New Zealand Summary

The 2019 Unisys Security Index™ surveyed more than 1,000 consumers in New Zealand, as part of an international study of more than 13,000 people across 13 countries, to gauge the public’s concern about various security issues and how they change over time.

The research was initially conducted in February 2019, before attacks on two Christchurch mosques on 15 March. As the attacks had such an impact on New Zealand society, media commentary and political priorities - both domestically and internationally - the research was re-fielded two weeks after the 15 March attack to gauge the impact on the security concerns of New Zealanders.

In February 2019, the overall measure of security concerns of the New Zealand public was 139 out of 300 – relatively unchanged from 138 in 2018. After the attacks the index rose to 143. Despite this increase, New Zealand has the third lowest level of concern of the 13 countries included in the survey, higher only than Germany and the Netherlands, and is well below the global average. However, the type of security concern has changed.

Prior to the attacks, New Zealanders ranked concern about war or terrorism only seventh out of eight types of security concerns. But New Zealanders’ attitudes toward their security changed immediately after the attacks, with war or terrorism now cited as the top security concern for Kiwis for the first time in 13 years with 51% of New Zealanders very/extremely concerned about this issue, up from 29% before the attacks. In Christchurch the concern about war or terrorism is even higher, with 58% of residents seriously concerned.

Before the attacks, New Zealanders had the lowest level of concern about criminal attacks at large events such as sporting World Cups and music festivals of 13 countries surveyed. Their concerns were primarily data security related, with 39% seriously (extremely/very) concerned about credit card data theft, and 38% seriously concerned about personal data theft through public Wi-Fi at such events. Fears of a criminal attacking and harming event attendees were lower, with 35% seriously concerned.

After the attacks there is also a clear public expectation on the role of social media to identify and prevent malicious activity. The vast majority, 80%, of New Zealanders believe social media companies are responsible for monitoring and removing inflammatory content, such as hate speech and racist memes. And more than half (56%) of New Zealanders agree that police, law enforcement and other government agencies should be able to access and monitor all social media channels to look for disturbing content and malicious activities. Overall, twice as many believe that free speech on social media should be monitored (43%) than believe that people should be able to post whatever they like on social media (25%).

While social media monitoring is welcomed, listening technology is less so. Forty percent of smart device owners say they have started receiving social media posts and ads about a topic they had recently talked about aloud, and more than half of that group are concerned about it.

Given this, it is unsurprising that New Zealanders prefer data to be collected by the government than by private companies. Nearly half (47%) support data collection for emergency service provision, while just 14% support data collection by retailers.
Global Summary
The Unisys Security Index has tracked security concerns around the globe for more than a decade and found those concerns to grow significantly over the past five years. This year, the global level of security concern was measured at its highest level since the survey began in 2007.

The 2019 Unisys Security Index stands at 175 (out of 300) globally, a two point increase since 2018. For the third consecutive year, Identity Theft and Bankcard Fraud continue to be the two most pressing concerns worldwide. Identity Theft continues to rank at the top out of the eight security threats measured by the index, with more than two thirds of those surveyed (69%) seriously concerned – exceeding reported concern related to National Security threats like war or terrorism and natural disasters. Bankcard Fraud also remains one of the top two security concerns globally, with two thirds (66%) of consumers seriously concerned about it.

Increasing internet security concerns are largely behind the rise in this year’s Unisys Security Index. Nearly two thirds (63%) of consumers report they are seriously concerned about the threat of Viruses/Hacking with more than half (57%) seriously concerned about Online Shopping and Banking.

In general, consumers in developing countries registered higher levels of concern than those in developed countries. Consumers in the Philippines reported the highest level of security concern of the 13 countries surveyed, and consumers in the Netherlands registered the lowest level – although their concern is rising. Younger respondents and those with lower incomes have higher security concerns in general.

The survey expanded its enquiry this year to include a look at the level of concern consumers register when they gather in large numbers at events such as the World Cup or large musical festivals. Following large public attacks around the world in the last year, the survey found that global security concern is high among consumers about attending these types of events.

Interestingly, consumers reported they are as fearful of having data stolen at large events as they are of being physically harmed. While 57% of respondents in the 13 countries surveyed registered serious concern (extremely/very concerned) about falling victim to a physical attack at a large event, the same percentage registered serious concern about having their personal data stolen when using public Wi-Fi at these events, and 59% were seriously concerned about someone stealing their credit card data.

Consequently, about a quarter of respondents globally (28%) have changed their plans to attend certain large-scale events and nearly four in 10 (39%) said they would “think twice” about attending. A quarter of those who have not changed their plans report they will take extra precautions about securing mobile devices and wallets.

1 The Unisys Security Index defines a “developed” country as one in which the gross domestic product per capita is measured at $12,000 or more.
The Unisys Security Index: 13 Years and Counting

Unisys Corporation (NYSE: UIS) launched the Unisys Security Index – the longest-running snapshot of consumer security concerns conducted globally – in 2007 to provide an ongoing, statistically-robust measure of concern about security. The index is a calculated score out of 300\(^2\) that measures consumer attitudes over time across eight areas of security in four categories:

The 2019 Unisys Security Index is based on national surveys of representative samples of at least 1,000 adult residents aged 18-64 years of age in each of the 13 countries surveyed, 13,598 in total. Interviews were conducted online 27 February–22 March, 2019. An additional question about security concerns at mass events was conducted 3 April–12 April, 2019 in some countries.

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 13 countries’ respective security indices. The margin of error is +/-3.1% per country at 95% confidence level and +/-0.9% for the global results.

The 2019 Unisys Security Index survey was conducted by Reputation Leaders, a global thought leadership consultancy delivering compelling research that causes people to think about brands differently.

---

\(^2\) The survey ranks concerns from zero to 300. One hundred means “somewhat concerned,” 200 means “very concerned” and 300 means “seriously concerned.”
Key Findings: New Zealand

The 2019 Unisys Security Index for New Zealand is 139 out of a maximum of 300 (rising to 143 post-Christchurch attack), where 300 represents the highest level of concern. This is up from 138 in 2018.

New Zealand has the third lowest index of the 13 countries surveyed and the lowest of the four Asia Pacific countries included in the study (Australia, Malaysia, New Zealand and the Philippines).

In New Zealand, the level of concern varies by gender, age and geography. In 2019 women are more concerned than men, people in the North Island are more concerned than those in the South Island, and younger New Zealanders aged 28-24 years are the most concerned age group and the level of concern drops with age.

The post-Christchurch index is a four point increase on the pre-Christchurch index and five points ahead of 2018 score, but 2019 still remains lower than the peaks seen in 2012 and 2016-17.
Concerns About War or Terrorism Escalate After the Christchurch Attacks

Prior to the Christchurch attacks on 15 March, 2019 New Zealanders’ top concerns centred on data security and natural disasters. The top three concerns were about computer hacking and viruses (52% of New Zealanders seriously concerned), online banking and shopping (52% seriously concerned) and natural disasters such as earthquakes, tsunamis or bushfires (47% seriously concerned). Threats to National Security in relation to war or terrorism ranked second lowest (29%) with only concern about personal safety lower (24%).

But New Zealanders’ attitudes toward their security changed immediately after the attacks, with war or terrorism now cited as the top security concern for Kiwis for the first time in the 13 year history of the Unisys Security Index with 51% of New Zealanders very/extremely concerned about this issue, up from 29% before the attacks. In Christchurch the concern about war or terrorism is even higher, with 58% of residents seriously concerned.

Concern about identity theft (49% seriously concerned) and computer hacking or viruses (48%) are also in the top three concerns.

“Clearly our most recent experiences drive our security concerns at a given time. It is no surprise that concern about terrorism in New Zealand has increased. While the attacks targeted Muslims as they worshipped, they registered throughout the country as attacks on all New Zealanders and brought the reality of such a threat into our backyard. However, it is important to note that New Zealanders continue to hold a much lower level of concern than most countries – only Germany and the Netherlands are lower,” said Andrew Whelan, vice president Commercial and Financial Services sectors, Unisys Asia Pacific who is based in Wellington, New Zealand.

New Zealand security concerns differ by age, geography and gender. Younger people aged 18-24 years are significantly more concerned about meeting their financial obligations, online transactions and personal safety than those aged 55-64 years. More females are seriously concerned about meeting financial obligations and natural disasters than males. And the North Island is more concerned about identity theft and personal safety than the South Island, whereas the South Island is more concerned about all other types of security than the North Island (spanning war or terrorism, natural disasters, bankcard fraud, meeting financial obligations, virus/hacking and online transactions).
1. Security Concerns at Large Events and Role of Social Media in Identifying Threats

In polling conducted two weeks before the Christchurch attack that examined the public’s security concerns at large-scale events such as a rugby match or music festival, New Zealanders were more concerned about theft of credit card data (39% seriously concerned) or personal data (38% seriously concerned) from a mobile device when using public Wi-Fi at the event, than a criminal attacking and harming event attendees (35% seriously concerned). Of the 13 countries surveyed, New Zealanders recorded the lowest concern about such criminal attacks.

Social media platforms came under scrutiny after the Christchurch attack was live streamed on Facebook. Polling conducted after the attacks found that the vast majority (80%) of New Zealanders believe that it should be the responsibility of social media companies to monitor and remove content that they deem to be hate speech, racist memes, inappropriate comments and malicious or disturbing content. Only 25% agreed with the statement that New Zealand is a free country and New Zealanders should be allowed to post whatever they like on social media as ‘free speech.’

New Zealanders are also keen to see authorities take control of negative content on social media. More than half (56%) think law enforcement agencies should be able to access and monitor all social media activity, including private chats, to check for malicious activities.
Tim Green, industry manager for Justice, Law Enforcement and Border Security, Unisys Asia Pacific said: “Social media has great value in bringing together people and communities, but other groups, darker in nature, use the same mainstream platforms to promote their causes and lifestyle. Social media platforms enable those groups to be just a few clicks away from our children and those most vulnerable to radicalisation. The Unisys Security Index indicates New Zealanders support legislative change and forgiving some privacy on social media to enable police investigations and intelligence operations to prevent the abuse of this technology.”

10 Tips to Stay Safe at Large Events
Salvatore Sinno, global chief security architect at Unisys, provides the following list of simple steps people can take to stay safe and secure at major sporting events, concerts and festivals:

1. **Only buy event tickets from official channels or websites you trust.** Make sure the website you're using to buy tickets shows the secure padlock icon in the browser and the address begins “https://”. And if ticket prices look too good to be true, they probably are.

2. **Plan ahead and check local authorities’ alerts.** Sign up for any travel or news alerts provided or recommended by the event organisers to receive updates on traffic or news of any potential disturbances on event day.

3. **If you’re going to a crowded event alone, let someone know.** Make sure your friends or family know where you’re going, when you plan to arrive and when you’re expected to return.

4. **Travel light.** There’s no need to take everything you own to a festival. Leave the valuables at home and travel light, with just the essentials – in your pockets if possible.

5. **As soon as you get to the event, survey your surroundings.** Make sure you know where the exits are and agree on a meeting place with your friends in case you should get separated from your group. Know where stewards and information points are so you can speak to someone if you need to.

6. **Update your mobile device and avoid unsecured Wi-Fi networks.** Make sure your phone is updated with the latest software, so it’s as secure as it can be. And only use password protected Wi-Fi. Unprotected Wi-Fi networks could give hackers access to personal or financial data on your phone.

7. **Don’t make electronic transactions with unofficial event vendors.** Be careful with your contactless cards or making mobile transactions, particularly outside event venues. Unscrupulous traders could be gathering your financial data to use or sell to other criminals.

8. **Be vigilant for suspicious activity at an event.** Don’t be afraid to report something you think is unusual, such as unattended baggage or people behaving in a suspicious or threatening way.

9. **Keep your phone charged in case of emergencies.** If possible, take a battery charger pack with you to ensure your phone is always available when you need it.

10. **In an emergency, stay calm and move to the edges of crowds.** Try to leave the area quickly and calmly. If you need to, get away from the incident quickly, hide yourself if need be, call 111 (or 112 from your mobile) when you can, and then let your family know you are safe.
2. New Zealanders Hit Back After Data Breaches

More than a quarter (28%) of New Zealanders say they have suffered a data breach in the last 12 months. This is lower than the other three Asia Pacific countries surveyed on this question (Malaysia 46%, Philippines 36% and Australia 29%). The most common types of breaches were email hacking (8%) and various forms of identity theft: social media profile hijacked (7%), credit card details stolen (6%) and suspicious behaviour in their bank account (6%).

Have you suffered any of the following data breaches or events in the last 12 months?

- My email was hacked: 8%
- My social media profile was hijacked: 7%
- My credit card details were stolen: 6%
- Suspicious behaviour in my bank account or credit card before any money was stolen: 6%
- I was a victim of a social engineering scam where I was called or emailed and tricked to provide my information or make a fraudulent transaction: 5%
- My mail was stolen: 4%
- My customer data held by a retailer was stolen: 2%
- My credit card was stolen: 2%
- My bank account details had been stolen: 2%
- My personal information held by a government department were accessed by someone unauthorized: 2%
- My customer data held by an airline was stolen: 1%

Those New Zealanders who suffered a data breach said they responded in a variety of ways. The most common action, taken by almost half (48%) was to change their password on the relevant organisation’s website and any other websites they were concerned about in a bid to protect their information.

However, many Kiwis took action against the organisations they hold responsible for not protecting their data against data breaches. And this action is designed to impact the bottom line: 14% said they stopped dealing with the organisation, such as closing their account, 11% publicly exposed the issue via social media and 7% took legal action.

If you were in any of the scenarios just described in the previous question, what action did you take?

- Changed my passwords on that organisation’s website and any other sites I was concerned about: 48%
- Replaced my credit card: 37%
- Stopped dealing with that organisation, such as closing your account: 14%
- Changed the lock on my mailbox: 12%
- Publicly exposed the issue via social media e.g., Facebook: 11%
- Changed from paper statements to electronic statements where possible: 7%
- Took legal action: 7%
- Continued dealing with the organisation but not online: 7%
- Continued dealing with the organisation but not online: 4%
- Publicly exposed this issue by taking it to the media: 4%
3. Support for Government and Commercial Organisations Collecting, Analysing and Sharing Personal Data Varies

Data analytics has been hailed by many as the “next big disruptor” across many industries for several years. But today’s hyper-connected world featuring wearable tech, social media, geolocation apps, smart devices and a “digital first” strategy by most governments and organisations to move their services online means that more information than ever about individuals is available for the taking.

However, New Zealanders are discerning about which situations they deem acceptable for an organisation to collect data from social media, online purchases, smartphones and wearable devices. Almost half of respondents (47%) support the government collecting this information to identify who is in the vicinity of a disaster, yet only 20% support the government monitoring an individual’s travel patterns to plan road and public infrastructure. Four in ten (38%) support airports and airlines collecting the information to efficiently guide a passenger’s journey through an airport, but only 10% support an employer doing the same to monitor an employee’s location during the work day.

More than a third (36%) of New Zealanders do not support data collection in any of the situations listed.

In which of the following situations, if any, do you support information being collected from any of your social media, online purchases, smartphone or wearable devices?

- The government being able to identify if I am in the vicinity of a disaster requiring emergency services: 47%
- Airports and airlines guiding my journey through an airport so that I don’t miss a flight: 38%
- The government monitoring my travel patterns so that they can plan road and public transport infrastructure: 20%
- Retailers monitoring my location and purchases so that they can offer me deals personalised to my preferences: 12%
- Banks and insurance agencies contacting me with loan or insurance offers after I have made a large purchase: 10%
- Employers monitoring my location during my work day: 10%
- Transport companies contacting me about deals to deliver goods I have researched online: 10%
- None of these situations: 36%

Similarly, the New Zealand public’s support varies for organisations sharing an individual’s personal information with other organisations. The highest support is for police sharing information with other law enforcement agencies within New Zealand (72%) or internationally (71%) to solve a crime. There is also strong support (67%) for doctors sharing a patient’s healthcare history with other healthcare providers the patient uses for a complete view of the individual’s health. Almost half of Kiwis (47%) support a government-administered proof-of-identity used to confirm a citizen’s identity to access commercial services such as a bank account. However, only 16% support banks sharing a customer’s financial data with another financial service provider to offer a single point of contact for multiple services.

For all scenarios, the most common reason given by New Zealanders for not supporting their data being shared is that they want control over exactly who has access to their personal information. This marks a concern around privacy, rather than the ability of an organisation to secure the data.
“New Zealanders are selective about how and when they support their personal information being collected or shared. They want a good reason before they are willing to forego the privacy of some of their information. To gain public support, organisations must show they can be trusted, clearly explain the purpose of sharing the data and show how it will benefit the individual,” explained Ashwin Pal, director security services Unisys Asia Pacific.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Support</th>
<th>Don’t Know/No Opinion</th>
<th>Do not support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police agencies sharing information with other agencies in the same country to solve a crime</td>
<td>72%</td>
<td>9%</td>
<td>20%</td>
</tr>
<tr>
<td>Police agencies sharing information with other law enforcement agencies internationally to solve a crime</td>
<td>71%</td>
<td>9%</td>
<td>20%</td>
</tr>
<tr>
<td>Doctors sharing your healthcare history with other healthcare providers for a complete view of your health</td>
<td>67%</td>
<td>9%</td>
<td>24%</td>
</tr>
<tr>
<td>A Government administered proof of identity so you can access commercial services such as bank accounts</td>
<td>47%</td>
<td>17%</td>
<td>36%</td>
</tr>
<tr>
<td>Airlines, airports and hotels sharing passenger information for streamlined luggage check-in and delivery</td>
<td>44%</td>
<td>16%</td>
<td>40%</td>
</tr>
<tr>
<td>Cargo/freight companies sharing shipment information with other companies involved in a processing a shipment</td>
<td>35%</td>
<td>18%</td>
<td>47%</td>
</tr>
<tr>
<td>Banks sharing your financial information with other financial service providers to offer you a single point of contact</td>
<td>16%</td>
<td>14%</td>
<td>71%</td>
</tr>
<tr>
<td>Retailers sharing your shopping information with other service providers to offer you relevant special deals</td>
<td>14%</td>
<td>9%</td>
<td>77%</td>
</tr>
<tr>
<td>Social media sites such as Facebook sharing information with retailers and service providers to offer you deals</td>
<td>11%</td>
<td>8%</td>
<td>81%</td>
</tr>
</tbody>
</table>

4. Kiwis Not Comfortable with Smart Listening Devices in Today’s Hyper-Connected World

Today we live in a hyper-connected world – for both individuals and organisations – from smart phones and smart watches through to smart homes and digital assistants. A growing component in this is the rise of voice-activated command driven digital assistants either embedded in smart phones and smart watches or in purpose-built devices such as smart speakers. The Amazon Echo and Google Home are the dominant brands in the US and Europe, while Chinese brands of Alibaba, Xiaomi and Baidu are popular across Asia.

The first devices were introduced just five years ago, but the global smart speaker market is expected to overtake tablets by 2021².

However, as more people have embraced technology, so has the speculation that these devices listen in or monitor conversations even when they haven’t been activated. This section of the study explores the New Zealand’s public’s perception of how emerging technology based on Internet of Things (IoT) and artificial intelligence (AI) might impact our privacy by monitoring our conversations and activity. It asks New Zealanders if they think this is happening, and if so, are they concerned about it: They believe it is and they are concerned.

---

2 – Canalys Media release: Global Smart Speaker Installed Base to Top 200 million by the end of 2019 (April 2019)
Forty percent of New Zealand smart device owners say they started receiving social media posts and ads about a topic they had recently talked about aloud, and 24% say they it concerns them. Just over a quarter (26%) report that while talking aloud the virtual assistant in their smartphone or smart watch had asked them for more information or to repeat themselves even though they had not turned it on. Similarly 23% say that while talking aloud, a voice activated smart speaker had asked them for more information or to repeat themselves even though they had not turned it on. In both cases, approximately half of people who experienced this say that it concerns them.

Have you experienced any of the following?

- I searched for something in a search engine (e.g., a holiday destination or illness) and was then sent ads and spam about that topic via social media. 17% Yes, 19% No, 31% Don’t know.
- I started receiving social media posts and ads about a topic I had recently talked about aloud. 25% Yes, 35% No, 16% Don’t know.
- My smartphone predicts my next destination even though it is not in my calendar, and tells me the expected travel time. 24% Yes, 45% No, 12% Don’t know.
- While I was talking aloud the virtual assistant in my smartphone or smart watch (such as Siri or Alexa) asked me for more information or to repeat myself even though I had not turned it on. 35% Yes, 40% No, 14% Don’t know.
- While I was talking aloud a voice activated smart speaker (such as Amazon Echo or Google Home) asked me for more information or to repeat myself even though I had not turned it on. 38% Yes, 39% No, 11% Don’t know.
The Unisys Perspective

CONSUMER CONCERN IS GROWING ACROSS THE BOARD

Given the political turmoil of recent years, combined with reports of incidents of physical violence and a seemingly endless series of cyber attacks on both governments and private enterprises, it comes as no surprise that the 2019 Unisys Security Index reports the highest-ever level of global security concerns among individuals in the years that the survey has been conducted. “There are security concerns in every sector of the world, in every industry, in everything that you do – and it's overwhelming,” says Chris Kloes, vice president of Unisys Security Solutions.

The continued growth in concern may be at least partially a product of greater awareness on the part of consumers of threats that exist both online and off. This growing recognition has caused consumers to lose trust in organisations that handle their personal data.

"Society is starting to wake up now and say, 'My personal information really is important, and I'm learning that people can do really bad things with it. For example, I've been alerted by the Government Tax Department that my social security number was being used to impersonate me. Until they contacted me, I had no idea this was going on. This seriously affects me directly'," says Jeff Livingstone, Unisys Vice President and Global Head of Life Sciences & Healthcare.

“In the world of healthcare, public concerns related to personal data security and privacy are increasing rapidly,” Livingstone continued. “And it's largely because, up until two years ago, highly-publicised attacks and massive releases of private information were not as proliferative as they are today. Another contributing factor is that financial and billing processes in healthcare organisations are highly “laggy”. Often there is substantial time between a medical service and the patient’s receipt of the actual bill. This gives hackers a large window in which they can do terrible things. Healthcare data can be used to establish entire online personas, and for this reason is much more valuable to cybercriminals than classic financial information. The value of healthcare information on the black market is exponentially increasing. Hence all these factors have come together in sort of a perfect storm, aimed directly at the healthcare consumer.”

Maria Allen, vice president and global head of Financial Services at Unisys, points to a similar trend at financial institutions. “There’s much more information out there, and the banks have become more open to digital solutions and automation, all of which is bringing some additional focus and additional concerns on the part of consumers about all aspects of security,” Allen said.

Ironically, the trend is exacerbated by attempts by healthcare providers and those in other industries to improve service to their clients through technology, Kloes notes. “Many organisations are now using technology to put more decision-making power in the hands of the consumer with things like new apps and home-based devices,” he said. “All of those things now create a risk for which neither the consumer nor the service provider is fully prepared. The consumer will make the incorrect assumption that the apps on his or her phone have been vetted and are secure, and there will be an inevitable collision between the consumer’s perception and the ability to serve that consumer from a cybersecurity perspective.”

SECURITY CONCERNS EXTEND TO LEISURE ACTIVITIES LIKE ATTENDING LARGE-SCALE EVENTS

Governments and private organisations have long been focused on ensuring the physical safety of attendees at global events such as the Olympic Games or the various World Cups. In recent years, however, several highly-publicised tragedies at concerts and other large gatherings have prompted concerns related to events that take place at a regional or local level. In addition, the 2019 Unisys Security Index results show that consumers are just as concerned about the security of their data at public events as they are about their physical security – in New Zealand they are even more concerned about the cyber threats than the physical ones.
This raises the question of how government public safety agencies, event organisers and others address the broad array of concerns raised by consumers.

Mark Forman, Unisys vice president and global head of Public Sector, says some governments and enterprises are finding ways to proactively deal with new threats. “Proactive defence requires a combination of technology, education to increase cyber security awareness and to support the development of skilled cyber security professionals.”

IDENTITY THEFT CONTINUES TO BE VIEWED AS A HUGE THREAT
Unisys chief information security officer Mathew Newfield notes that consumers’ growing dependence on online identities extends to nearly every aspect of their lives. “From my perspective, I see identity theft as encompassing a lot of other parts of the security conversation,” said Newfield. “I think there’s been an awakening in the world that if someone steals your identity, they’re getting to your bankcard, your finances, your tax returns, your online shopping and more. And when they start realising that someone can buy identities in bulk for less than a dollar apiece, I think people are getting scared.”

Newfield added that the consequences of identity theft can vary from country to country. “In 2018 the European Union adopted the General Data Protection Regulation (GDPR) to tighten rules about how companies harvest and manage data, with hefty penalties for violators. Similarly in New Zealand the Privacy Act controls how organisations collect, use, disclose, store and give access to personal information, however currently it is not a mandatory requirement to report data breaches. Whereas in Australia, under the Notifiable Data Breaches (NDB) scheme, Australian Government agencies and the various organisations with obligations to secure personal information are mandated to notify individuals affected by data breaches that are likely to result in serious harm.”

Conclusion
Consumer concern continues to grow around the world, in all areas of security and across all sectors and industries. These concerns have profound implications for the companies and government agencies they rely upon to protect them and their data. These organisations must prioritise security to address these concerns, starting with a Zero Trust approach to identify all actors, systems and services operating within the enterprise.
Calls to Action
So, what can businesses and governmental agencies that serve consumers do? Unisys believes there are tangible steps they can take.

1. **Continue to move toward adoption of a Zero Trust security model that assumes all network traffic is a potential threat.**

The continued increase in consumer concern about online security reflected in the 2019 Unisys Security Index underscores the continuing imperative to take all measures possible to assure clients that their data is protected when they work with an organisation.

Unisys recommends a five-step methodology as a roadmap for getting to a complete, start-to-finish Zero Trust implementation. The five steps to Zero Trust are:

- **Prioritise:** The Zero Trust journey starts with total ecosystem visibility, enabling organisations to understand their vulnerabilities and set priorities.
- **Protect:** Based on their priorities, organisations must first protect their most vulnerable people, devices and networks, and then extend protection to all.
- **Predict:** Organisations must get ahead of threats and strengthen their risk postures with AI-powered predictive threat prevention and objective, data-driven, cyber risk forecasts.
- **Isolate:** Organisations should isolate critical data and systems, preventing access from rogue users.
- **Remediate:** Unisys helps organisations minimise the operational impact of attacks by reducing their incident response time.

2. **Technology is important for addressing consumer security concerns, but people are important, too.**

The best security technology can go a long way toward analysing network activity and identifying security issues before they escalate. But even the best technology won’t be effective without experts possessing the ability to interpret and act upon information received. Unisys recommends that organisations focus on both technology and people in order to meet the expectations of increasingly concerned customers.

"Security is a multi-dimensional discipline," says Forman. "Technology can do a lot in terms of assembly and analysis of information, but you need a way to engage the right people in using the insights. We see this, for example, with border security technology, which often is focused on data analysis but lacks the ability to communicate insights in a timely and useful manner needed to stop a threat. Unisys recognises that the last mile is the big gap in many of these tools that must be addressed."
3. **Address the risk associated with the growing number of devices in and around the enterprise and where employees are taking them.**

The results of the 2019 Unisys Security Index clearly illustrate the slowly disappearing line between physical and online security. And as mobile devices proliferate throughout the enterprise, employees are also taking them to physical locations where they may encounter a high amount of cyber risk. While many enterprises work hard to guarantee the physical safety of their people, the safety of their data may not be getting as much attention as it requires.

Programs in which employees were travelling to high-risk areas are issued temporary, prepaid burner devices are helpful in terms of allowing them to work more safely and without as much risk to the enterprise. Organisations also should provide clear guidance to their people on what to do and what not to do when operating in risky physical environments.

"A lot of companies are missing the opportunity to help their associates, employees and executives to work safely when they travel to areas where security concern is high," says Livingstone. "Companies should not only safeguard these employees' devices and data but also provide guidance such as, 'Do not go to specified risky areas, only accept rides in specified types of vehicles, do not get a first-floor hotel room and so on.'"

For more information on Unisys security offerings, visit: [unisys.com/security](http://unisys.com/security).

**About Unisys**

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most demanding businesses and governments on Earth. Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing. For more information on how Unisys builds better outcomes securely for its clients across the Government, Financial Services and Commercial markets, visit [unisys.com](http://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** including war or terrorism and natural disasters or epidemics; **Financial Security** spanning bankcard fraud and the ability to meet financial obligations; **Internet Security** concerns of viruses/hacking and online transactions; and **Personal Security** concerns around identity theft and personal safety. The 2019 Unisys Security Index is based on online surveys conducted 27 February–22 March, 2019 of nationally representative samples of at least 1,000 adults in each of the following countries: Australia, Belgium, Brazil, Chile, Colombia, Germany, Malaysia, Mexico, Netherlands, New Zealand, Philippines, the U.K. and the U.S. The margin of error at a country level is +/-3.1% at 95% confidence level, and +/-0.9% at a global level.

For more information on the 2019 Unisys Security Index for New Zealand visit [unisyssecurityindex.co.nz](http://unisyssecurityindex.co.nz) and for all 13 countries visit [unisyssecurityindex.com](http://unisyssecurityindex.com).