2021 UNISYS SECURITY INDEX™ AUSTRALIA & NEW ZEALAND

REFLECTING ON 15 YEARS OF SECURITY INSIGHTS – WHAT DOES THE FUTURE HOLD? A FUTURIST'S VIEW...

UNISYS | Securing Your Tomorrow®

unisyssecurityindex.com

INTRODUCTION

Letter from Andrew Whelan, Vice President Client Management, Unisys Asia Pacific

When the Unisys Security Index™ launched in 2007, to gain an understanding of how people around the globe felt about a wide range of security issues, spanning financial, internet, personal and national security, who could have predicted how much the world would change in the next decade and a half?

The world looks very different to how it did at the time of the first Unisys Security Index in 2007. Smartphones had just entered the market, social media was in its infancy, much of our online activity was still done on a desktop computer, we were in the midst of the global financial crisis, the 9/11 and London bombing terror attacks were still raw, and while some regions were familiar pandemics such as SARS, most of us would not have considered one on a global scale. Since then we have dealt with earthquakes, bushfires and local terror attacks.

In 2021 we take the chance to pause and reflect on the role technology plays in our lives, how that has evolved since the first Index, and what our current attitudes towards security might reveal about our future.

To this end, we've asked tech commentator and futurist Mark Pesce to examine the data from the 2021 Unisys Security Index for Australia and New Zealand, reflecting on where we've come from, and where we might be heading post-COVID.

Each iteration of the Unisys Security Index tracks consumer sentiment around their personal, financial, national and internet security, revealing how our priorities and concerns change over time. Each year we also deep-dive into particular topical issues that impact how we go about our personal and work lives. In this study, security is not about bits and bytes. Instead we approach security from its widest sense: being free from danger or threat.

For citizens of Australia and New Zealand, the pandemic has fundamentally changed the way most of us live and work; and escalated the risks we face online. With such rapid change in our lives and our growing reliance on the digital world, this year we've chosen to deep-dive into two areas that impact our work and home life today:

1. With the trend for more of us to work remotely, how do employees feel about being monitored while we work from home?

2. Where does responsibility lie to protect against cyber security threats when working from home, and people up to the task?

The research findings and Mark's observations show we'll need more than just great technology to face the future, we'll need transparency, trust and empathy in equal measures.

Andrew Whelan
Unisys Vice President
Client Management, Unisys Asia Pacific

> “In Australia security concerns have reached their highest point since the survey began in 2007.”
>
> **Mark Pesce**
> Futurist

A CHANGED WORLD

Humanity has taken the measure of the COVID-19 pandemic; vaccines developed and deployed in record time shifted our fears away from our health, toward permanent changes in the way we live, work and learn. We feel exposed and vulnerable to pervasive dangers online that we cannot see, and that we do not know how to defend ourselves against.

These fears dominate the Unisys Security Index in both New Zealand, and particularly, in Australia where security concerns have reached their highest point since the survey began in 2007. Yet, these fears also serve to illuminate the darkness, showing us how and where to provide support – with insight, openness, and empathy. Listening to our fears allows us to hear (and meet) our unspoken needs.

Our fears mirror our times. In the years following the GFC, personal financial concerns loomed large in survey results. The 2019 Christchurch Mosque attack shocked New Zealanders into a new awareness terrorism threats. The COVID-19 pandemic made everyone conscious of natural disasters and their personal safety.

What can the past tell us about the shape of our current fears – and how we might learn to live with them? To find out, we need to look back across the years surveyed by the Unisys Security Index.

FEAR OF THE UNFAMILIAR

The 2008 Unisys Security Index (one of the earliest reports) highlighted a now-forgotten concern – those surveyed did not trust mobile devices for shopping, banking or anything else finance-related, with just 7% saying they would use one to pay bills, bank, or shop online.

Before the iPhone came to Australia and New Zealand in 2008, a mobile meant a sturdy but not-very-functional ‘feature phone’. In 2021, nearly 90% of the adult population uses a smartphone, and thinks nothing of ordering groceries, paying bills, or even applying for a mortgage via an app.

How did we cross the chasm from fear to everyday reality? Part of it lies within a generational shift.

As user interface pioneer Alan Kay once noted, “Technology is anything invented after you were born.”

A generation born with both the Web and mobile devices had no trouble grasping the power and capability of mobile commerce, while an older generation, accustomed to bricks-and-mortar and bank teller windows could feel everything they once knew to be solid suddenly melting into air.

As those older generations grew more comfortable – and as the institutions they trusted offered their support – they grew as capable in their online operations as those ‘digital natives’ born to it. As we find our comfort zone, we ‘export’ these technologies from our homes and personal lives. They enter our workplaces and organisations, and soon we use all of them (including governments, all too often the slowest adopters) to deliver their services using these newly comfortable channels.

This pattern pops up repeatedly in the Unisys Security Index. In 2012 those surveyed indicated a worry about facial recognition technologies. Five years later, Apple and others introduced FaceID (a biometric technology employing machine learning and facial recognition), adding additional security to their mobile devices, and everyone embraced it.

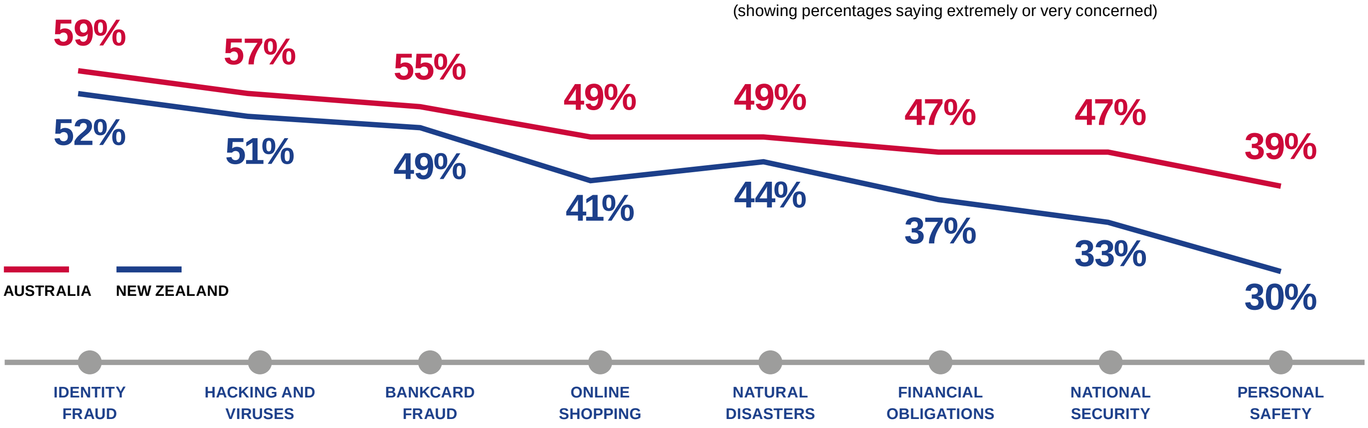
In 2017, only 29% of those surveyed in Australia thought they’d ever use a smartwatch for payments. Just four years (and one ‘touchless’ pandemic later) we think nothing about waving our wrist over an EFTPOS terminal.

Everything feels scary when we first encounter it. When we take the measure of a new technology, we cut our own fears down to size. The pandemic forced so many first encounters on us – at home, in the home office, and in the home school – we have suddenly become sensitised to all of the potential threats presented by all of these new situations and tools. Our anxieties about work and the post-pandemic future have attached themselves to our need for (and the dangers of) continuous, productive connectivity.

As we’ve learned from the history of the Unisys Security Index, our red-hot ‘new normal’ will quickly cool to just plain ‘normal’, as individuals and institutions move toward new levels of understanding and comfort with our new ways of working.

CURRENT SECURITY MINDSET

How concerned are you about the following issues?
(showing percentages saying extremely or very concerned)



> **With the arrival of multiple, highly effective vaccines, the threat of COVID-19 faded, to be replaced in the 2021 Unisys Security Index with concerns amplified by pandemic-driven changes in the way we work. We are online almost continuously – for both work and play.”**

IDENTITY AND INTERNET FEARS DOMINATE

The 2020 Unisys Security Index demonstrated how concerns about the health and safety of our family, and ourselves comprehensively override all others. During a pandemic, other matters recede into the background, but they never vanish completely.

With the arrival of multiple, highly effective vaccines, the threat of COVID-19 faded, to be replaced in the 2021 Unisys Security Index with concerns amplified by pandemic-driven changes in the way we work. We are online almost continuously – for both work and play – as are our children, still being homeschooled.

The survey reveals that Australians and New Zealanders have had very different reactions to this changed environment. In 2021, Australia reported its equal highest overall index score of 159 – still only near the average of the 11 countries surveyed – while New Zealand sits toward the bottom of the global survey, at just 140.

Even so, Australia saw a smaller rise (+2) than New Zealand (+4), possibly owing to the New Zealand public's perception of more effective barriers against the spread of the pandemic.

In both countries, identity theft stands out as the number one security concern – increasing by an extraordinary seven points in Australia. Identity theft has been a perennial concern, visible even in the earliest Unisys Security Indices. As more of our lives move online, people have grown increasingly aware that identity theft puts them at risk for fraud or abuse. There seems to be an age-related component to fears around identity theft – older people are more concerned than the young, perhaps because the young have grown up within a different privacy environment.

Hacking and viruses come just behind identity theft in the survey of people's concerns, likely because the past year has seen a range of high-profile hacks: a ransomware attack that brought the Waikato Health Board to its knees for two weeks; the Colonial Pipeline attack, which cut off the flow of liquid fuels to the East Coast of the United States; and an email-based hack of the West Australian Parliament's computer network.

We are most aware of things that have directly impacted us. Networks empower, but they also make us vulnerable – Australia's 2021 Cyber Threat Report[1] noted a 20% year-on-year increase in reported attacks. Pandemic-enforced isolation only amplifies our sense of vulnerability.

> **Almost three-quarters of respondents in Australia and New Zealand do not know how to respond when they believe they've been hacked.**

UNISYS | Securing Your Tomorrow®

One result of the survey leaps out: almost three-quarters of respondents in Australia and New Zealand do not know how to respond when they believe they've been hacked.

Feelings of vulnerability multiplied by perceived powerlessness can create a toxic confusion that results either in denial ('nothing bad can happen to me online') or in aversion ('I won't go online, it's too dangerous').

This confusion also shows up in our attitudes toward devices: nearly half (48%) of Australians and 40% of Kiwis say they are less careful with their mobiles than with their laptops – even though smartphones present an increasingly attractive target for hackers.

By identifying these points of confusion, the Unisys Security Index also points to a way through. Only about one in five respondents in Australia had heard of SIMJacking (where an attacker gains control of a user's SIM – and thereby gets access to all of the services accessed via that SIM), except in the Australian Capital Territory, where 70% knew about the practice. Why? Because the public service, headquartered in Canberra, offers significant training and support around online security threats.

This tells us there is a job to do when it comes to education on these points of confusion and concern for our online safety.

1. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

> **"Cyber professionals must work to install zero-trust infrastructure to protect users at all times and ensure education can empower users to protect themselves in an ever-changing cybersecurity landscape."**
>
> **Gergana Winzer**
> Unisys Industry Director of Cybersecurity, Asia Pacific

THERE IS STILL A NEED FOR BETTER CYBER EDUCATION IN 2021, BUT WE CAN'T RELY ON IT

Cyberattacks have increased throughout the pandemic largely due to scammers capitalising on the shift to remote working and people spending more time online. Aussies and Kiwis are aware of this too, with identity fraud, and hacking and viruses our top two concerns when it comes to our personal security.

Australians generally accept responsibility for this when working from home, with 60% claiming that their online safety is up to the individual, rather than their employer or the government.

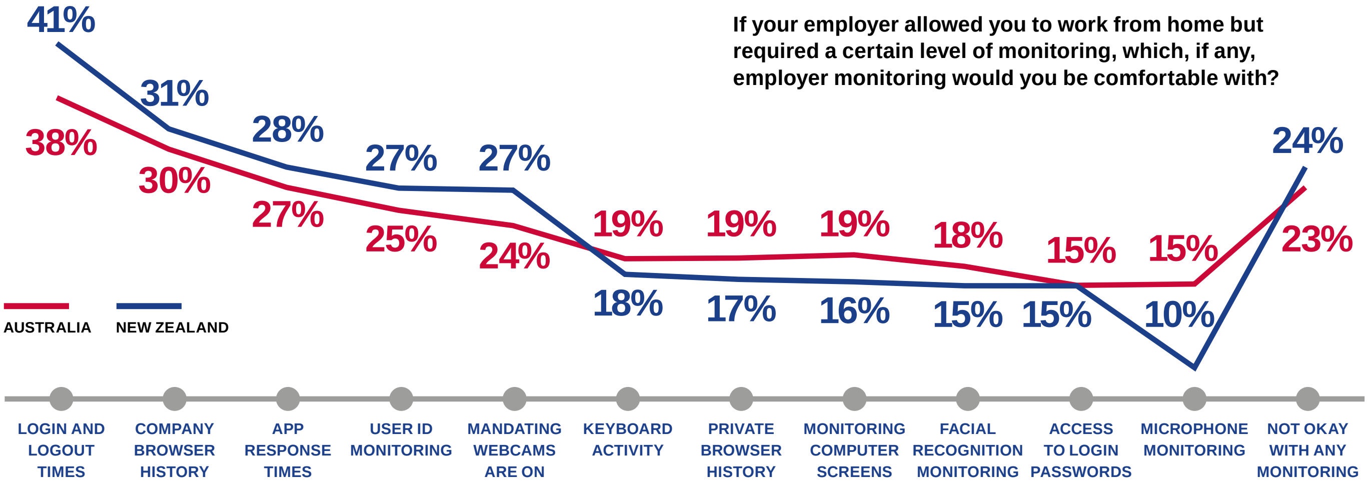
However, the rapid increase in our online activity has allowed cybercriminals to develop new strategies that are infiltrating systems and taking advantage of people who get caught off-guard in their home environment.

While most Australians (61%) and New Zealanders (67%) are wary of a risky link in an email, that still leaves many who will click on it. And more than half (55% of Aussies and 54% of Kiwis) don't know what SMishing (phishing via SMS) is. Alarmingly, nearly three quarters of us don't know when or where to report a cybersecurity breach (73% AU and 74% NZ). These are your employees and customers.

Training in how to handle cyberattacks must continually evolve to ensure people are capable of protecting themselves online, but the onus cannot be placed solely on the user in an age of increasingly sophisticated attacks. Training must be repeated and continually updated to ensure people are alert to new sophisticated threats. But humans will still make bad decisions – accidently or intentionally. So organisations also need a holistic approach to security that also includes processes, policies and technologies to make it extra hard for people to, without intending, do the wrong thing.

Effective protection requires a combination of technology, processes and human behaviour. To achieve this, cyber professionals must create a secure environment that protects users at all times using a Zero Trust security model, with Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE) that is regularly assessed against leading standards and frameworks. In parallel, repeated and updated education about identifying and avoiding cyber threats will empower employees to protect themselves in an ever-changing cybersecurity landscape.

A CHANGED WORK ENVIRONMENT



> **“People clearly want to draw a line around their homes. We will work in our homes, respondents say, but that does not imply permission to allow ourselves to be surveilled in our most private spaces.”**

WFH: WATCHED FROM HOME?

The pandemic significantly accelerated the arrival of ‘work-from-home’ (WFH) or even ‘work-from-anywhere’. Although the essential technologies for WFH have been introduced, piecemeal, over the last decade, 2020’s global-scale lockdowns forced a rapid adoption and integration of these WFH tools, together with a redesign of work practices – while battling non-technology barriers, such as trust and management style, that prevented it happening earlier.

An event that wouldn’t have been conceivable a generation ago – everyone going home without significantly impacting productivity – went off nearly seamlessly. This new knowledge about how we can work together at a distance will not be forgotten, even after the pandemic fades into memory.

Our old workplace habits persist, even where they’re a poor fit to the changed environment. Managers, used to having daily eyeball-to-eyeball contact with their reports look for ways to stay across the operations of their staff. This has quickly become a new area of contention, as employers try to deploy technical solutions to what are, in essence, human questions of trust, transparency, and power.

Six in ten Aussies and Kiwis are not comfortable with employers monitoring their login and log out times when they’re working from home.

Even though employees are monitored more-or-less continuously when in the office: badging in and out of areas, logging onto office IT systems, etc., respondents clearly want to draw a line around their homes. We will work in our homes, respondents say, but that does not imply permission to allow ourselves to be surveilled in our most private spaces.

This resistance becomes even more fierce when it comes to requirements to keep our webcams on during meetings (only 28% of New Zealanders approve of this, and just 24% of Australians), monitoring computer use by facial recognition (AU 18%, NZ 16%), or monitoring via microphone (AU 15%, NZ 10%).

Although many respondents are likely to log onto computers via facial recognition with Windows Hello and smartphones using FaceID or use Siri or Google Assistant to issue commands to their mobiles, they are only happy doing so if they feel they are in control. Handing those controls to employers feels like a violation – although younger workers are more comfortable with employer monitoring than their more senior peers.

At the same time, WFH means that the security threats to the business have suddenly multiplied dramatically, producing significant confusion around who is responsible for securing corporate information. Almost two-thirds of those surveyed believe it is the individual’s responsibility to keep data safe – yet as already noted, three-quarters of them don’t know who to contact to report a data breach.

Almost half of respondents in Australia and New Zealand admit to installing unauthorised software on their devices (which means the actual percentage is likely far higher) even knowing that this could potentially compromise their devices - and the organisations they work for.

Respondents provide a variety of reasons to justify a behavior that could put them and their organisations into jeopardy: some want to use the same tools they use in their personal lives for work purposes; others needed to use a tool and their employer didn't provide an authorised alternative; some said their own choice of tools was superior to the those provided by their employer, or that they simply wanted to use a work device for entertainment or personal reasons. With the exception of this last example, all of these point back to employee experience, exposing a fundamental link between security and employee experience: employees who download unauthorised software in search of a better tool for their work risk creating unsecured links into devices and systems.

Here we hit a paradox: WFH has empowered employees, potentially to make decisions that could be dangerous to the business. Yet, these same employees resist the kind of continuous monitoring that would help detect and potentially thwart attacks before they could cause significant damage.

This highlights a dangerous 'trust gap' between employer and employee. Because neither trusts the other enough, neither feels able to offer the other the kind of support needed to ensure the safety of both.

> **"When adopting an outcome focused workplace, organisations use technology to empower their employees' productivity and ability to get the job done, not spend valuable time monitoring to ensure work is being completed."**
>
> **Leon Sayers**
> Unisys Director of Advisory, Asia Pacific

AT THE HEART OF THE WORKPLACE REVOLUTION IS THE SHIFT IN FOCUS FROM OUTPUTS TO OUTCOMES

The sudden prevalence of remote work was welcomed by many across Australia and New Zealand, who found flexible working practices to be a silver lining to rolling lockdowns. However, a tension between employers and employees has arisen as old office monitoring practices to measure employee performance and productivity are replicated in the home through technology.

This tension can quickly lead to a breakdown in trust between workers and their bosses and undo the progress towards flexible work that's taken place in the last 18 months.

According to the Unisys Security Index, the majority of us are not comfortable with any form of monitoring when WFH. While monitoring of login/logout times is the most accepted among Australians and New Zealanders alike, only 38% of Aussies, and 41% of Kiwis would be comfortable with this taking place.

When adopting an outcome focused workplace, organisations use technology to empower their employees' productivity and ability to get the job done, not spend valuable time monitoring to ensure work is being completed.

To do this, organisations need to look at shifting to solutions that offer positive benefits to employees such as proactive IT support or facial recognition technology for convenience and security, not monitoring login/logout times or screen activity.

There is also an education piece that comes with a shift to outcome-based work. When enabling systems that monitor employee activity, regardless of reason, organisations must be considerate of privacy and security, ensure communication is clear and transparent and clearly convey how solutions will help them do their job better.

By sharing the purpose and the benefits of these tools and solutions, organisations can gain employees' trust and encourage a more productive hybrid workforce.

CONCLUSION

> **“We can and must learn how to trust one another in our work environments. In this decade, ‘fortune favours the flexible’. Organisations that can adapt to change will emerge from the pandemic with both the capacities and the vision to navigate an era of increasing dynamism.”**

THE FUTURE WILL FAVOUR THE FLEXIBLE

The middle years of the 2020s will see individuals and organisations negotiate a range of ‘hybrid’ forms of work: WFH, four-day weeks, new and more well-attuned management styles, etc. The change has already come. Now we need to adapt to it.

Adaptation always increases anxiety. It requires the mastery of new skills, the development of new tools and processes, and the reinvention of business models. In this decade, ‘fortune favours the flexible’. Organisations that can adapt to change will emerge from the pandemic with both the capacities and the vision to navigate an era of increasing dynamism.

As always, our best resources lie with each other. We can and must learn how to trust one another in our work environments. ‘Helicopter management’ will give way to a new respect, one that emphasises outcome over output, and support over surveillance.

All of this rests on a foundation of transparency, trust and empathy.

We know that as the office overtops its boundaries and becomes synonymous with the world-at-large, we need to balance new freedoms with new responsibilities. If the security of the business does call for increased levels of monitoring, then that business needs to lead the conversation – not with demands, but with transparency, clearly informing employees:

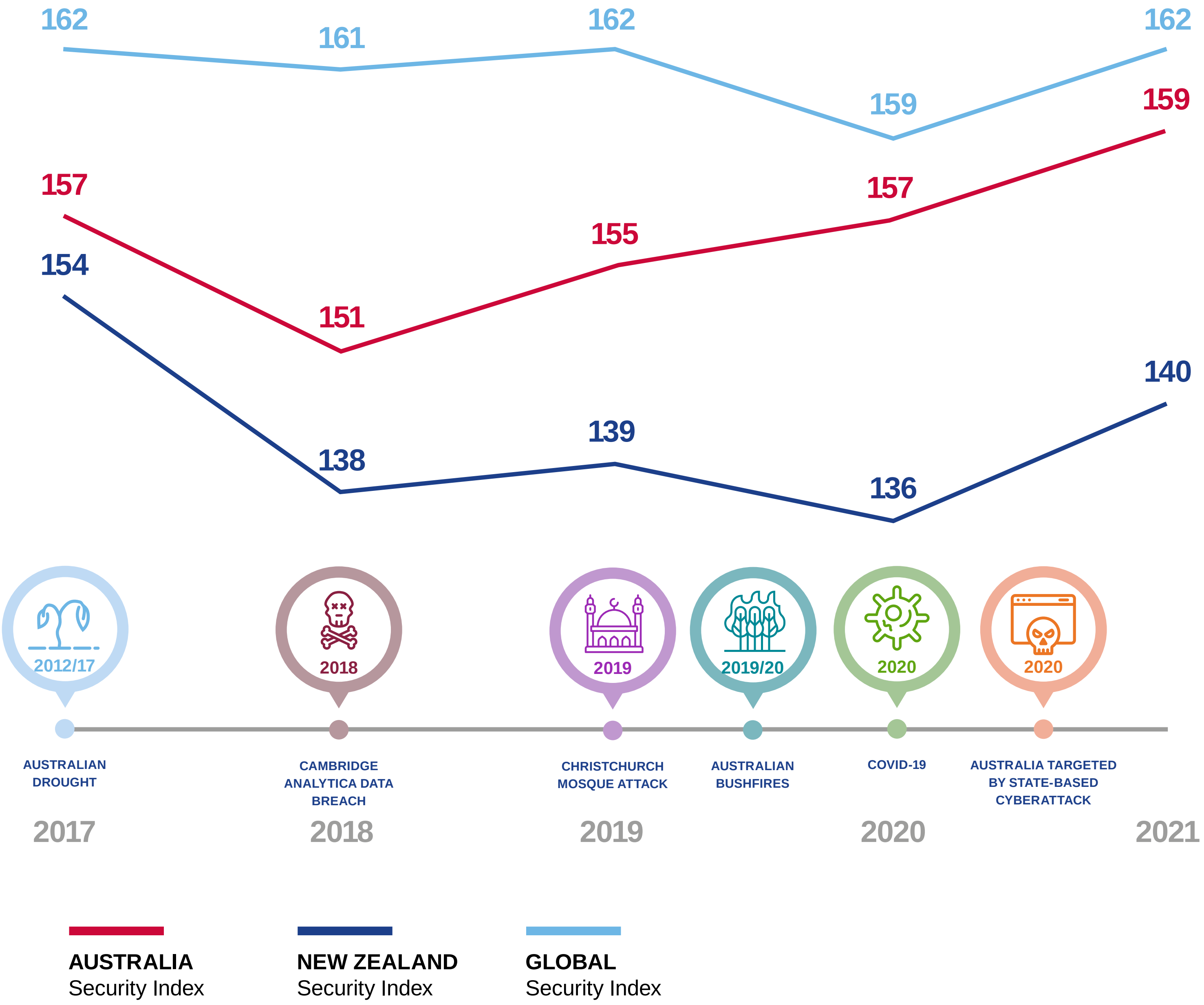
- What monitoring data is being collected – and why?
- How will it be used to protect the employee?
- How will it be used to protect the organisation?
- How long will that data live?

The answers to these questions should not be framed in absolutes, but rather as invitations to a conversation between employer and employee, one that serves to build trust, as both parties co-design a security environment that feels both natural and comforting. We don’t mind being watched over by someone we trust – in fact, we treasure that feeling. That’s what we need to work toward, as office work leaves the office building behind.

Finally, we need to remember that we all have fears for the future – often nothing more than a fear of the unknown. Education, delivered empathetically, dispels the shadows of fear, builds trust, and offers a path into a safer and more secure world.

If you’d like to learn more about the Unisys Security Index, and how Unisys can provide solutions to enhance the security of your organisation, please visit **unisyssecurityindex.com**

DISRUPTIVE EVENTS DRIVE EVOLVING SECURITY CONCERNS OVER TIME



UNISYS SECURITY INDEX METHODOLOGY

Launched globally in 2007, the Unisys Security Index is the longest-running snapshot of consumer security concerns conducted globally covering a broad range of financial, internet, national and personal security issues. The 2021 Unisys Security Index surveyed 11,000 adult consumers in 11 countries, including 1,000 each in Australia and New Zealand. The online survey was conducted 2-28 July 2021. In all countries, the sample is weighted with respect to national adult demographic characteristics such as gender, age, and region.

UNISYS | Securing Your Tomorrow®

unisyssecurityindex.com