2019 **UNISYS SECURITY INDEX™**

GLOBAL REPORT

UNISYS | Securing Your Tomorrow®

Executive Summary

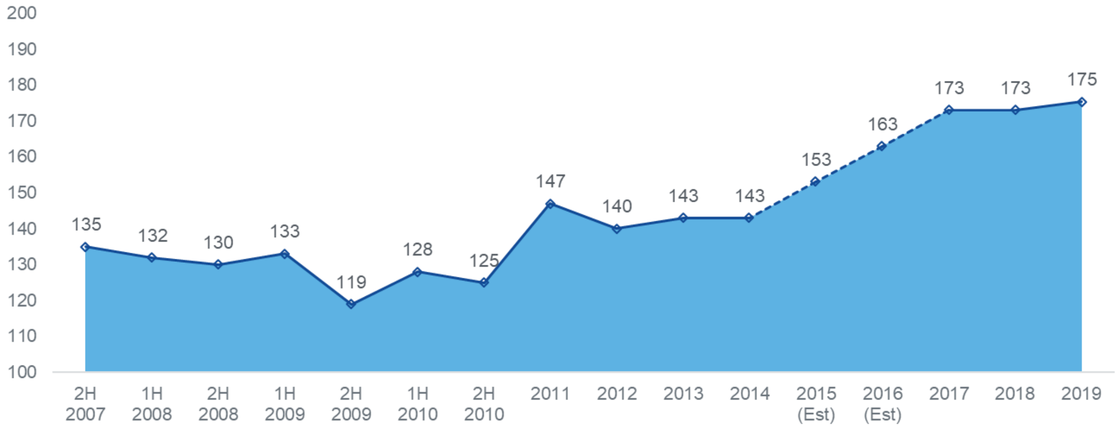
The Unisys Security Index™ has been tracking security concerns around the globe for more than a decade and finding those concerns to be growing significantly over the past five years. This year, global security concern remains at the highest level in 13 years of the Unisys Security Index.

The 2019 Unisys Security Index stands at 175 (out of 300) globally, a 2 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 threats like war, 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[1] registered higher levels of concern than those in developed countries. Consumers in the Philippines reported the highest levels 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.

13 years of the Unisys Security Index



The survey expanded its inquiry 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 (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 are not changing their plans reported they will take extra precautions about securing mobile devices and wallets.

[1] Developing countries are defined as <$12,000 per capita GDP.

The Unisys Security Index: 13 Years and Counting

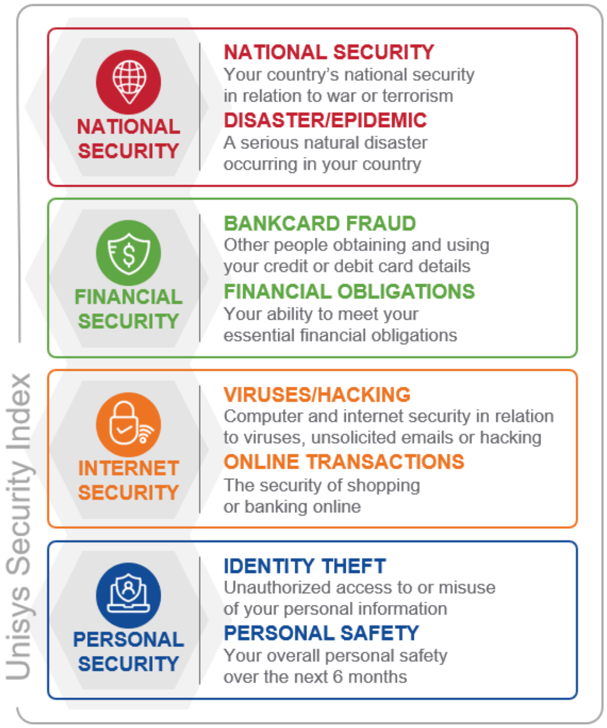
Unisys Corporation (NYSE: UIS) launched the Unisys Security Index – the longest-running snapshot of consumer security concerns conducted globally– in 2007 to provide an ongoing, statistically-robust measure of concern about security. The index is a calculated score out of 300[2] that measures consumer 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 13,598 adult residents aged 18-64 years of age. Interviews were conducted online in each of the 13 markets. All national surveys were conducted February 27-March 22, 2019. An additional question on mass events was conducted April 3–April 12, 2019.

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.



Unisys Security Index

NATIONAL SECURITY

NATIONAL SECURITY
Your country's national security in relation to war or terrorism

DISASTER/EPIDEMIC
A serious natural disaster occurring in your country

FINANCIAL SECURITY

BANKCARD FRAUD
Other people obtaining and using your credit or debit card details

FINANCIAL OBLIGATIONS
Your ability to meet your essential financial obligations

INTERNET SECURITY

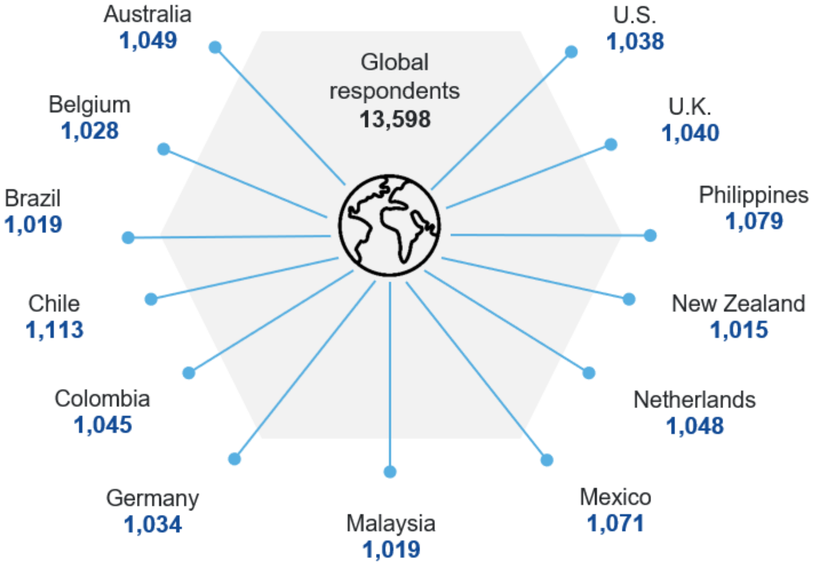
VIRUSES/HACKING
Computer and internet security in relation to viruses, unsolicited emails or hacking

ONLINE TRANSACTIONS
The security of shopping or banking online

PERSONAL SECURITY

IDENTITY THEFT
Unauthorized access to or misuse of your personal information

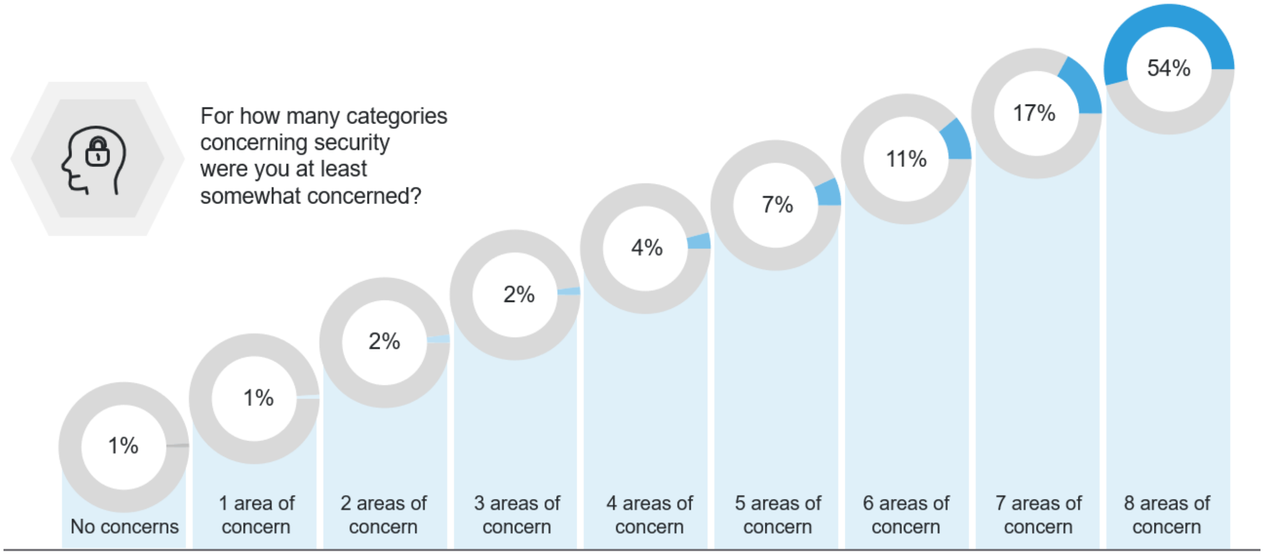
PERSONAL SAFETY
Your overall personal safety over the next 6 months



[2]. The survey ranks concerns from zero to 300. One hundred means "somewhat concerned," 200 means "very concerned" and 300 means "seriously concerned."

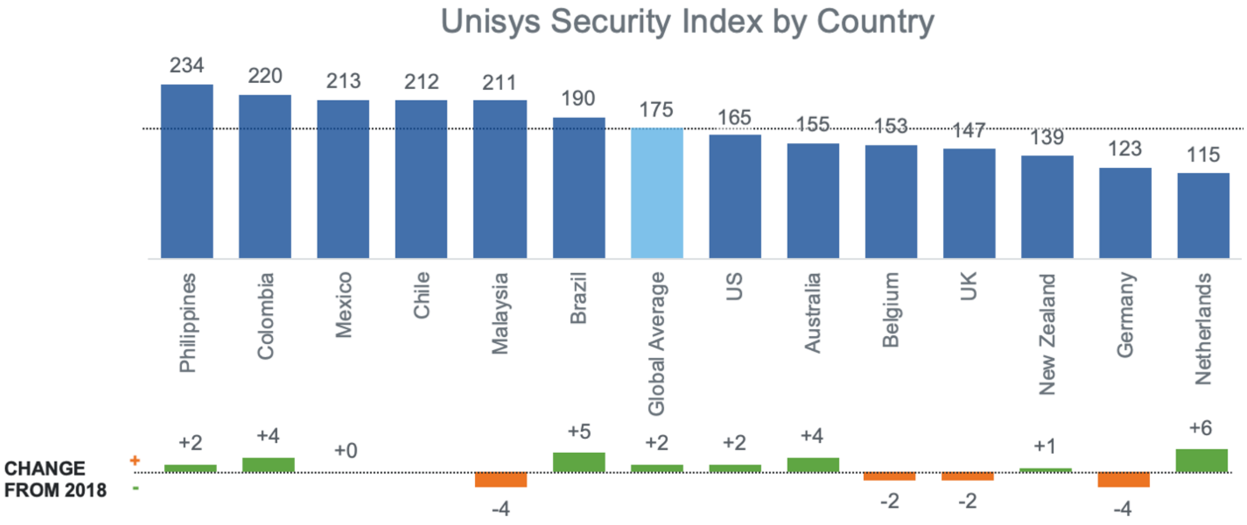
Security Concerns Remain at Historical High In 2019

Globally, nearly all consumers (99%) are at least somewhat concerned about at least one security area affecting their lives both online and off, and more than half (54%) are concerned with all areas.



Strong Regional Differences Still Exist in 2019

Security concerns saw a slight decrease in four out of 13 countries in 2019, most notably in Malaysia and Germany. However, these decreases have been offset by moderate increases in concern in Colombia, Brazil, Australia and the Netherlands.



However, the index continues to be highest in developing countries such as the Philippines and Colombia and lowest in developed countries like Germany and the Netherlands (despite a six-point increase).

Experiencing a two-point rise in concerns in 2019, the Philippines still ranks as reporting the highest level of overall security concern of all 13 countries surveyed, registering 234 points out of 300. As a region, Latin America has the highest overall security concerns and Europe has the lowest.

Global Security Concerns In 2019

With increasing global media coverage of data breaches and hacking scandals involving the personal and financial data of millions of consumers, data security concerns drive the rise in this year’s Unisys Security Index.

The end of 2018 saw Western countries accusing adversarial nation-states of running global hacking campaigns and social media giants suffering their worst data beaches yet, with hackers accessing digital login codes allowing them to take over millions of user accounts. Despite the introduction of new data protection regulations across all regions, the steady drumbeat of media coverage surrounding data leaks and hacking scandals has resulted in a sustained increase in data security concerns globally.

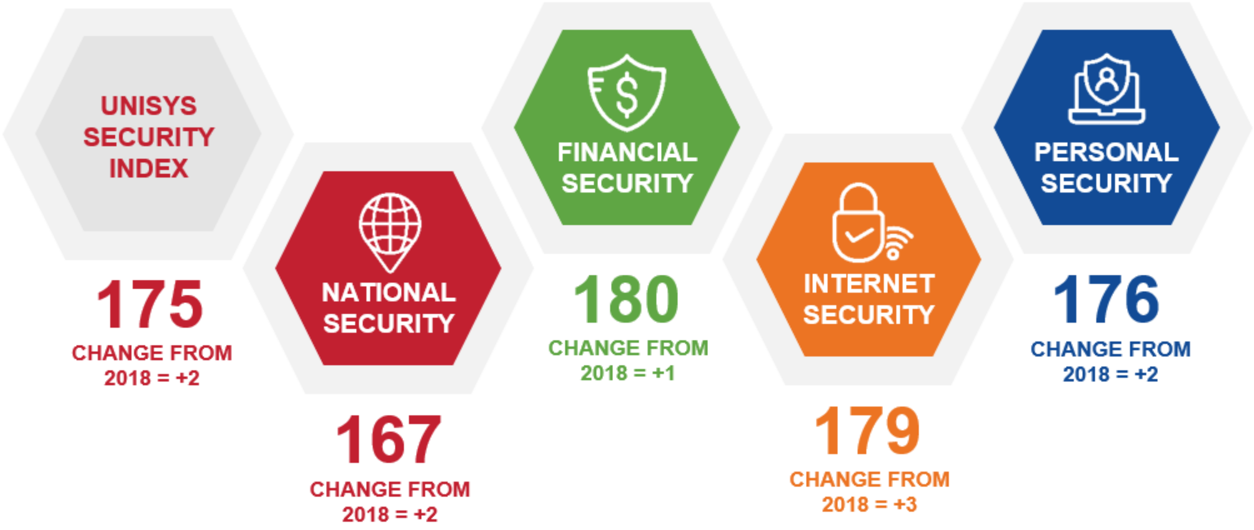
Consumers are as concerned about their data security as their physical safety, even when attending large events like the World Cup and musical festivals, where they fear their data can be accessed and misused through accessing public Wi-Fi. In Latin America, for example, four in five consumers reported they experienced cyber threats targeting them or someone they know over the last year.

Changes in the Global Concern

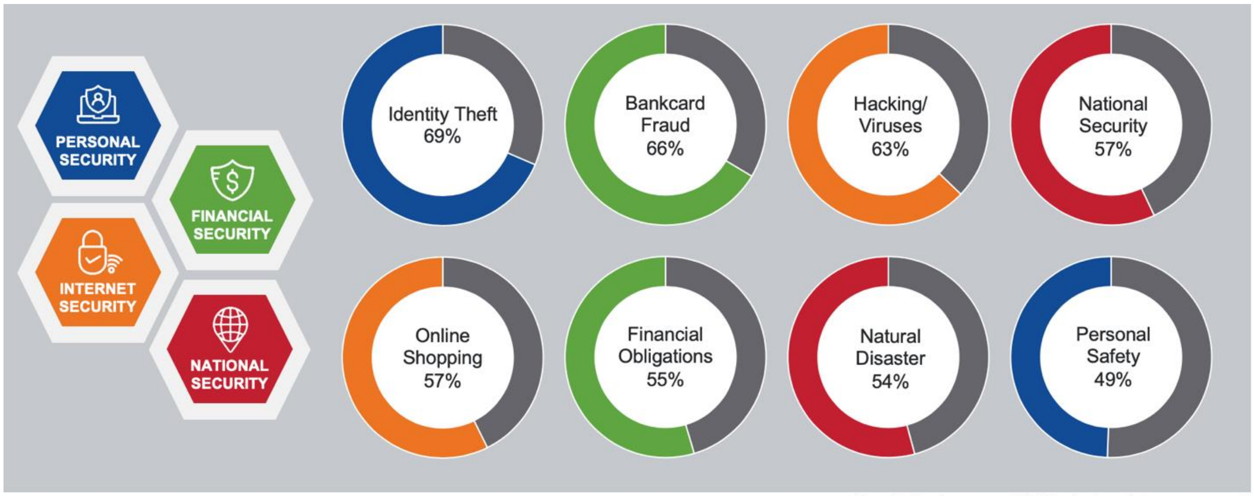
Reviewing the trends that sit behind the Unisys Security Index components

The Unisys Security Index increased slightly in 2019, continuing a pattern of gradually increasing global concern that began in 2013. This year, the survey reported slight growth in all four of the security categories covered: Financial Security, Internet Security, Personal Security and National Security.

Concerns around Internet Security saw the biggest increase compared to 2018, rising three points. Concerns about Identity Theft and Bankcard Fraud continue to eclipse worries about threats from War or Terrorism or Natural Disasters and Epidemics. However, National Security concerns, on the whole, rose by two points.



Identity Theft and Bankcard Fraud are the highest concerns for the third year running



% are "seriously concerned" (NETs of extremely + very concerned)

Financial Security (**Bankcard Fraud and Financial Obligations**)
Of the four security categories measured by the survey, Financial Security continues to be the area of greatest concern around the world, increasing one point to a record high of 180 out of 300 (a four-point increase since 2017). While technological developments in smart FinTech applications have brought convenient new payment and banking solutions to consumers globally, the security of these solutions appears to remain an area of high concern among consumers.

Globally, new payment solutions such as apps and fingerprint and face recognition technology also bring with them new security concerns. Large majorities of consumers in Mexico believe that fingerprint technology will increase their financial security, but one-quarter is concerned it would bring new risks of hacking or fraud from cybercriminals. A similar sentiment is echoed among Belgian consumers, who believe that their smart payment devices are very likely to be hacked in the next year.

The survey results indicate that businesses and government regulatory agencies should consider what more can be done to help arm consumers with the knowledge and tools they need to protect themselves against the dangers of Bankcard Fraud and help them feel less alone in an increasingly digital age. Concerns about Bankcard Fraud remain high among large majorities in Latin America and represent the area of highest concern among consumers in Colombia, Mexico and Chile. With Latin America making significant moves toward widespread digital payment systems and global major payment giants increasing their presence in the region, consumer confidence there is more critical than ever.

Internet Security (Viruses/Hacking and Online Transactions)
From smartphones to cars to locks and even lightbulbs, 2019 has already seen the arrival of new technological solutions that aim to bring efficiency to consumers lives globally. However, the increase in new technology and the increasing amounts of data collected has left consumers in support of a more secure and controlled internet.

Technological developments related to the Internet of Things (IoT) offer efficient solutions to consumers globally, but these solutions come with security concerns. Consumers across the U.K. and the Netherlands are seriously concerned that their voice-controlled technology is listening to them, Germans are worried about the safety of smart cars and drones and Belgians are seriously concerned that connected cars and home devices could be hacked. A vast majority of Americans believe that with the proliferation of new apps and growing amounts of data, it is high time for a more secure and controlled internet.

The 2019 Unisys Security Index illustrates that consumers are as concerned about their safety online as offline. Businesses and governments need to find ways to address consumers' anxieties surrounding the safety of new technological developments, such as voice-controlled devices, autonomous vehicles or drones, as well as online safety on social media platforms.

Personal Security (Identity Theft and Personal Safety)

Concerns about Personal Safety span both the physical and online worlds in 2019. Increasing reports of racially-, religiously- or sexually-motivated hate crime, violence and harassment have dominated headlines for most of the year. Yet the Unisys Security Index once again shows that consumers are more concerned about having their identities stolen and used for nefarious purposes than their overall well-being. Globally, 69% of respondents registered serious concern about Identity Theft – the highest level of serious concern among all eight of the threat areas covered in the survey. On the other end of the spectrum, fewer than half (49%) of respondents registered serious concern about Personal Safety, the lowest level of serious concern of all eight threats.

Also, as seen in previous years, the 2019 Unisys Security Index hints at a widespread perception that consumers do not fully trust the organizations that hold their personally identifiable data. Businesses and government agencies that hold this type of data on their clients or constituents should make its protection the highest priority, while clearly communicating the steps they are taking to keep it safe.

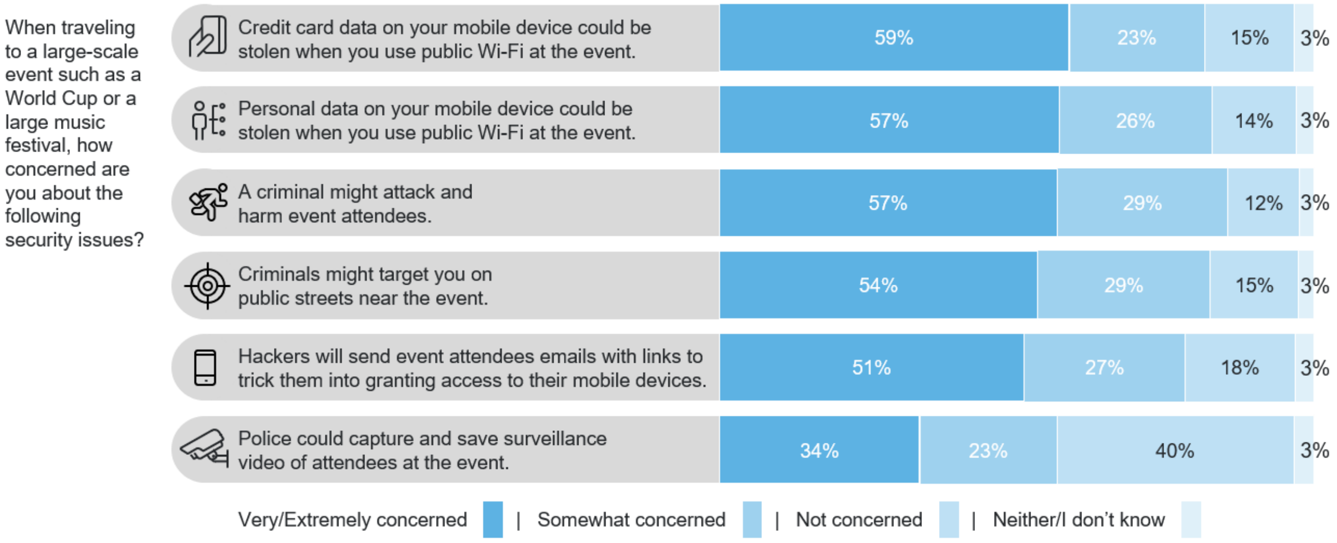
National Security (**National Security and Disaster/Epidemics**)

From wildfires in North and South America to Typhoon Mangkhut, the world's largest storm yet, hitting Southeast Asia, the latter half of 2018 saw a significant increase in natural disasters. Recent terrorist attacks in New Zealand, Sri Lanka and Nairobi provide a backdrop to a rise in national security concerns globally.

The unpredictable nature of both natural disasters and terrorist attacks makes preparedness a challenge. However consumers are wise to embrace secure, end-to-end communication devices and apps along with an awareness of how to manage social media privacy and location settings to secure their personal data and to make their own online world a safer place.

Security Concerns Are High When Attending Large Events

The start of 2019 has seen a rise in large-scale attacks around the world, resulting in consumers globally reporting high security concerns when attending large events such as the World Cup or large musical festivals over the summer period.

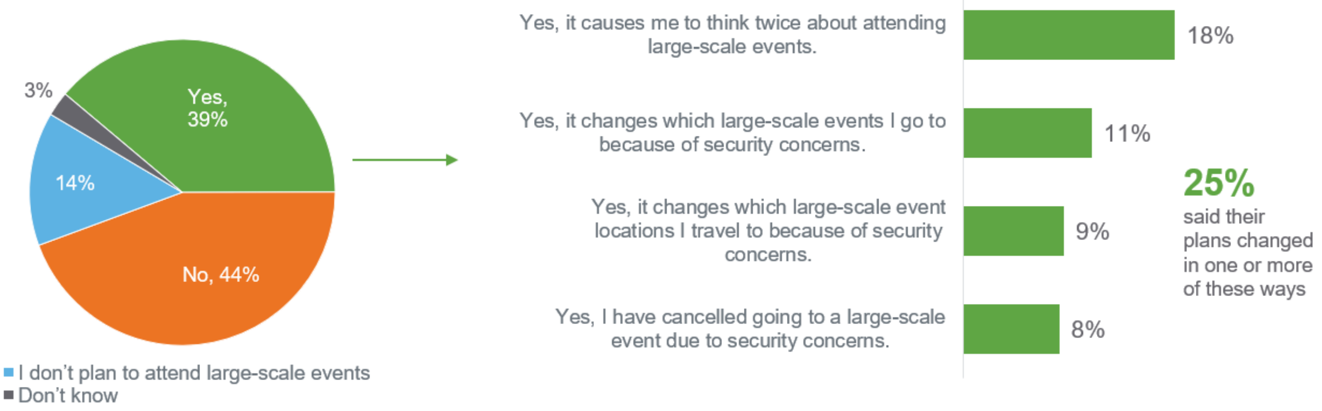


At such events, more than half (57%) of respondents are seriously concerned that a criminal attack may affect attendees, with the highest concern among consumers in the Philippines (86%), Malaysia (75%) and Colombia (74%). Before the Christchurch attack in New Zealand, consumers in that country reported the lowest concern (35%) about criminal attacks harming event attendees, along with consumers in the Netherlands (36%) and Germany (39%). After the Christchurch attack, the percentage of respondents in New Zealand who said they are seriously concerned about terrorism went from 29% to more than half (51%). In Christchurch alone, the percentage more than doubled from 24% to 58% for people seriously concerned about war or terrorism.

Globally, consumers are as fearful of having their personal data stolen as being physically harmed at these events, with 57% seriously concerned about having their personal data stolen when using public Wi-Fi at large events and 59% seriously concerned about having their credit card data stolen. Concerns are highest in Latin America, where nearly seven in 10 consumers were seriously concerned about the security of personal data (69%) and their credit card data (71%) being stolen at large events.

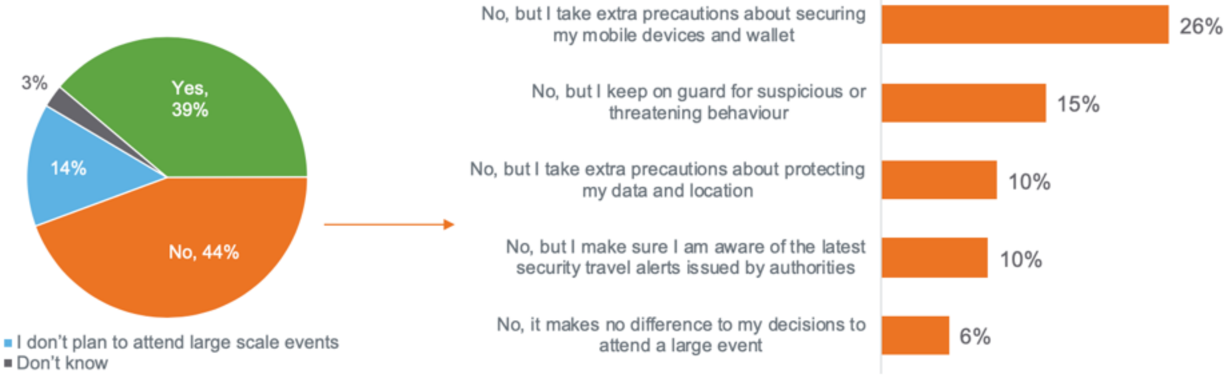
The Unisys Security Index conducted additional research in seven of the countries surveyed (Australia, Brazil, Germany, Mexico, Philippines, the U.K. and the U.S.) and found that about four in 10 (39%) of respondents in those countries said they would think twice about attending these events, and that one-quarter have changed their plans to attend in one or more ways. Levels of concern varied by country. For example, more than half of respondents in the Philippines (56%) and exactly half of those in Brazil (50%) reported they would think twice about attending such events, compared to only 25% of respondents in Germany and 30% in the U.K. and Australia.

Has the possibility of having your data stolen or being subject to physical harm at a large-scale event such as a World Cup or a large music festival caused you to think twice about attending?



Globally, about a quarter (26%) of those who are not changing their plans to attend these events will take extra precautions about securing mobile devices and wallets. But despite high concerns of a criminal attack taking place, only 15% say they will keep on guard for suspicious or threatening behavior. Consumers in Germany (20%) and the U.K. (18%) are the most likely to report that they will stay alert in terms of reporting such behavior. In contrast, countries such as Brazil and the Philippines reported the highest concern about a criminal attack at large events but are least likely to keep on guard for suspicious or threatening behavior, with 10% of Brazilians and 8% of Filipinos reporting they would stay vigilant.

Has the possibility of having your data stolen or being subject to physical harm at a large-scale event such as a World Cup or a large music festival caused you to think twice about attending?



The Unisys Perspective

Staying safe at large events

Salvatore Sinno, global chief security architect at Unisys, provided a list of simple steps for people to 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 organizers 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 at 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, follow the standard police advice of "Run, Hide and Tell. Get away from the incident quickly, hide yourself if need be, call 911 when you can, and then let your family know you are safe.

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 Unisys Security Index reported 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," said 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 organizations 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 Internal Revenue Service 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,'" said 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-publicized 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 organizations 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, pointed 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 noted. “Many organizations 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 organizations have long been focused on ensuring the physical safety of attendees at global events such as the Olympics or the World Cup. In recent years, however, several highly-publicized 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.

This raises the question of how government public safety agencies, event organizers and others address the broad array of concerns raised by consumers.

Mark Forman, Unisys vice president and global head of Public Sector, said some governments and enterprises are finding ways to bring physical and cybersecurity protection together. “In the U.S., fusion centers were created to facilitate collaboration needed for both cybersecurity and physical security. There are U.S. states that have been leaders because they have very good information-sharing practices. And at the end of the day, no matter how much technology you put into it, it's still very much based on people willing to share information, use information from other entities, and do so within a set of operational and policy guidelines. Unless that trust bond is set with local law enforcement, the state and the federal data sources, it's very hard to actually use that information and act on it.”

Unisys Chief Trust Officer Tom Patterson believes that governments in countries such as the U.S. are more focused on the issue than ever. “In the U.S., there is now better cooperation, focus and sharing on ensuring security at very large events,” said Patterson. “Case in point, the Super Bowl, where federal and local law enforcement all work very well together. They produce not just threat intelligence but have also deployed massive drone capabilities. So, we are starting to see that the help is coming with respect to very large private events.”

IDENTITY THEFT CONTINUES TO BE VIEWED AS A HUGE THREAT

Unisys Chief Information Security Officer Mathew Newfield noted 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 realizing 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 the U.S. and some of the more modernized countries, we have protections from the government that kick in if someone were to steal my bankcard," he said. "If I were to lose my money in my bank, I'm protected by the government. And that doesn't happen in every country. So, there can be a life-altering impact for people in different areas of the world."

But Allen asserted that this growing sense of unease among consumers has a silver lining in terms of greater recognition of the threat, and in turn, a consumer base that will be more vigilant as well as more demanding that the organizations they deal with should protect their identities. "Identity theft is a big deal," she said. "And it's about time that the average consumer globally realized it. I am excited seeing this come out of the survey."

CONSUMERS ARE PREPARED TO SHARE BIOMETRIC DATA IN RETURN FOR SAFETY OR CONVENIENCE

The results of the 2019 Unisys Security Index show that biometrics can play a positive role in addressing security fears when consumers travel or shop online. For example, 81% of Americans reported they are comfortable with using biometrics to confirm their identities in airports for reasons most often associated with safety from terrorism or simply convenience. "People will trade some privacy for physical safety," Kloes noted.

Forman added that the question of privacy vs. security is not a zero-sum game or an either/or proposition. "When you're giving up your privacy, you're not giving up your liberty," he said. "You're getting more liberty of movement, with fact-based data and biometrics tools that will make it easier for public safety officials to target the bad actors. Along those same lines, the real privacy and effectiveness are a result of false positives. And the good news is that improved use of technology – including biometrics – can help remove bias and reduce the number of false positives. So, better accuracy and removing bias on who is the real bad actor come together to improve people's feeling of safety."

Unisys Chief Technology Officer Vishal Gupta said biometric identities are becoming an imperative as traditional modes of identity verification become obsolete. "It's straightforward for a hacker to get access to and to impersonate an identity conventionally using the 'name password' method and this has created this identity theft epidemic," said Gupta. "And if you link that up with the high level of bankcard fraud concern, this is perhaps the reason why more and more banks are willing to look at biometrics, because they're realizing that the conventional process is just not working."

GROWING CONCERN MAY BE INFLUENCED BY MEDIA AND POLITICS

Forman noted that the Unisys Security Index measures consumer security perception, which are highly influenced by factors like the media and politics. For that reason, perception may not fully equal reality. "If you look at the parts of the world where you see elevated scores, especially around personal safety, it's often where there are nationalist movements underway, and the politicians have been highlighting security issues," he said. "Perception is always based on what is reported in the media, and that drives fear; it's human nature. So, it's not surprising that there's a link between higher levels of concern and nationalist movements. The question is, is the nationalist movement a result of actual risks, or are these numbers a result of nationalist politicians stoking these fears?"

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 organizations they rely upon to protect them and their data. These organizations must prioritize 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 are protected when they work with an organization.

   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:

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

   > *"IT decision-makers have long recognized that the network perimeter is indefensible in today's technology ecosystem," said Kloes. "Unisys Security Solutions addresses this by implementing a Zero Trust architecture that grows with today's organizations. Leveraging dynamic isolation™ capabilities to quickly isolate devices or users at the first sign of compromise, Unisys identifies, validates and secures trusted users, devices and data flows."*

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

   The best security technology can go a long way toward analyzing 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 organizations focus on both technology and people in order to meet the expectations of an increasingly concerned clientele.

   > *"Security is a multi-dimensional discipline," said 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 recognizes that 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 traveling 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. Organizations 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,” said 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.”*

4. *Protect clients by establishing irrefutable identities using biometrics and other advanced technology.*

Establishing an irrefutable identity has become integral to everyone who conducts a transaction online, wants to gain physical access to a facility, passes through airport security or crosses a border into another country. Government organizations and businesses must commit to making the lives of consumers easier by allowing them to establish their identities while earning their trust by ensuring the highest standards of safety. Internally, organizations need to make the process of identity enrollment and verification simple, tamper-proof, cost-effective and sustainable by leveraging technology advancements.

> *“It is not a stretch to say that our identities are one of the most critical assets we have in our lives,” said Gupta. “The Unisys Security Index clearly shows that people are ready to embrace biometrics as a way to protect them physically and online by confirming their identities as well as the identities of bad actors. Unfortunately, the survey also shows that many consumers do not trust organizations to adequately protect their biometric data. Companies and government agencies must take concrete steps to protect their clients’ personal data, using products like Unisys Stealth® to isolate the most critical data and protect it from intruders who will inevitably find their way into the environment.”*

For more information on Unisys security offerings, visit: www.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 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; viruses/hacking and online transactions, in the Internet Security category; and identity theft and personal safety, in the Personal Security category. The 2019 Unisys Security Index is based on online surveys conducted February 27–March 22, 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, visit www.unisyssecurityindex.com.