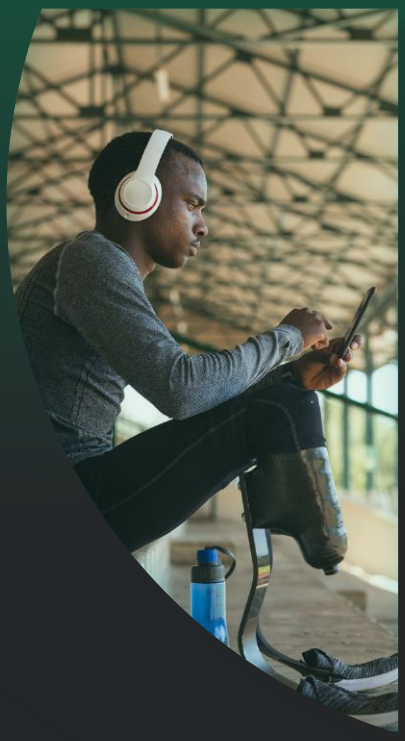
2021 UNISYS SECURITY INDEX™

GLOBAL REPORT



UNISYS | Securing Your Tomorrow®

TABLE OF CONTENTS

CHAPTER ONE
FOREWORD

The coronavirus pandemic caused a seismic shift in the way people live, learn, shop and, most notably, how organizations and their employees do business. Nearly overnight, it seemed as though every organization the world over experienced significant disruption as they tried to enable employees to work remotely, while also providing those employees with the digital tools to be as productive and collaborative as possible.

This year's Unisys Security Index™ -- the longest-running snapshot of consumer security concerns conducted globally – took on an outsized level of importance in light of this backdrop. This year's research sought to explore two key, interrelated areas.

The first is this:

HOW HAVE CONSUMER CONCERNS AROUND LIVING AND WORKING DURING A GLOBAL PANDEMIC SHIFTED OVER THE PAST 18 MONTHS?

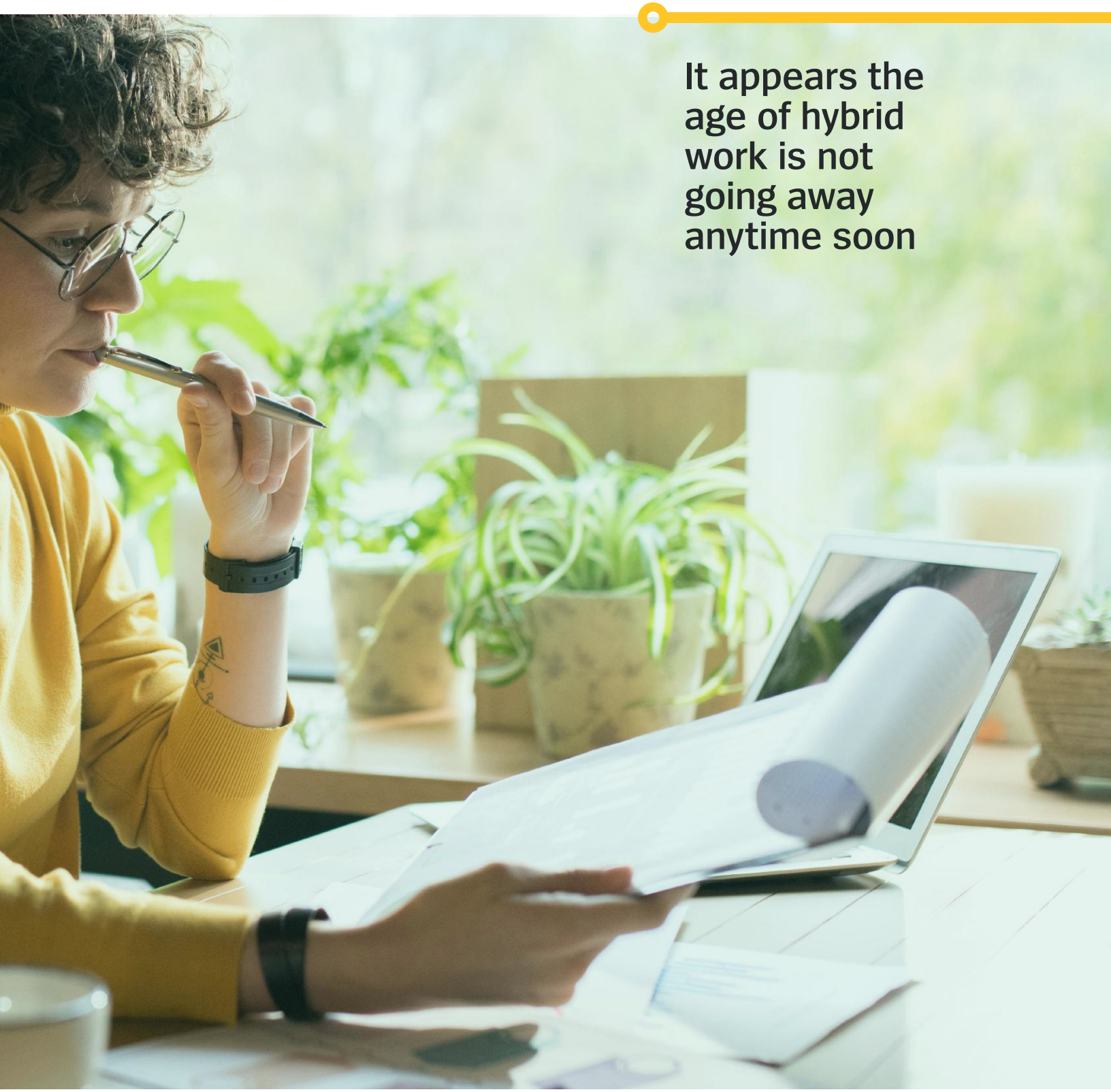
And then, as a result, the research sought to understand:

HOW THOSE CONCERNS HAVE AFFECTED THE MANNER IN WHICH PEOPLE WORK, AND WHAT THAT MEANS FOR THE BUSINESSES THEY WORK FOR GOING FORWARD – especially since it appears the age of hybrid work is not going away anytime soon.

This report outlines Unisys' findings from surveying 11,000 consumers across 11 countries around the world. Our findings reveal that despite high levels of overall concern around internet security, a lack of awareness around basic cybersecurity risks and threats is causing employees to unknowingly undertake risky behavior – putting their employers in jeopardy in the process. This report covers the importance of transparency and open communication with employees, especially those with remote or hybrid situations, as well as the need for organizations to deliver on the promise that the latest secure digital workplace and cloud-based solutions can provide.

Through this research, we garner invaluable insight from workers around the world, many of whom are working in hybrid or remote environments. As a result, we are not only able to gain a better understanding of their concerns, but more importantly, we are able to identify actionable behaviors that address unmet needs or areas of opportunity.

As we all look to emerge from the pandemic, we believe these insights will help to better determine how we collectively can help reshape the future of the hybrid workplace for both organizations and employees going forward – one that enables us all to continue to grow and succeed. We hope you will join us.



It appears the age of hybrid work is not going away anytime soon

CHAPTER TWO
EXECUTIVE SUMMARY

For the past 15 years, Unisys has conducted the Unisys Security Index as a leading way to gauge consumer concerns on a global level.

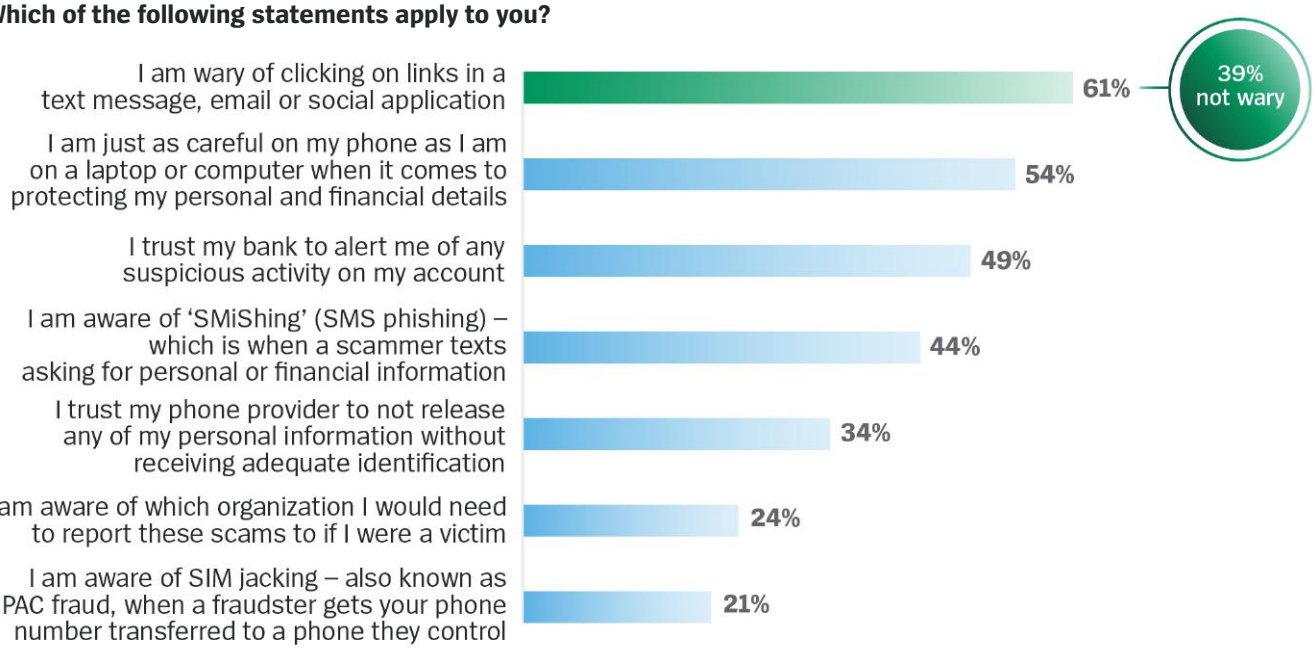
This year's survey took place 18 months after the outset of the pandemic, as hybrid and remote work became "the new normal," with nearly two-thirds of workers[1] (62%) globally working remotely at least part time. For many organizations, the shift happened quickly. COVID-19 required significant and rapid changes to the workforce, accelerating the adoption of digital workplace and cloud solutions as the pandemic prompted a shift to remote working.

As employees and their employers have adjusted to their new reality, their area of focus has shifted, as well. At the outset of the COVID-19 pandemic, many employees were understandably focused on their health and the health of their loved ones. As people have grown accustomed to life during the pandemic, the survey found that concerns around personal health have receded while Internet Security concerns have risen in every country. The result is a 12-point increase – putting it back at the top of the global agenda.

However, despite this increased level of concern around internet security, the survey found that a lack of awareness around cybersecurity threats is leading employees, especially those working from home part or full-time, to inadvertently put their employer's network at risk.

The survey identified a widespread lack of consumer awareness on avoiding and addressing online threats. Two out of five (39%) people report not being wary of clicking on suspicious links, despite phishing attacks accounting for more than 80% of reported security incidents[2]. Just 21% are aware of more sophisticated scams like SIM jacking, which is when a scammer gets your phone number transferred to a phone they control, and only a quarter (24%) know where to report these types of scams.

Which of the following statements apply to you?



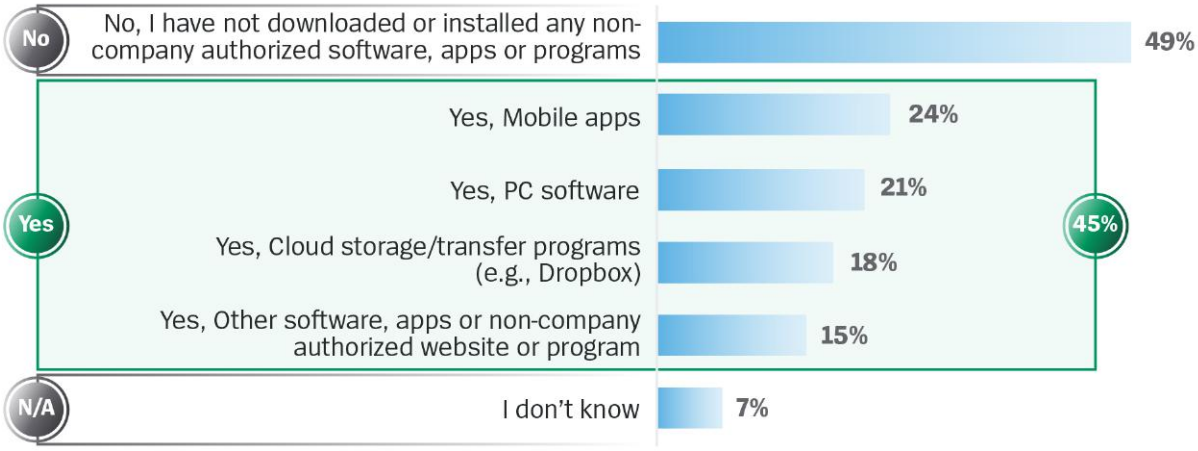
Unisys USI 2021; Q9: *Which of the following statements apply to you?; base n = 11000*

The resulting risks to businesses cannot be overstated. The move to remote working occurred alongside a marked increase in cybersecurity threats – with malware rising as much as 358%[3] from 2019 to 2020.

Worryingly for employers, this low level of awareness around cybersecurity threats is leading to risky behavior in employees' digital activities in the workplace. For example, almost half (45%) in the U.S., Australia and New Zealand have downloaded or installed software not approved by their IT department.

As more organizations attempt to keep up with and manage multiple cloud environments, the idea that employees could be downloading unauthorized software or apps, potentially from an unsecure cloud environment, opens up additional risk as they then connect back to their employers' networks. Consider that a recent survey[4] found that malware delivered over the cloud increased by 68% in Q2 of 2021, with cloud storage apps accounting for more than 66% of cloud malware delivery.

Have you downloaded or installed any software, apps or programs for work purposes, which your IT department has not authorized or approved? Asked in Australia, New Zealand and the U.S.



Unisys USI 2021; Q13: *Have you downloaded or installed any software, apps, or programs for work purposes, which your IT department has not authorized or approved? [AU, NZ, US ONLY]; base n = 2140*
**As the respondents were able to select multiple options, the underlying data points add up to over 100%*

When asked why they were choosing to bypass their IT department and download unauthorized software and apps, respondents noted that the apps they downloaded are ones that they use in their personal life (42%) or because they are perceived to be better than those provided by their company (42%).

All of this brings a stark reality to light. The fact is that people have choices in their personal lives, and now, they want choices in the tools they use at work, too. The implication for organizations and IT departments in particular is to move away from a "one-size-fits-all" model, and find a way to meet individual preferences and needs. Importantly, this does not mean employees have the right to install whatever they want, but that they have an opportunity to communicate with their employer about the tools they want to use. And for organizations, soliciting that feedback and listening to employees is critical, too.

Given the volume and complexity of cybersecurity threats today, businesses need to build trust with employees, closely monitor how and where applications are hosted, ensure the entire workforce has seamless connectivity and experience and implement centralized controls if organizations want to guarantee protection from cybersecurity threats no matter where their employees are connecting from.

[1] https://www.apollotechnical.com/statistics-on-remote-workers/
[2] https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=35ed6c0d58d3
[3] https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=35ed6c0d58d3
[4] https://www.zdnet.com/article/even-after-emotet-takedown-office-docs-deliver-43-of-all-malware-downloads-now/#ftag=RSSbaffb68

CHAPTER THREE

THE HYBRID WORKPLACE AT RISK: THE IMPORTANCE OF THE EMPLOYEE'S DIGITAL EXPERIENCE

Driven by the onset of the pandemic, remote and hybrid-work models that span the physical and digital spaces have become more common and, in many cases, preferred. It is unlikely that the office-based norm of the pre-pandemic world will return: More than four out of five (83%) employers now say the shift to remote work has been successful for their company, and more than half of employees (55%) would prefer to be remote at least three days a week once pandemic concerns recede[5].

THE RESULTING COMPLICATION IS THAT EMPLOYERS ARE NOW MANAGING A DIGITAL WORKPLACE THAT DEPENDS ON VIRTUAL COMMUNICATIONS, COLLABORATION TOOLS AND NETWORK ACCESS, LARGELY FROM EMPLOYEES' HOMES.

In line with the rise in remote and hybrid working, this year's survey saw Internet Security concerns increase more than any other area. Concerns around both Hacking & Viruses (up 6 percentage points from last year's study, to 57% seriously concerned) and Online Shopping (up 5 percentage points, to 51% seriously concerned) suggest heightened awareness of the risks surrounding internet use.

HOWEVER, IT IS CLEAR THAT DESPITE THEIR INCREASED CONCERNS AROUND HACKING, THEIR BEHAVIOR IS NOT REFLECTING GREATER CAUTION.

Two out of five (39%) are not wary of clicking on links in text messages, emails or social media. Fewer than half (44%) are aware of so-called SMiShing, which is when a scammer texts asking for personal or financial information, and only a quarter (24%) know which organization or department in their company to report scams to.

WORRYINGLY FOR EMPLOYERS, THIS LOW LEVEL OF AWARENESS OF CYBERSECURITY THREATS ALSO LEADS TO RISKY BEHAVIOR IN EMPLOYEES' DIGITAL ACTIVITIES IN THE WORKPLACE.

For example, almost half (45%) in the U.S., Australia and New Zealand have downloaded or installed software not approved by the IT department, typically because these other apps are ones that they use in their personal life (42%) or because they are perceived to be better than those provided by their company (42%).

57%

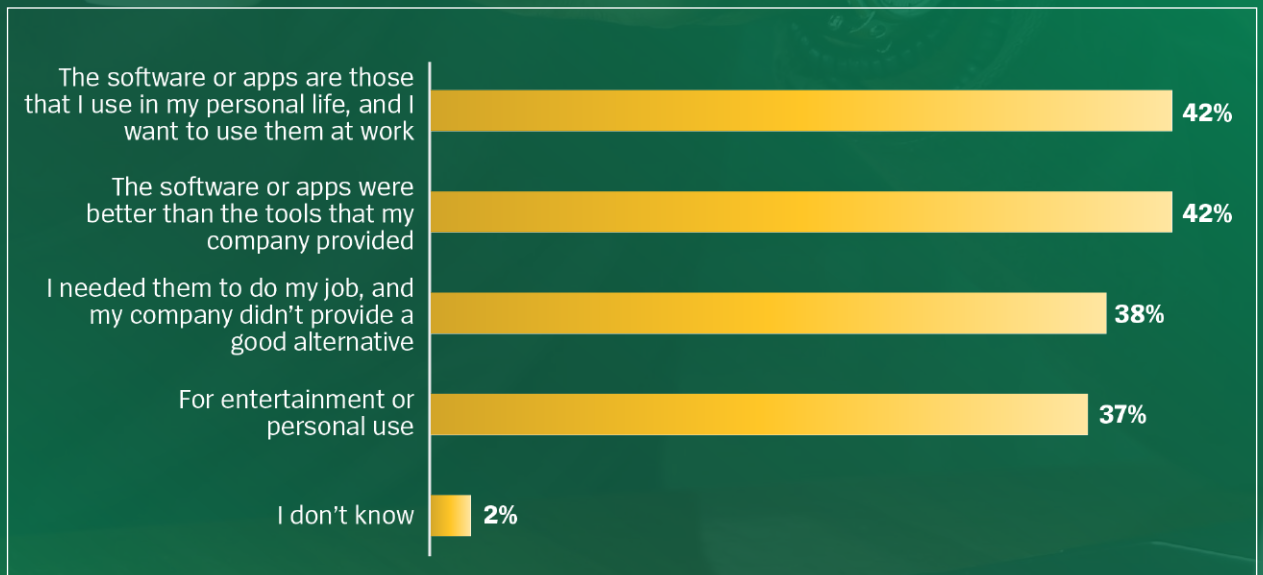
SERIOUSLY CONCERNED
About Hacking & Viruses
+6% points Year on Year (YoY)

51%

SERIOUSLY CONCERNED
About Online Shopping
+5% points (YoY)

[5] https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

It is unlikely that the office-based norm of the pre-pandemic world will return



Unisys USI 2021; Q14: *What are some of the reasons you choose to download or install non-supported software or apps for work purposes? [AU, NZ, U.S. ONLY]; base n = 966*

CHAPTER THREE (CONTINUED)

THE HYBRID WORKPLACE AT RISK: THE IMPORTANCE OF THE EMPLOYEE'S DIGITAL EXPERIENCE

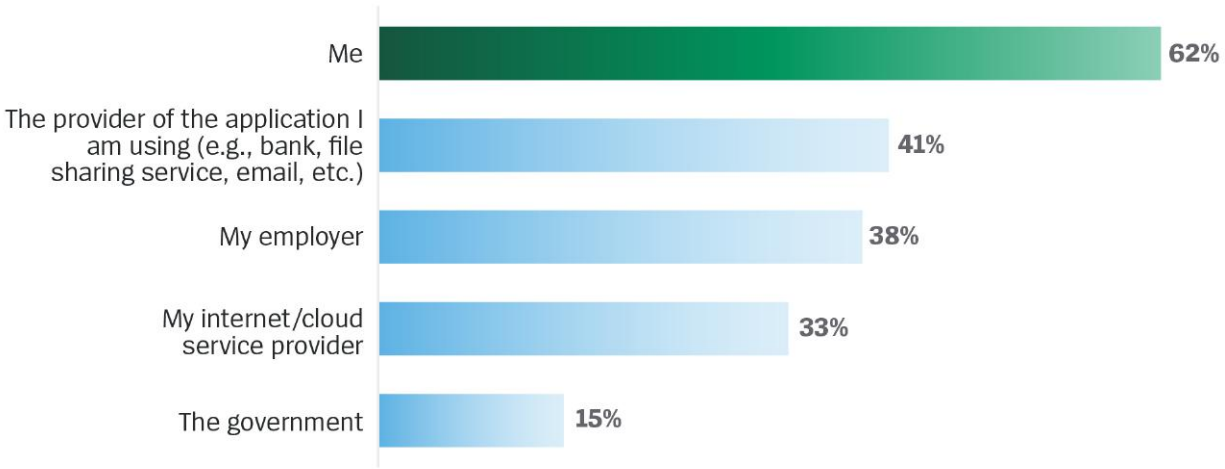
For employers, this opens up access points to the network, which typically is made up of more than one cloud environment[6]. While most organizations have security controls in place, there are still risks or holes that can be created by downloading unauthorized software or apps. For example, popular file-sharing apps can allow users to easily upload, store and download files, but they may contain viruses or malware that can spread to an employers' network.

Another concern for employers – many of which provide employees with smartphones – is that awareness of phone-related hacks is equally low. Only 21% of consumers are aware of SIM-jacking – which is when a scammer gets your phone number transferred to a phone they control.

The age of hybrid work presents a new challenge for employers as they look to define the lines between work life and home life, which have become understandably more blurred. The rise in remote working coupled with a lack of awareness of cybersecurity threats could lead to problems for businesses. The question of who bears responsibility for data privacy has therefore taken on even greater significance.

Most employees (62%) consider it their own responsibility to keep their personal data safe and secure while working from home, though a significant proportion – nearly two out of five (38%) – say that they consider it to be the responsibility of their employer.

While working from home, who do you believe is primarily responsible for maintaining your digital security – ensuring your data is kept safe and secure? Asked in Australia, Brazil, Colombia, Germany, Mexico, the Netherlands, New Zealand, UK



Unisys USI 2021; Q11: *While working from home, who do you believe is primarily responsible for maintaining your digital security – ensuring your data is kept safe and secure? [AU, BR, CO, DE, MX, NL, NZ, UK ONLY]; base n = 5954*

[6] https://www.factioninc.com/blog/hybrid-multi-cloud/multi-cloud-trends/

The common theme connecting these points together is the importance of a positive employee digital experience. When employees feel like they don't have the right tools to do their job, they bypass their own IT departments and download third-party apps or software, which means that malware or viruses can enter work networks.

AS A RESULT, ORGANIZATIONS MUST LOOK BEYOND SIMPLY PROVIDING ACCESS TO BUSINESS RESOURCES, AND FOCUS ON ENSURING EXPERIENCE PARITY – THE REQUISITE THAT ALL EMPLOYEES HAVE ACCESS TO THE SOFTWARE, APPS AND COLLABORATION PLATFORMS THEY NEED TO DO THEIR JOBS, REGARDLESS OF WHETHER THEY ARE WORKING FROM THE OFFICE OR THE HOME.

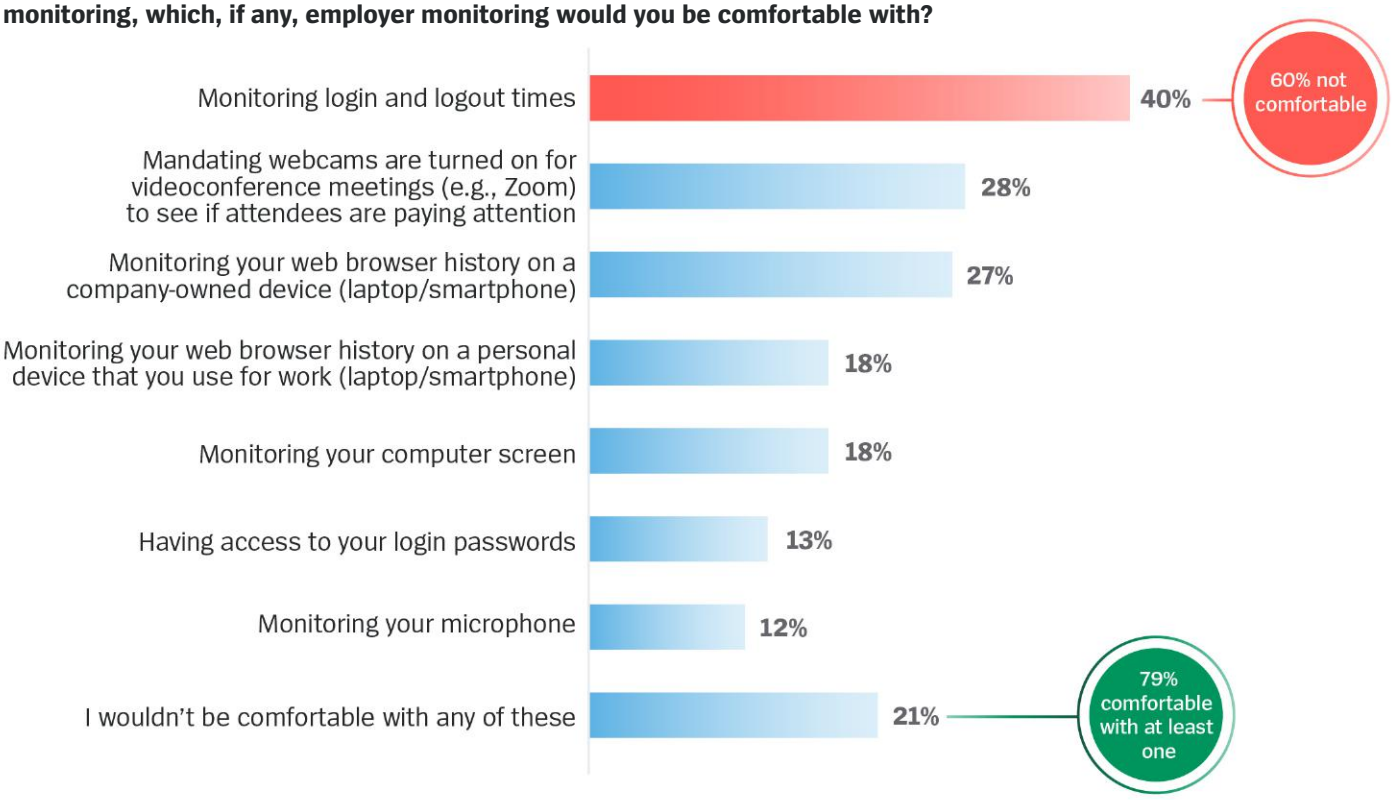
CHAPTER FOUR

TRANSPARENCY AND (DIS)TRUST IN THE DIGITAL WORKPLACE

The pandemic may have allowed the office into peoples' homes, but employees draw the line at employers using monitoring technology. The findings signal a need for new, outcome-based approaches to performance management and open conversations about privacy, trust and permission as employers try to balance productivity against employees' privacy concerns.

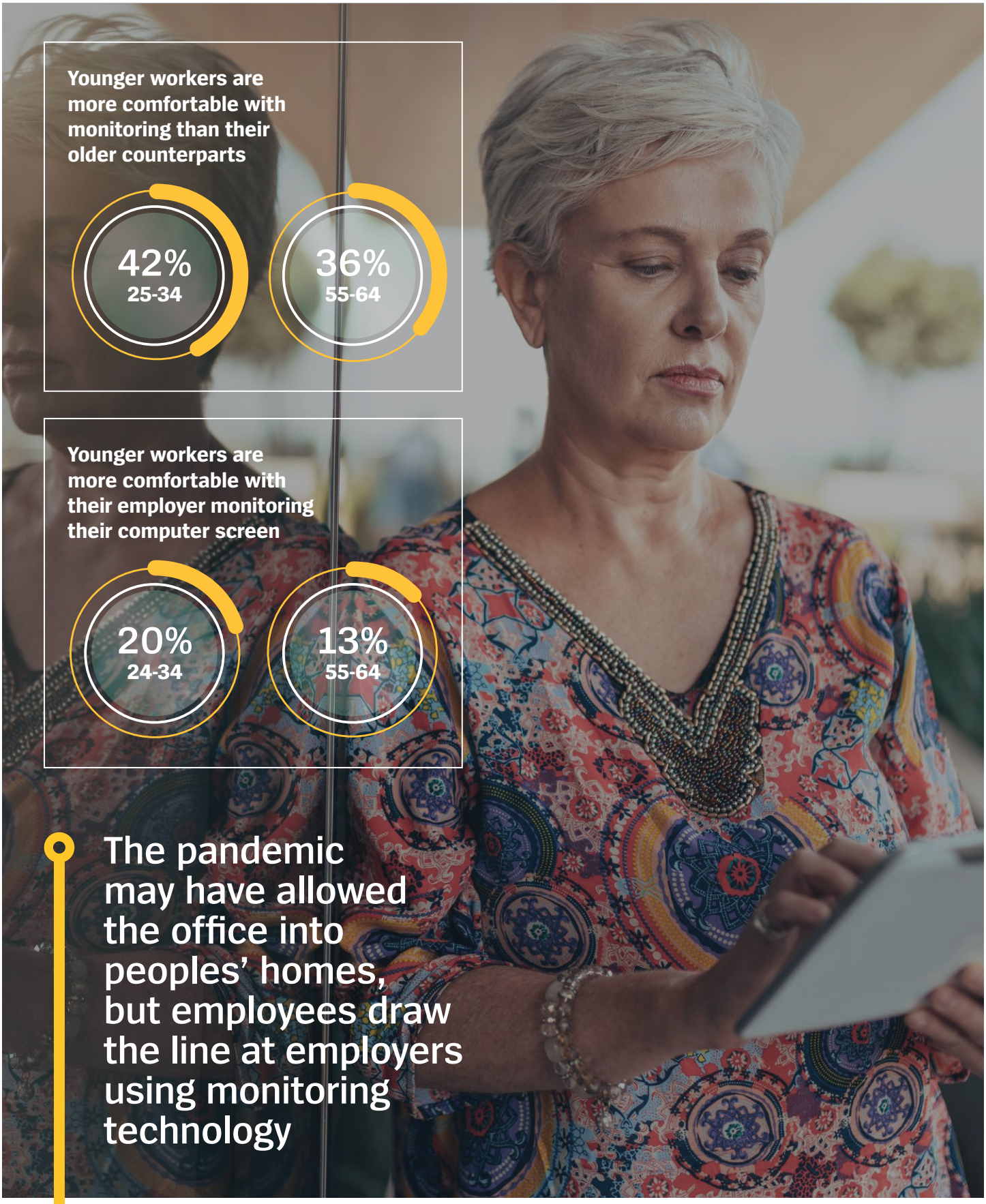
Most people – four out of five (79%) – are willing to be monitored by their employer in some way if it meant being allowed to work from home, but the information they are willing to share varies widely. Employees are most comfortable sharing data that reflects what is shared in physical, in-person offices – namely, login and logout times (40% are comfortable). Closer monitoring of work activity that is often considered more like 'looking over the shoulder' of workers is less welcome, with just 18% saying they would be comfortable with their screen being monitored, and only 12% saying they would be comfortable with microphone monitoring.

If your employer allowed you to work from home but required a certain level of monitoring, which, if any, employer monitoring would you be comfortable with?



Unisys USI 2021; Q10: *If your employer allowed you to work from home but required a certain level of monitoring, which, if any, employer monitoring would you be comfortable with?; base n = 8067*

Younger workers, particularly those aged 25-34, are more comfortable with monitoring than their older counterparts. Of note, 42% of 25-34 year-olds are comfortable with their employer monitoring login and logout times, as compared to 36% of 55-64 year-olds; and 20% of 24-34 year-olds are comfortable with their employer monitoring their computer screen, as compared to just 13% of 55-64 year-olds.

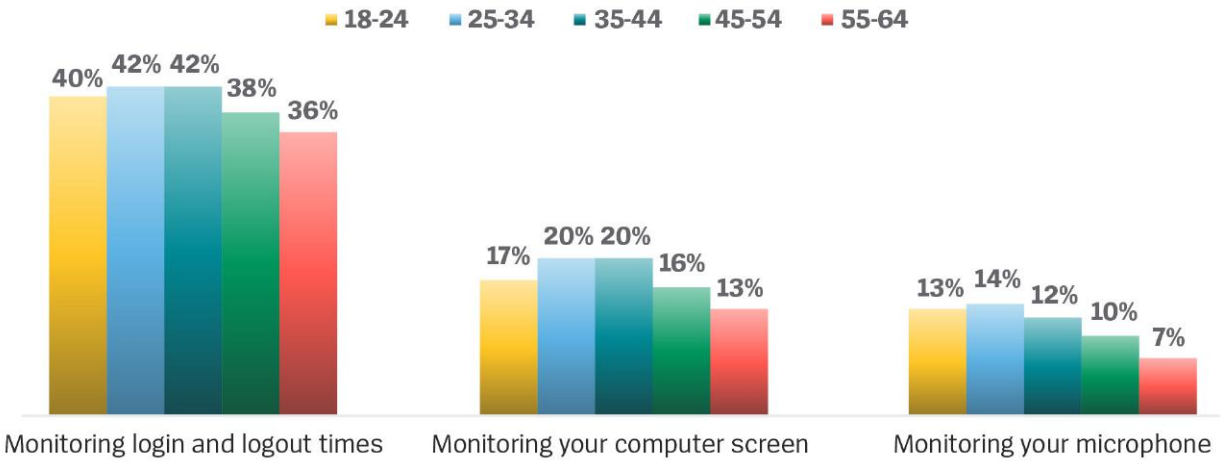


The pandemic may have allowed the office into peoples' homes, but employees draw the line at employers using monitoring technology

CHAPTER FOUR (CONTINUED)

TRANSPARENCY AND (DIS)TRUST IN THE DIGITAL WORKPLACE

If your employer allowed you to work from home but required a certain level of monitoring, which, if any, employer monitoring would you be comfortable with?



Unisys USI 2021; Q10: *If your employer allowed you to work from home but required a certain level of monitoring, which, if any, employer monitoring would you be comfortable with?; base n = 8067*

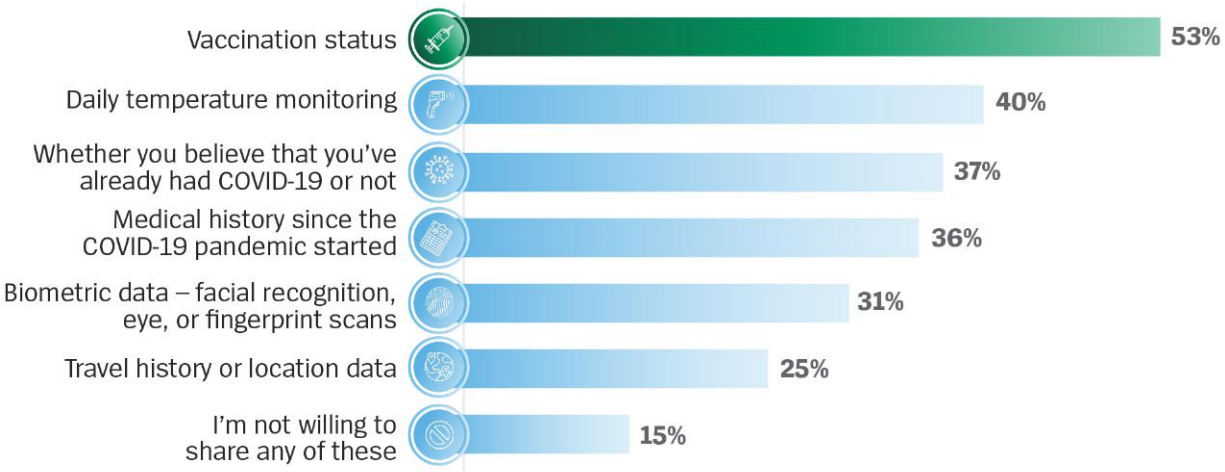
As employees operate in a hybrid workplace, switching between in-office and remote networks, businesses are challenged to maintain visibility into employee activities, but not for nefarious purposes. For starters, some monitoring measures offer positive benefits to employees – such as monitoring software response time so that the IT team can proactively fix impending issues before they impact the employee – called "intelligent IT support."

However, employee concerns also extend beyond monitoring. As many businesses juggle the pandemic with trying to safely enable return to office for some, employee concerns extend to data sharing with an employer.

For example, sharing of health data has also become a major consideration in the wake of the pandemic. This presents a tension between safety and privacy that is being responded to in different ways around the world.

In Europe, people are somewhat guarded when it comes to their personal health data. Thinking about apps that help trace COVID-19 contacts, Germans are split on sharing whether data privacy (39%) or tracing COVID-19 infections (38%) is more important. Half of people (50%) in France are unsure or uncomfortable with the idea of a digital health passport, and three-quarters (73%) of people in the Netherlands do not agree with a third party storing their biometric information in a central space. In contrast, biometric data is favored in Mexico, where 71% are confident that a biometric digital ID – the 'Cédula Única de Identidad Digital' that is soon to be brought in by the Mexican government – will better protect their personal data and identity.

What personal information are you willing to share with your employer to ensure access to a safe and healthy working environment? Asked in Colombia, Germany, Mexico, UK, U.S.



Unisys USI 2021; Q12: *What personal information are you willing to share with your employer to ensure access to a safe and healthy working environment? [CO, DE, MX, UK, US ONLY]; base n = 3726*

Overall, as employees and employers navigate this "new normal," opinion is divided on whether privacy or health should be prioritized. For example, nearly one-third (31%) are willing to disclose biometric data to ensure safe access to their facility, while 69% are not. And only 20% of workers are comfortable using facial recognition to authenticate that they are the person using their computer remotely.

Regardless of whether employees are concerned over monitoring or data sharing, studies have shown[7] this lack of trust is collectively attributable to a fear of the unknown. In this scenario, employees are not clear how their data or information might be used. It is this fear of the unknown that makes transparency and trust so important to improving the employer-employee relationship.

In order for business leaders to empower employees and create an optimal experience, there needs to be give-and-take when it comes to information sharing, built on a foundation of trust and transparency.

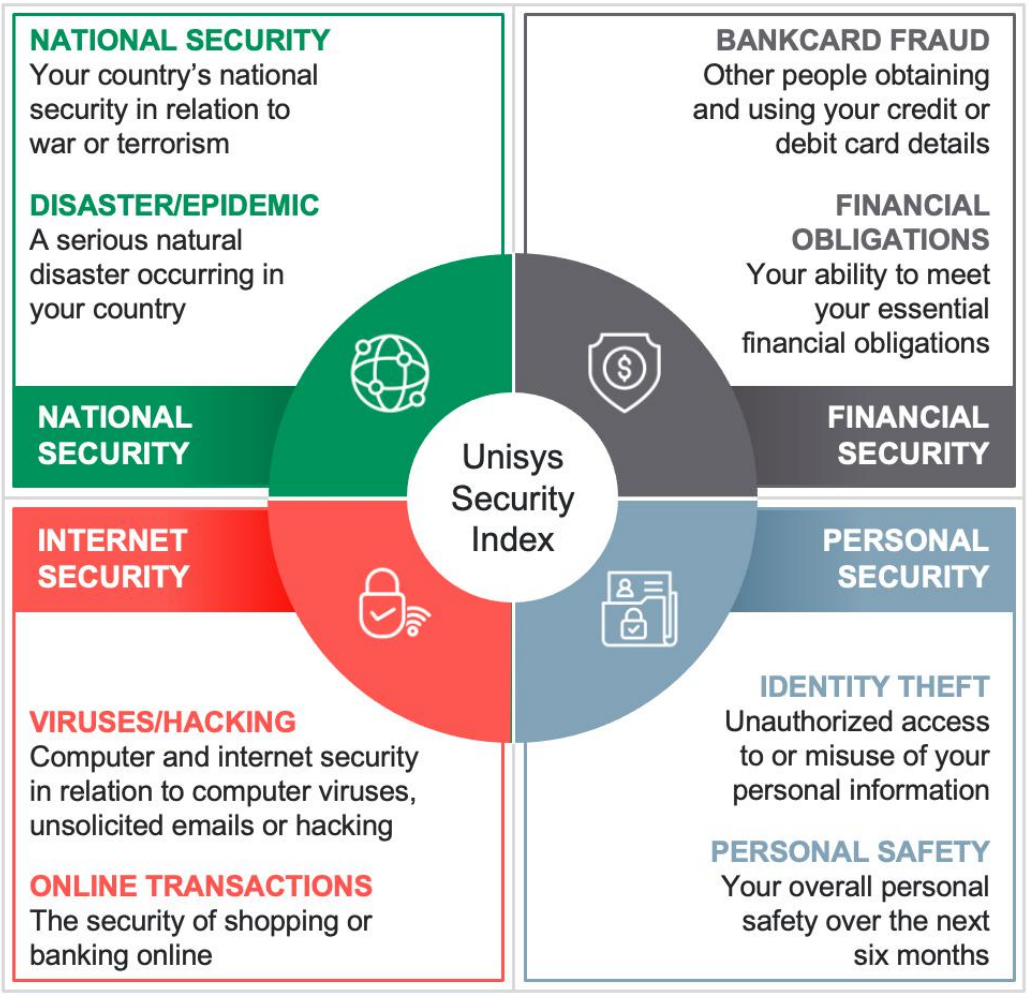
The reality is that it can be harder for organizations to build trust when their people are working remotely. Organizations need to be clear, concise and forthcoming in order to build and foster trust with their employees. According to Larry Prusak, senior advisor, Columbia University, "If I had to pick the one thing to get right about any collaborative effort, I would choose trust. Yes, trust. More than incentives, technology, roles, missions or structures, it is trust that makes collaboration really work. There can be collaboration without it, but it won't be very productive or sustainable in the long run."

Organizations need to be transparent with workers to make sure they feel like they are part of the team, are comfortable with what their employer is doing and, most importantly, why they are doing it and how it can benefit them. Establishing this trust will go a long way toward ensuring that employee productivity increases, as well.

[7] https://hbr.org/2021/02/wfh-is-corroding-our-trust-in-each-other

CHAPTER FIVE

THE UNISYS SECURITY INDEX: 15 YEARS AND COUNTING

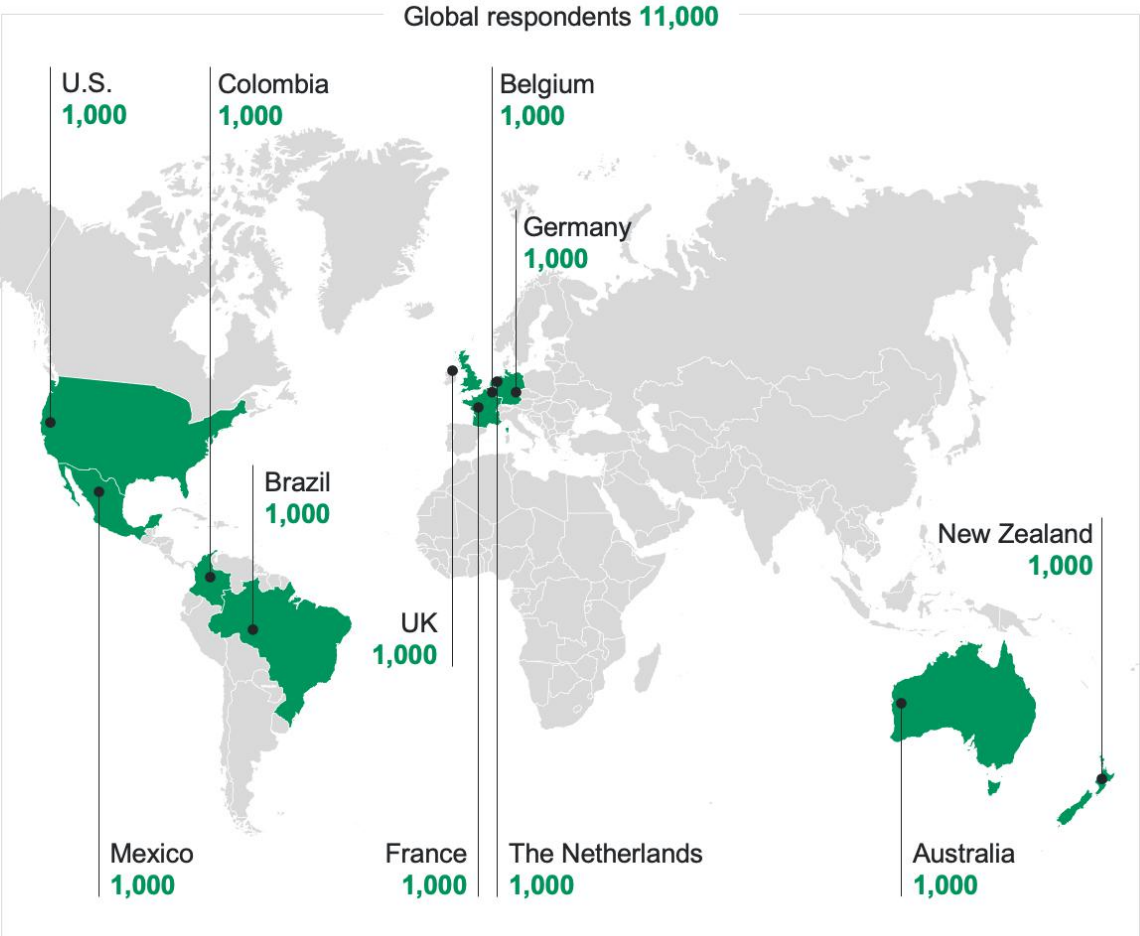


In 2007, Unisys Corporation (NYSE: UIS) launched the Unisys Security Index – the longest-running snapshot of consumer security concerns conducted globally – to provide an ongoing, statistically-robust measure of concern about security. The index is a calculated score out of 300 that measures consumer attitudes over time across eight areas of security in four categories.

The 2021 Unisys Security Index is based on national surveys of representative samples of 11,000 adults from 18-64 years of age. Interviews were conducted online in each of 11 countries: Australia, Belgium, Brazil, Colombia, France, Germany, Mexico, the Netherlands, New Zealand, the UK and the U.S.

All national surveys were conducted July 2-28, 2021. During the research, the COVID-19 pandemic was continuing in each of the countries surveyed.

In all countries, the sample is weighted to national demographic characteristics such as gender, age and region.



Global security indices are unweighted averages of the 11 countries' security indices. The margin of error is +/-3.1% per country at a 95% confidence level and 0.9% for the global results, also at a 95% confidence level.

The 2021 Unisys Security Index survey was conducted by Reputation Leaders, a global thought leadership consultancy.

CHAPTER SIX
REGIONAL DIFFERENCES

Security concerns are high across all countries surveyed, driven by concerns around viruses and hacking that have risen across the board. As in previous years, developed markets show lower concern than emerging markets – though the U.S. has seen a dramatic increase relative to its peers.

There remains a wide gap between the most-concerned country (Mexico, with a score of 217) and the least-concerned (the Netherlands, with a score of 115). Latin America shows the highest security concerns compared to other regions surveyed. This is led by Mexico, where concern is on the rise – up 5 points since 2020 – and centered on Financial and Personal Security. Colombia and Brazil make up the rest of the top three most concerned countries. Banking remains an area with low confidence: a quarter of Brazilians are not at all confident in bank-supported pay applications' ability to protect their data.

Overall Security Index year-on-year comparison

2020		2021
Colombia: 217	1	**Mexico:** 217
Mexico: 212	2	**Colombia:** 215
Brazil: 197	3	**Brazil:** 192
U.S.: 159	4	**U.S.:** 175
Australia: 157	5	**Australia:** 159
France: 156	6	**France:** 156
Belgium: 144	7	**UK:** 150
UK: 144	8	**New Zealand:** 140
New Zealand: 136	9	**Belgium:** 139
Germany: 122	10	**Germany:** 125
The Netherlands: 100	11	**The Netherlands:** 115
11 Country Average: 159		**11 Country Average:** 162

UNISYS SECURITY INDEX

The U.S. is fast approaching the levels of concern seen in Latin America, with a 16-point rise in overall security concerns – making it the most security-concerned of all developed markets included in the survey. This is the greatest overall increase among any of the 11 countries surveyed and the country's highest level of concern in the 15 years that Unisys has been running this study. The U.S. is more concerned about Internet Security than ever before, with a score of 182 – an increase of 25 points over 2020's score.

Across Europe and the U.S., Financial Security concerns rose. This was particularly true for the UK (rising 11 points) and the U.S. (rising 8 points). Financial challenges created by the pandemic, including job losses, are likely to have created financial burdens for more people than in previous years. Belgium bucks this trend with a drop of 3 points, thanks to successful government support measures.

Financial Security Index year-on-year comparison

2020		2021
Colombia: 227	1	**Colombia:** 224
Mexico: 220	2	**Mexico:** 221
Brazil: 203	3	**Brazil:** 202
U.S.: 158	4	**U.S.:** 166
Australia: 162	5	**Australia:** 160
France: 150	6	**France:** 155
Belgium: 145	7	**UK:** 152
New Zealand: 143	8	**New Zealand:** 143
UK: 141	9	**Belgium:** 142
Germany: 108	10	**Germany:** 115
The Netherlands: 88	11	**The Netherlands:** 103
11 Country Average: 158		**11 Country Average:** 162

UNISYS SECURITY INDEX

The pandemic has been a wake-up call for European markets, prompting awareness of security issues that consumers had previously been unaware of or shielded from. The Unisys Security Index scores for all European markets rose, other than France, which remained stable.

The Netherlands, typically the market with the lowest concern, remains at the bottom but has nonetheless seen a 15-point rise. This could be linked to the country experiencing the second-highest COVID-19 infection spike since the start of the pandemic during the fieldwork, as well as several recent hacking and ransomware[8] scams undermining trust in businesses and the government.

Australia and New Zealand, in line with other developed markets, saw a steep increase in Internet Security concerns, which rose 14 and 19 points, respectively. The global nature of COVID-19's impact has meant that Internet Security concerns linked to remote working and cyberattacks have risen in every country. The U.S. and the Netherlands have felt this most keenly: each saw an increase of 25 points.

[8] https://nltimes.nl/2021/07/03/dutch-companies-also-targeted-large-ransomware-attack

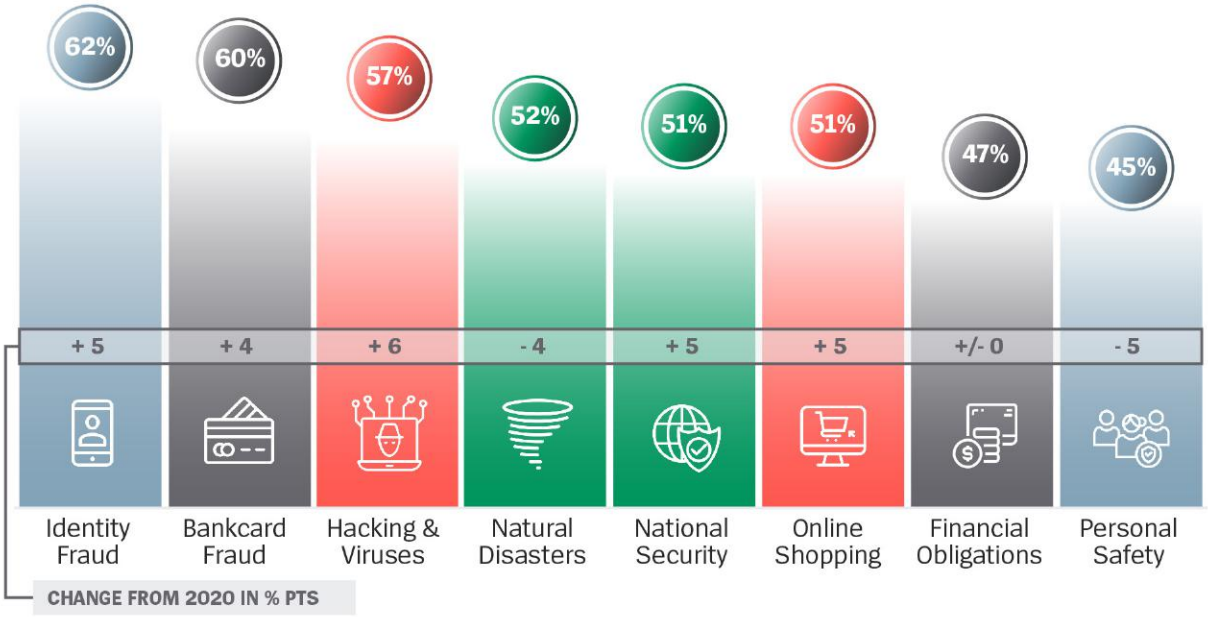
CHAPTER SEVEN
CHANGES IN THE GLOBAL CONCERN

The overall 2021 Unisys Security Index score remains consistent with previous years, increasing from a slight dip in 2020 back up to a high of 162.

Eighteen months on from the outbreak of COVID-19, the four areas of security concern returned to the pattern seen pre-pandemic. The shift in focus in 2020 – toward Personal Safety and Natural Disasters – has reversed, with consumers' gaze returning to Internet and Financial Security. Internet Security saw the most notable change, moving from the lowest to the highest area of concern in a 16-point increase.

Personal Safety and Natural Disasters both dropped, as the immediate impact of the pandemic subsided. Attention shifted instead to security concerns linked to the pandemic's knock-on effects: namely, a world that is more online than ever before.

How concerned are you about the following issues (showing top 2, extremely or very concerned)



Unisys USI 2021; Q8: *On a scale of 1 to 4 where 1 is not concerned, and 4 is extremely concerned, how concerned are you about the following issues?; base n = 11000*

Consumer concerns around Online Shopping – which became commonplace for many, with U.S. e-commerce sales projected to grow by 17.9% in 2021[9] – rose to 51% seriously concerned, an increase of 5 percentage points. Forced to change the way they live, work and shop, consumers have become more aware of the risks associated with paying online – driving, too, an increase in concern around Bankcard Fraud (60% seriously concerned, up 4 percentage points). This and the related issue of Identity Theft (62% seriously concerned, up 5 percentage points) remain the top areas of concern for the fifth consecutive year and are on the rise.

[9] https://www.emarketer.com/content/us-ecommerce-forecast-2021


60%
SERIOUSLY CONCERNED
About Bankcard Fraud
+4% points (YoY)
62%
SERIOUSLY CONCERNED
About Identity Theft
+5% points (YoY)
Concerns about Personal Safety and Natural Disasters both dropped, as the immediate impact of the pandemic subsided

CHAPTER EIGHT
THE UNISYS PERSPECTIVE

This year's survey results in some ways represented a return to normalcy. Internet Security was the top area of concern in 2021, as it had been in 2018 and 2019. However, the circumstances behind the rise in Internet Security concerns compared to 2020 are different than those from previous years. The pandemic prompted a spike in internet usage around the world, especially as working and learning remotely became "the new normal."

According to Leon Sayers, director of Advisory at Unisys Asia Pacific, *"With many countries in and out of lockdown, often requiring people to quickly go back to working from home, homeschooling and online shopping, they are more and acutely aware of their reliance on online channels. The flip side for employers is that the home network has become a target for corporate attacks, not just personal attacks."*

With more people than ever working and shopping from home – and sharing their financial details with online retailers around the world – the risk of being compromised or scammed has never been higher. Cyberattacks have increased exponentially, driven largely by ransomware attacks, which were up 600% globally[10] over the previous year.

According to Unisys Chief Security and Infrastructure Officer Mat Newfield, the shift to hybrid or remote work exacerbated the issue. *"A year and a half ago,"* noted Newfield, *"the collective global 'we' had to take everybody out of these generally secure, closed-office environments and put them on the most vulnerable networks on the planet. And that's each of your homes."*

CYBERSECURITY AWARENESS REMAINS LOW, LEADING WORKERS TO PUT COMPANIES AT RISK

While the rise in Internet Security concerns is understandable, what is surprising is that many are generally unaware of cybersecurity risks or where to report them. The survey found that globally, more than half (56%) say they are not familiar with the threat of SMS phishing (also known as 'SMiShing'), nearly four in five (79%) are unaware of SIM jacking and more than three in four (76%) do not know where to report scams if they were to be victimized.

According to Leon Gilbert, senior vice president and general manager, Digital Workplace Solutions, Unisys, *"As the shift to remote work blurred the lines between work and home, everyday employee tasks like opening an attachment can have serious consequences if employees aren't paying attention to the source. For businesses, it also raises the concern around device performance and visibility, and how they are being used. It makes the challenge for IT that much harder."*

The survey found many workers engaging in risky behavior. Almost half of people (45%) surveyed in the U.S., Australia and New Zealand acknowledged downloading or installing software not approved by their organization's IT department because the other apps are ones that they use in their personal life (42%) or because they are perceived to be better than those provided by their company (42%).

[10] https://www.infosecurity-magazine.com/blogs/ransomware-rise-companies-respond/

"It's likely that most haven't thought about the security risks of ad-hoc and personally-preferred software and applications. What began as BYOD (personally-preferred devices like iPhones) has grown into the apps, services, social and gaming environments," said Gene Chao, senior vice president and general manager, Enterprise Computing Solutions and Cybersecurity Solutions, Unisys. *"But as nearly half of employees download unauthorized tools and software as our personal and professional lives weave into each other, it means that malware or viruses can enter work networks, oftentimes with little or no record of a breach. That's a big problem."*

The global shift to remote work also accelerated companies' move to cloud-based apps and platforms, as organizations have recognized that an "as-a-Service" model can better help prepare them for digital disruption. Cloud-based applications and solutions allow employees to work from anywhere and help organizations become more agile and resilient to constant changes in market dynamics. At the same time, cloud computing and hybrid environments add considerable complexity, especially as the multi-cloud model becomes more commonplace.

"This shines a light on the risk and complexity of current environments," said Mike Morrison, senior vice president and general manager, Cloud and Infrastructure Solutions, Unisys. *"Organizations need to understand what's happening in your IT environment so you can take action to address gaps and incidents. Two of the main factors that hamper best practices in cloud security are a lack of platform-specific knowledge in cloud configurations and the lack of governed automation for infrastructure deployments. Cloud-appropriate security and compliance must be established prior to migration and governed continuously."*

THE CONSUMERIZATION OF IT HAS CHANGED EMPLOYEE EXPECTATIONS

When asked why they were downloading software or apps that were not authorized, the top answers point to the consumerization of IT. More than two in five (42%) say that the software or apps are better than the tools that their company provides, and 38% say that they need the tools to do their job and the company didn't provide a good alternative.

"This highlights the extent to which users are looking for consumer-friendly services and apps, including at work," said Sayers. *"And sometimes, the business apps just don't cut it."*

According to Patrycja Sobera, global vice president, EUX Delivery, Digital Workplace Solutions, Unisys, *"Inadequate software may push end users to find better alternatives, so ultimately they can be more productive and achieve their job objectives. This poses multiple security risks and drives unnecessary cost for an organization. IT needs to break out of the 'one-size-fits-all' model and address individual preferences and needs by placing key focus on understanding how an end user feels, how to ensure quality communication and collaboration experiences and equip the workforce with appropriate tools that are adopted rather than bypassed."*

CHAPTER EIGHT (CONTINUED)
THE UNISYS PERSPECTIVE

EMPLOYEES LACK TRUST IN THEIR EMPLOYERS

For employees, willingness to share personal information varies based on who they are sharing their information with and how they expect that information to be used. However, largely speaking, most employees are averse to the idea of sharing data, especially when asked about their comfort level with employer monitoring – even if it allows them to work remotely. For example, 60% of workers are not comfortable with their employer monitoring login and log-out times if they were working from home, and one-fifth (21%) are not comfortable with any monitoring whatsoever.

This trend also covers the extent to which people trust institutions to monitor their data for protective purposes. Globally, less than half (49%) of respondents say they trust their bank to alert them of any suspicious activity and only one-third (34%) say they trust their phone provider to not release their personal information without adequate notification. When asked what information they would be willing to provide to their employers to ensure access to a safe environment, only 31% are willing to share biometric data.

As Kevin Turner, Digital Workplace Solutions strategy lead, Unisys Europe, Middle East and Africa said, *"In the new world of the hybrid workplace, we see very mixed reactions to employer monitoring and tracking. This often includes monitoring on both corporate and personal devices. Corporations therefore need to be very transparent and consistent in their communications with the workforce, to avoid a culture of reluctance and mistrust. In the same way, continual and repeated awareness or education of all corporate systems usage is imperative to drive improvements in attitude to drive responsibility. A change in culture can mitigate a lot of risk for organizations."*

This lack of trust extends across institutions at the country level, as well. A quarter of Brazilians are not at all confident in bank-supported pay applications' ability to protect their data, and 73% of people in the Netherlands do not agree with a third party storing their biometric information in a central space.

60%

Are not comfortable with their employer monitoring login and log-out times if they were working from home

49%

Say they trust their bank to alert them of any suspicious activity

21%

Are not comfortable with any monitoring whatsoever

34%

Say they trust their phone provider to not release their personal information without adequate notification

CONCLUSION

Despite the renewed attention to internet security, many people around the world are unaware of specific types of cybersecurity threats, unsure whose responsibility it is to safeguard personal and company data, and worse, actively bypassing their own IT departments to download software and apps to do their jobs. In short, businesses around the world find themselves in a precarious place.

"If you are an employer and you have the mindset 'no news is good news,' then you are forgetting that 'no news' is just something you haven't heard about yet," said Newfield. "No news is not good news. If you haven't been all over the news because you haven't had an issue in the last year that you are aware of and you continue to think allowing your employees to buy their own laptops and connect to the workplace network is okay – then you are a statistic waiting to happen."

CALLS TO ACTION

So, what can businesses and governmental agencies that serve consumers do? Unisys believes there are tangible steps they can take.

1 Balance security with a positive employee digital experience

Protecting your network and giving employees access to productivity and collaboration software is not a mutually-exclusive decision. While it is true that the rapid shift for many organizations to a remote or hybrid model brought challenges, including the lack of visibility into employee activities, it is still very possible for organizations to increase their focus on employee experience without sacrificing security at any level.

"For starters, you need to make it easy for people to know what they can and cannot do with their work-issued machines, full-stop," said Gilbert. *"Users want their technology to work, and they don't care what happens in the back end as long as they can reliably and consistently access the resources they need. As an employee, what you do have the right to do is challenge your organization regarding the tools you use. And for organizations, making sure that you are soliciting that feedback and listening to your employees is very, very important."*

2 Protect the cloud(s)

Today, almost every organization is utilizing the cloud to some degree. And while most organizations have security controls built into the cloud where they store company data, there are still risks or holes that can be created, as cloud storage apps account for more than two-thirds of malware delivery. Research has found that most cloud users are not intentionally lax in their approach to security and compliance, but lack the tools, knowledge or processes to respond properly. As a result, the cloud is an essential component of remote work security.

"Organizations need to embrace a cloud-first security strategy. The survey found a large percentage of people downloading unauthorized software and apps, and that not only increases your company's attack surface, it also brings the question of whether this other software – that's now being brought into your company network – is secure," said Morrison. *"One of the greatest challenges for organizations is maintaining visibility into your company's cloud deployments. It's hard to defend things that you don't know about. This is why cloud requires continuous re-examination and remediation, and why security must be closely entwined with how your cloud infrastructure is defined and used, especially in fast-paced DevOps environments."*

3 Use transparency as a way to build trust

Getting employees on board with the importance of cybersecurity by changing their viewpoint – and their behavior – comes down to transparency and education. It is crucial to build trust by being open and explaining exactly what is being monitored and why. Ultimately, many of the areas of conflict and misunderstanding could be resolved by education and information from the employer. It is the responsibility of the organization to educate and help employees to understand where their fears are irrational – or open their eyes to dangers they are not yet aware of.

"Employee education is important, but it must be repeated and continually evolve to ensure they are alerted to new sophisticated threats. But employee education alone is not enough – it must be backed up by processes and technologies to make it extra hard for people to do the wrong thing. Users expect consistent and good quality experiences no matter where they are. This means IT needs a higher level of visibility when users work from home, to ensure a consistent experience regardless of location. At the same time, it is natural for humans to make mistakes, and visibility is key to reducing the opportunities for human errors to occur," said Gergana Winzer, industry director of Cybersecurity, Unisys Asia Pacific.

4 Go on the offensive: build security controls into your network

Organizations need to recognize that the employee does not see themselves as a protector of the company. Employers need to be proactive in protecting the use of corporate equipment in the home (and sometimes also for personal use). The onus remains with the company to be clear on what their specific IT security boundaries are in the work environment and to be consistent in maintaining these standards.

"As this survey shows, when people work from home they can inadvertently create security risks," said Chao. *"Unisys believes that organizations need to put technical controls in place to help protect the organization from human error. Part of that approach entails adopting a Zero Trust security model made possible by a software-defined perimeter that leverages micro-segmentation. Our Unisys Stealth® software suite is trusted by government and commercial organizations to transform your existing network, both on-premises and in the cloud. It dramatically reduces your attack surface and is scalable for users at organizations of any size."*

5 Rethink your security training – it should be personal, frequent and unapologetic

Almost every company offers annual security training at least when a new hire joins the company. However, large gaps persist. A 2020 survey[11] found that only three in five employers allocated budget for employee security training, and fewer than half made it mandatory. With remote and hybrid work changing the threat landscape, employers can no longer rely on the closed environment of the office workspace to guard against cybersecurity threats. A robust, continual training program is now more important than ever.

"Doing cybersecurity training once a year is useless," said Newfield. *"It's got to be ongoing. You test that the employees are learning, then you test again. Constantly test without fear of reprisal and make it personal. CISOs need to stop training people to protect the corporation. It's not employees' responsibility to protect the company, it's the CISO's. So what organizations need to do is change their approach to make it about the employee and his or her family. It's not [the employee's] responsibility to make all of the CISO's policies personal. It's the CISO's responsibility to make their policies personal to [the employee]."*

[11] https://symbolsecurity.com/2020/03/24/why-are-security-awareness-training-programs-doomed-to-fail/

About Unisys

Unisys is a global IT solutions company that delivers successful outcomes for the most demanding businesses and governments. Unisys offerings include digital workplace solutions, cloud and infrastructure solutions, enterprise computing solutions, business process solutions and cybersecurity solutions. For more information on how Unisys delivers for its clients across the commercial, financial services and government markets, visit **www.unisys.com**.

About the Unisys Security Index

Unisys has conducted the Unisys Security Index – the longest-running snapshot of consumer security concerns conducted globally – since 2007 to provide an ongoing, statistically-robust measure of concern about security. The index is a calculated score out of 300 covering changing consumer attitudes over time across eight areas of security in four categories: national security and disaster/epidemic, in the National Security category; bankcard fraud and financial obligations, in the Financial Security category; computer viruses/ hacking and online transactions, in the Internet Security category; and identity theft and personal safety, in the Personal Security category. The 2021 Unisys Security Index is based on online surveys conducted July 2-28, 2021. Surveys were conducted with nationally representative samples of at least 1,000 adults in each of the following countries: Australia, Belgium, Brazil, Colombia, France, Germany, Mexico, the Netherlands, New Zealand, the UK and the U.S. The margin of error at a country level is +/- 3.1% at a 95% confidence level and +/-0.9% at a global level.

For more information on the 2021 Unisys Security Index, visit **www.unisyssecurityindex.com**.

#SecurityIndex

Research services and analysis for the Unisys Security Index were provided by Reputation Leaders Ltd

UNISYS | Securing Your Tomorrow®