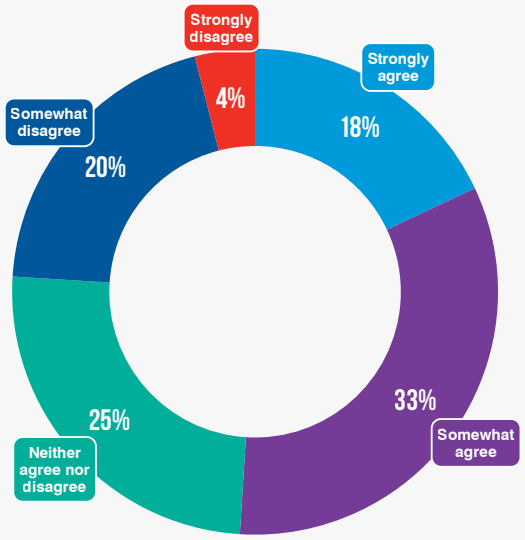


FINDING 4: EMPLOYEES ARE NOT EQUIPPED TO COMBAT CYBER ATTACKS

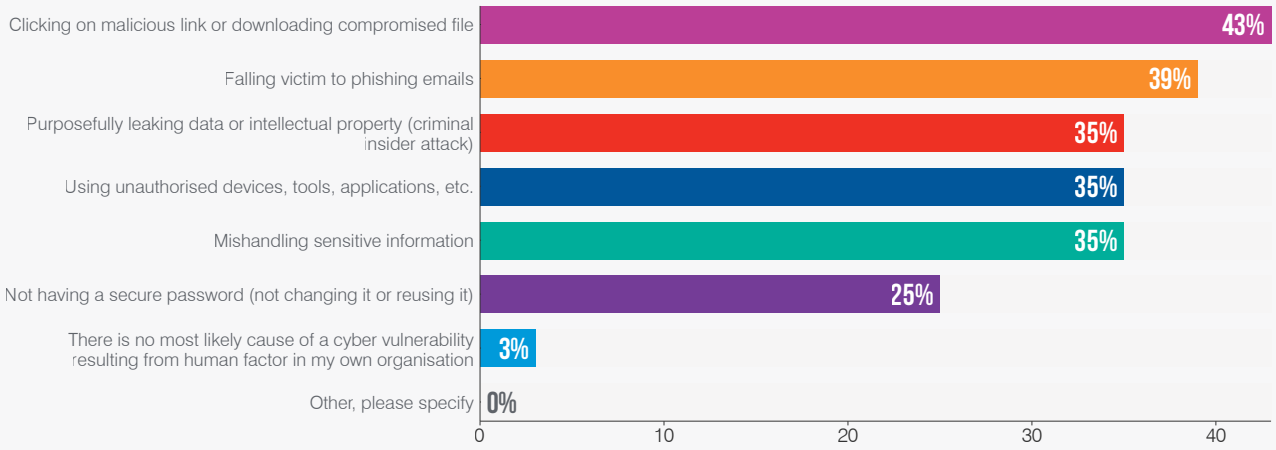
Despite end-users forming a last line of defence against cyber attacks, security knowledge and awareness is found to be lacking among the UK&I's workforce. CSOs/CISOs are well aware of this hole in their defences – in fact, over half (**51%**) agree that human error is the biggest vulnerability in their organisation.

Common employee behaviours likely to result in cyber vulnerability include clicking on a malicious link or downloading a compromised file (**43%**), followed by falling victim to phishing emails (**39%**), intentional leaking of data (**35%**), use of devices and applications (**35%**), and mishandling of sensitive information (**35%**). The fact the statistics behind these human actions are fairly close, indicates that a compromise can come from any of the listed channels, making it extremely hard for CISOs/CSOs to predict what actions may trigger an attack.

Human error is my organisation's biggest vulnerability



What, if anything, is the most likely cause of a cyber vulnerability resulting from the human factor in your organisation? (Tick up to three)



Insider threats on the rise

As aforementioned, when asked what they consider to be the biggest risk to their organisation in the next year, a third (**33%**) of CISOs/CSOs from UK&I organisations see insider threats as the key attack vector.

Globally, insider threats are a growing concern for businesses, with the number of incidents up by 47 percent in just two years. The 2020 Ponemon Institute Cost of Insider Threats report shows that companies in Europe experience high levels of contractor negligence, criminal insider threats, and credential theft.

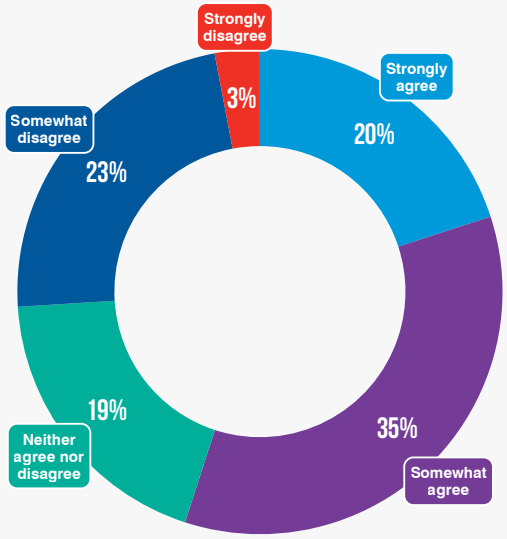
FINDING 5: EMPLOYEE CYBER AWARENESS IN THE SPOTLIGHT

CSOs/CISOs in the UK&I display a keen awareness of common threats and points of attack. Over half (**55%**) believe that, despite all other security protections, it is human error and lack of cybersecurity awareness that present the most significant risk to organisations.

While IT leaders in the UK&I are aware of the risk employees may pose to their business, they are not aware who their most targeted individuals are. When asked if they knew who the most at-risk employees in their organisation were, almost half (**44%**) said that they did not know.

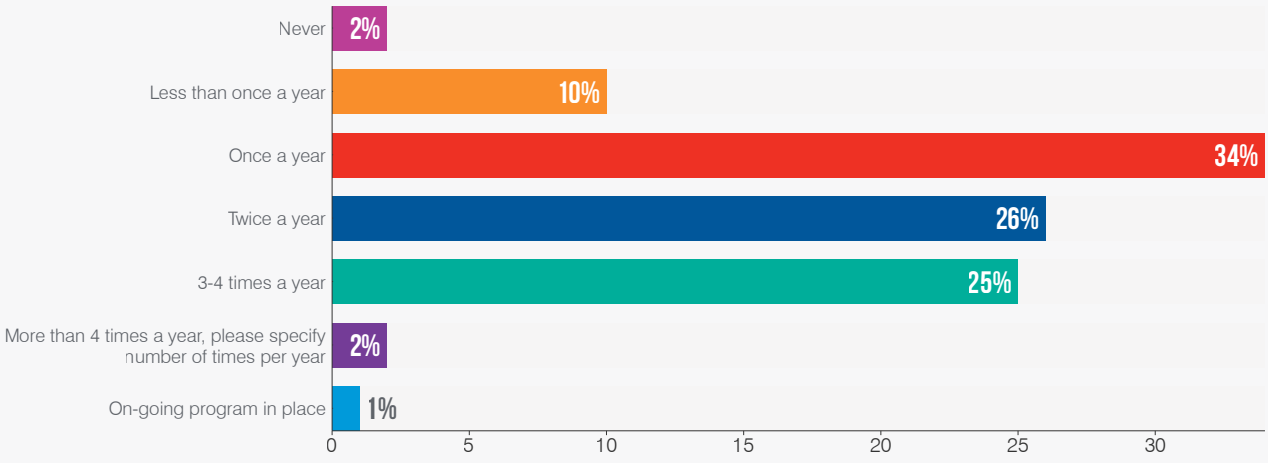
However, this level of awareness is not reflected in many UK&I organisations' cybersecurity awareness training programs, or lack thereof. Despite facing a fast-evolving threat landscape, the majority (**72%**) admitted to training their employees on cybersecurity best practices as little as twice a year or less, with only **28%** running a comprehensive program three times a year or more.

No matter what cybersecurity solutions are put in place, human error/lack of cybersecurity awareness (by employees or third parties within my ecosystem) is the biggest risk for my organisation



Promisingly, however, a number of organisations are adapting their cybersecurity awareness training in line with the current pandemic-related pressures, with **76%** saying they have given employees additional education on how to stay secure while working remotely.

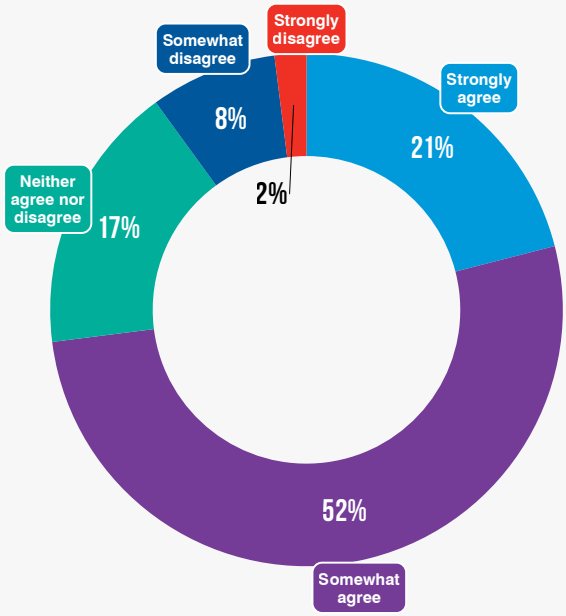
On average, how often, if at all, do you train your employees on cybersecurity awareness/best practices?



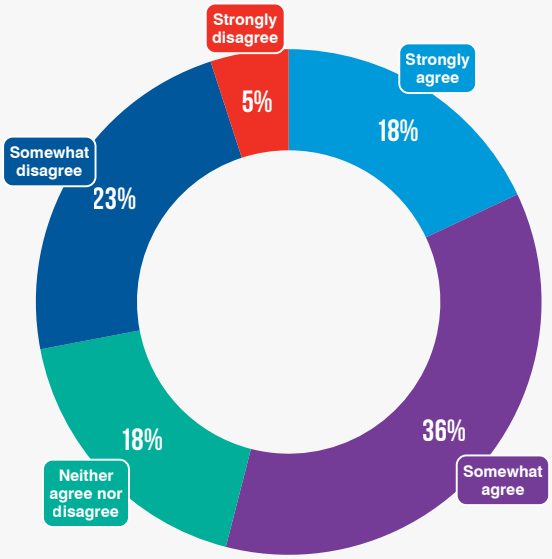
Regular and comprehensive training is vital to cybersecurity defence. All programs must be continually reviewed to ensure they remain relevant and keep pace with the evolving threat landscape.

Employee awareness is a cause for concern for many IT leaders in the UK&I. Almost three-quarters (**73%**) assert that their company's cybersecurity training program requires improvement. Unfortunately, however, over half (**54%**) believe that a lack of time and resource is the biggest obstacle in achieving this aim.

Our cybersecurity awareness training program needs to be improved to be more efficient



Lack of time/resources is the biggest obstacle to a more effective cybersecurity awareness program within my organisation



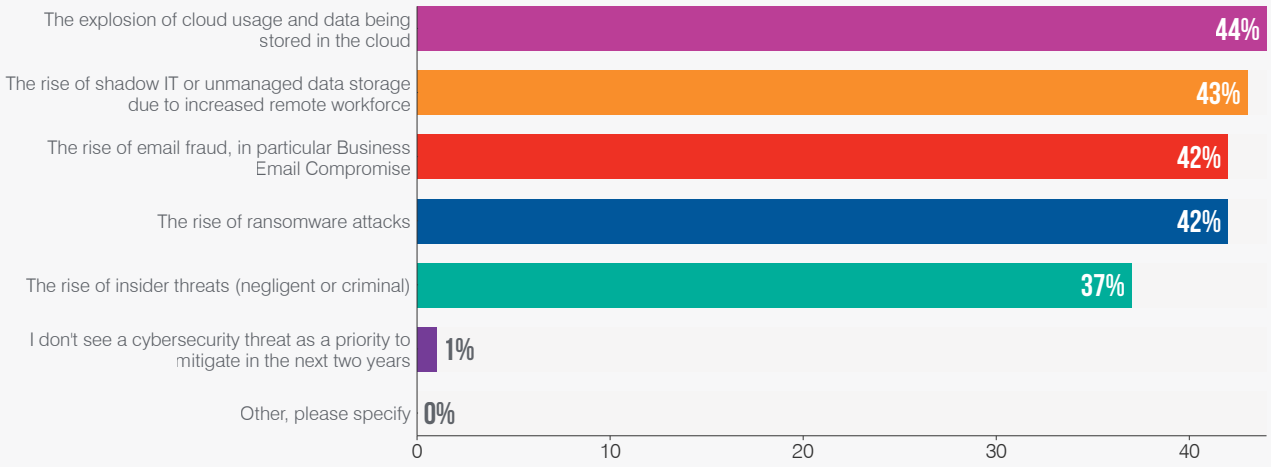
Regular and comprehensive training is vital to cybersecurity defence. All programs must be continually reviewed to ensure they remain relevant and keep pace with the evolving threat landscape.

FINDING 6: EVOLVING ATTACK VECTORS AND ADAPTED CYBER STRATEGIES IN 2021

Looking ahead, as we embark on another year of sustained remote working, **44%** of IT leaders in the UK&I believe that the explosion of cloud usage and data being stored in the cloud is likely to be one of the biggest cybersecurity threats to mitigate in the next two years. This is followed closely by the rise of shadow IT or unmanaged data storage due to increased remote workforce (**43%**) and the rise in email fraud, in particular Business Email Compromise (BEC) attacks (**42%**).

This suggests that senior security leaders see a multitude of threats targeting them with little clarity as to what attack vector they ought to prioritise, which makes it difficult for teams to action a clear defence strategy, increasing already high stress levels.

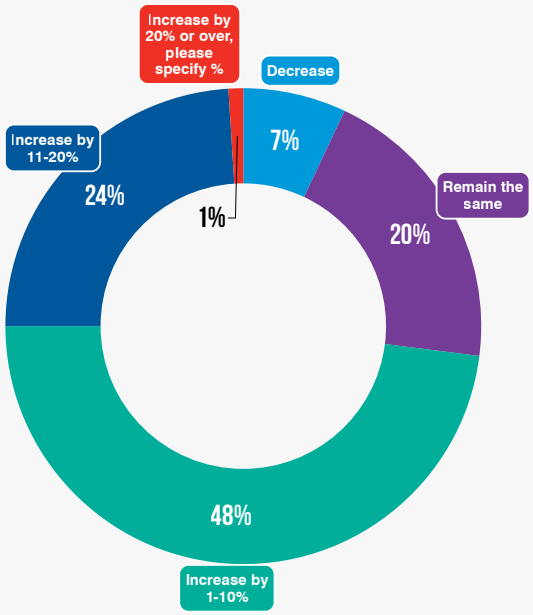
Beyond your organisation, which cybersecurity threat do you see as a priority to mitigate in the next two years? (Tick up to three)



This evolving threat landscape calls for a shift in cyber defences and constant re-assessment of an organisations' strategic priorities.

Most (**73%**) CSOs/CISOs in the UK&I expect to see increased investment in cybersecurity to support this adaptive strategy with **25%** expecting a rise of more than **10%**. Just **7%** expect their cybersecurity budget to decrease, while **20%** expect it to remain the same.

How do you expect your cybersecurity budget to evolve over the next two years, if at all?

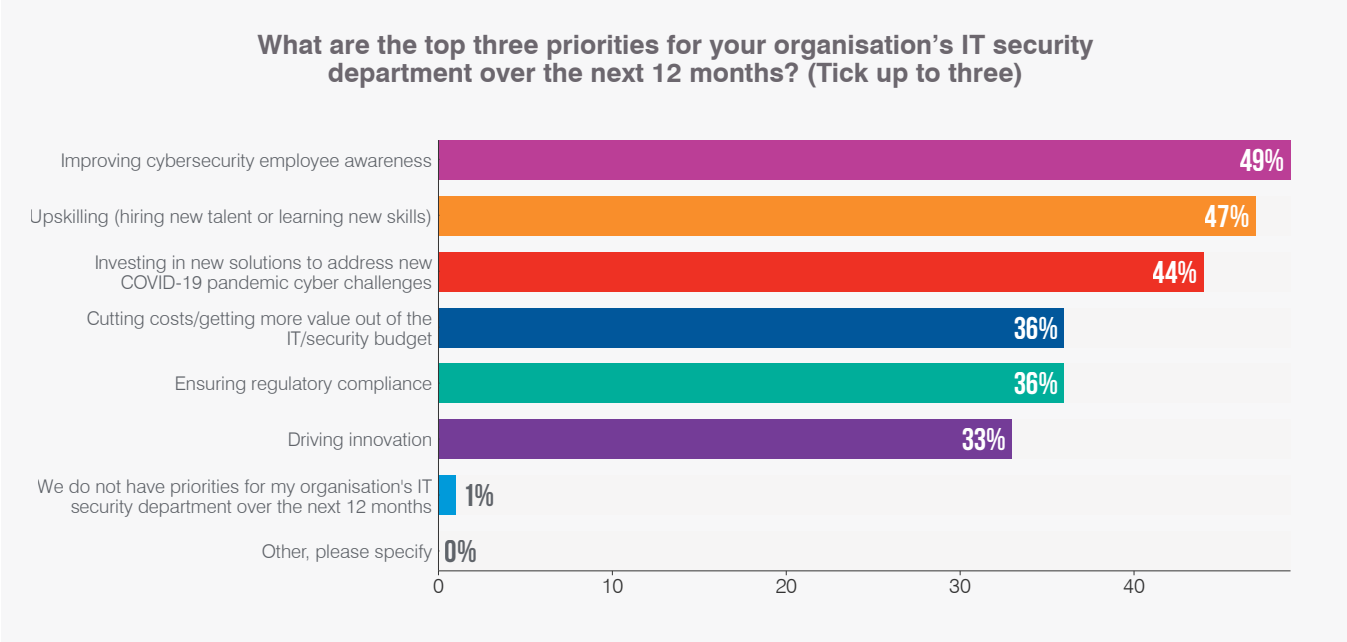


Improving cybersecurity employee awareness: the number one goal in 2021

When asked to name their top priorities for the next 12 months, CISOs and CSOs in the UK&I cited improving cybersecurity employee awareness as their number one goal in 2021.

Employee education and awareness of the latest threats is often the difference between an attempted cyber attack and a successful one. Failure to implement and review such programs leaves organisations dangerously exposed.

Investment is expected to focus in several areas – with a strong focus on improving employee cyber security awareness. IT leaders in the UK&I will look to improving employee cybersecurity awareness (**49%**), upskilling employees or hire new talent (**47%**), and invest in new solutions to address new COVID-19 pandemic cyber challenges (**44%**).



The COVID-19 pandemic is also predicted to have a lasting effect on UK&I organisations' digital strategies. While **69%** of CSOs/CISOs in the UK&I agree to some extent that the pandemic has accelerated their business' digital transformation roadmap, **54%** feel the global crisis may limit and restrict their organisation's future planned spending on cybersecurity.

CONCLUSION

Irrespective of the means of attack – email, cloud applications, the web, social media – threat actors continue to take advantage of the human factor. Whether it is impostors posing as trusted colleagues, or increasingly convincing phishing emails and malicious links, it is end-users who are on the frontline in the battle against cybercriminals.

Our study has shown that CSOs and CISOs across the UK and Ireland clearly recognise the cyber risks faced by employees and are prioritising their response and investments accordingly in 2021. However when looking at which threats should be prioritised, there seems to be disconnect in grasping the scale and importance of some vectors such as Business Email Compromise (BEC) and the correlation between cloud account compromise and insider risk management – two classes of threats that are growing significantly with today's global shift to remote working.

> *"Cybercriminals are focused and constantly improving their skills and techniques. If you don't do the same, there can only be one winner."*
>
> **Andrew Rose, Resident CISO, EMEA at Proofpoint**

That's why a people-centric strategy is a must for organisations. This starts with identifying your most vulnerable users and ensuring they are equipped with the knowledge and the tools to defend your organisation.

Along with technical solutions and controls, a comprehensive training program must sit at the heart of your cyber defence. Training should be regular, comprehensive and adaptative and cover a range of topics – from the motivations and mechanics of cyber threats, to how simple behaviours such as password reuse and inadequate data protection can increase the likelihood of a successful attack.

Cybercriminals are focused – forever honing their skills and techniques. If you're not doing the same, there can only be one winner.

proofpoint®

Contact us at info@proofpoint.com to better protect your business.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint's people-centric security and compliance solutions to mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.