U.S. Summary

The 2019 Unisys Security Index™ survey – the longest-running snapshot of consumer security concerns conducted globally – shows security concern among U.S. consumers remaining at its second-highest level since the survey began in 2007. Concern reached its highest level in 2017 but dropped slightly the following year and then increased slightly this year by two percentage points. On a scale of zero to 300, with 300 representing the highest level of concern, the U.S. index is measured at 165, considered a serious level of concern and the highest among the seven developed countries surveyed.

In 2019, Americans are more concerned about Identity Theft and Bankcard Fraud than National Security. Nearly two-thirds of U.S. respondents (63%) are seriously concerned (extremely/very concerned) about the unauthorized access to or misuse of their personal information, and more than half (58%) are seriously concerned about other people obtaining and using their credit or debit card details. Personal Safety concerns also rose by 5 percentage points in 2019, with 42% of Americans now seriously concerned.

In addition, large majorities of Americans express some level of concern when attending large-scale events, such as sporting events or music festivals, where they are just as afraid of having their data accessed by hackers when they use public Wi-Fi as they are of physical criminal attacks.

The survey found that a high majority (83%) of Americans are concerned about a criminal attack causing physical harm at large-scale events— with half of respondents (50%) registering serious concern.

Asked about data safety at such events, 81% of respondents reported some level of concern about someone stealing their personal data when using public Wi-Fi at such events, with 52% seriously concerned. And 78% are concerned about someone stealing their credit card data when using public Wi-Fi at such events — with 52% seriously concerned.

More than one in five (22%) Americans say they have canceled plans or considered canceling plans to attend large-scale public events due to concerns about physical attacks and the safety of their data.

Because many have to travel by air to attend such events, the survey also asked U.S. respondents about their support for using biometric data to verify their identities at airports. The Unisys Security Index found a large majority approved of the use of biometrics for reasons related to security, reliability and convenience. The survey found that 81% of respondents are comfortable with using biometrics for air travel, with 42% citing safety and terrorism prevention as the reason. Those who do not support the use of biometrics for air travel most often cited lack of trust in government or airport authorities or concerns that the data would be lost or hacked as the reasons they do not support it.

The survey also showed that nearly three-quarters of Americans support the use of facial recognition in some situations. For example, more than half (51%) support facial recognition for airport security. Nearly a third (32%) support its use at voting stations.

---

1 The survey ranks concerns from zero to 300. One hundred means “somewhat concerned,” 200 means “very concerned” and 300 means “seriously concerned.”

2 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.
Global 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 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 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.

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 will “think twice” about attending. A quarter of those who are not changing their plans reported they will take extra precautions about securing their mobile devices and wallets.
A report on the global results of the 2019 Unisys Security Index™
©2019 Unisys Corporation. All Rights Reserved
Key U.S. Findings
The 2019 Unisys Security Index for the U.S. is 165 out of a maximum of 300. This is 10 points lower than the global average of 175 but a slight increase of two points over last year’s score. Security concerns in the U.S. are trending upward, just four points below 2017’s peak.

In 2019, U.S. consumers registered the highest level of overall security concern of the seven developed nations surveyed, with higher security concerns than any European country in the study.
Changes in the U.S. Concern

Reviewing the trends that sit behind the Unisys Security Index components

2019 saw an increase in U.S. Personal and National Security concerns over last year

Personal Security and National Security concerns are back on the rise in the U.S., after having dropped significantly in 2018. Meanwhile, Internet Security and Financial Security remain steady as Americans’ leading areas of security concern.

In 2019, the Personal Security index increased to 161 out of 300 — making it the lowest but fastest rising area of concern. The seven-point index rise in Personal Safety was the main reason behind this year’s two-point rise in the overall U.S. Unisys Security Index.

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.
Personal Security (Identity Theft and Personal Safety)

Identity Theft continues as the threat area of highest concern among U.S. citizens in 2019, increasing two percentage points since last year. Almost two-thirds (63%) of Americans are seriously concerned that their identity could be stolen and/or misused — indicating that U.S. consumers continue to feel an overall sense of vulnerability about how their personal data is being captured, stored and used by organizations.

While Americans feel comfortable using advanced technologies such as facial recognition and biometrics for personal identification in certain situations such as airport security, there is less confidence in personal information being securely protected while conducting everyday financial or online transactions.

Americans increasingly feel that their physical safety as well as their online safety are threatened, as indicated by a five-percentage point rise in Personal Safety concerns.

Financial Security (Bankcard Fraud and Financial Obligations)

Financial Security continues to be Americans’ second highest area of concern, remaining steady since 2017 at 167 out of 300.

Concern related to Bankcard Fraud in particular remains high, with 58% seriously concerned – making this the second highest security threat concern among U.S. citizens alongside the threat of war or terrorism.

This indicates that despite convenient new payment and banking solutions, fears about Bankcard Fraud are not being adequately addressed. The security of these solutions appears to remain an area of high concern among consumers.

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.
**Internet Security (Viruses/Hacking and Online Transactions)**

Internet Security concerns remain steady since 2017, at 170 out of 300, with U.S. consumers registering the highest levels of concern of the four security areas covered by the survey for the second year running. The threat of Hacking and Viruses is driving much of the concern around Internet Security, with 57% of Americans seriously concerned about the risks of being hacked or their security compromised while online.

Concerns surrounding Online Shopping and Banking are also increasing. More than half of Americans are seriously concerned about the security of their online shopping and banking activities, an increase of three percentage points since last year.

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.

Overall, 70% of Americans would agree that with the growing amount of data, apps and devices, it is high time to create a new, more secure and controlled internet – with one-third saying they strongly support this idea to protect us against potential cyber threats.

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

National Security concerns relating to war or terrorism remain higher, with 58% seriously concerned, an increase of one percentage point since 2018. This makes war and terrorism the second-highest area of concern among Americans alongside Bankcard Fraud.

Globally, the latter half of 2018 also saw a significant increase in natural disasters, including the deadliest wildfire season on record in California. At an estimated damage cost of $16.5 billion, the devastating and deadly Camp Fire that ravaged California in November was the world's costliest natural disaster in 2018. Consequently, fears of Natural Disasters – such as floods, hurricanes, brushfires or epidemics – are up three percentage points, so that half of all Americans are now seriously concerned.

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 at Large-Scale Events

When attending large-scale events such as sporting events or concert festivals, consumers are just as concerned about having their personal data stolen as they are about physical harm. A high majority (83%) of Americans are concerned about a criminal attack causing physical harm at large-scale events, and a similar number (81%) are concerned about the theft of personal data through public Wi-Fi at the event. Among Americans who registered serious concerns about these events (very or extremely concerned), more are seriously concerned about data theft (52%) than about physical harm (50%).

One in three American respondents (34%) say they will think twice about attending large events, and more than one in five (22%) say they have canceled plans or considered canceling plans to attend large-scale public events due to concerns about physical attacks and the safety of their data. Nearly half (48%) haven’t changed their plans to attend large events, but 44% are taking extra security precautions.
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 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 911 when you can, and then let your family know you are safe.
U.S. Air Travelers Report Comfort with Biometric Identification

A large majority (81%) of U.S. air travelers approve of the use of biometrics as a way to enhance security, reliability and convenience at airports. Four out of five respondents say they are comfortable sharing their biometric data at the airport for at least one reason, preferring safety over speed. More than four in 10 (42%) cite safety and terrorism prevention as the reason they are willing to provide biometric data.

<table>
<thead>
<tr>
<th>Reason (Percentage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I’m willing because I think it will make my flight safer and prevent terrorism. 42%</td>
</tr>
<tr>
<td>I’m willing because I think it’s more reliable than showing an ID card like a driver’s license. 35%</td>
</tr>
<tr>
<td>I’m willing because I think the authorities should know who is at the airport at all times. 33%</td>
</tr>
<tr>
<td>I’m willing if it can get me through airport security faster. 32%</td>
</tr>
<tr>
<td>I’m willing to give my biometric data when traveling by air. 80%</td>
</tr>
</tbody>
</table>

80% of air-travelers are willing to give biometric data to the airport or government.

Reasons air travelers gave for being willing to provide biometric data when traveling by air.

<table>
<thead>
<tr>
<th>Reason (Percentage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>None of the above. I’m not willing to give my biometric data when traveling by air. 20%</td>
</tr>
<tr>
<td>I think this technology is less convenient than showing an ID card like a driver’s license. 17%</td>
</tr>
<tr>
<td>I am concerned that my biometric data could be lost or hacked. 52%</td>
</tr>
<tr>
<td>I don’t trust airport authorities or airlines to possess my biometric data. 55%</td>
</tr>
<tr>
<td>I don’t trust the government to possess my biometric data. 63%</td>
</tr>
<tr>
<td>Other reasons (please write). 2%</td>
</tr>
<tr>
<td>My race or gender doesn’t read as easily on facial recognition software. 4%</td>
</tr>
<tr>
<td>I prefer not to say/ don’t know. 3%</td>
</tr>
<tr>
<td>I think this technology is less reliable than showing an ID card like a driver’s license. 16%</td>
</tr>
</tbody>
</table>

Those who do not support the use of biometrics for air travel most often cite lack of trust in government (63%) or airport authorities (55%), or concerns that the data would be lost or hacked (52%), as the reasons they do not want to share their biometric data.

<table>
<thead>
<tr>
<th>Reason (Percentage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>None of the above. I’m not willing to give my biometric data to the airport or government. 20%</td>
</tr>
<tr>
<td>I’m willing to give my biometric data when traveling by air. 80%</td>
</tr>
<tr>
<td>Other reasons (please write). 2%</td>
</tr>
<tr>
<td>I think this technology is less convenient than showing an ID card like a driver’s license. 17%</td>
</tr>
<tr>
<td>I am concerned that my biometric data could be lost or hacked. 52%</td>
</tr>
<tr>
<td>I don’t trust airport authorities or airlines to possess my biometric data. 55%</td>
</tr>
<tr>
<td>I don’t trust the government to possess my biometric data. 63%</td>
</tr>
<tr>
<td>Other reasons (please write). 2%</td>
</tr>
<tr>
<td>My race or gender doesn’t read as easily on facial recognition software. 4%</td>
</tr>
<tr>
<td>I prefer not to say/ don’t know. 3%</td>
</tr>
</tbody>
</table>
When asked about their concerns related to the use of facial recognition technology in general, nearly three-quarters of Americans (74%) say they support the use of facial recognition in some situations. Acceptance appears to depend on the perceived benefit consumers believe they will obtain through the use of facial recognition. For example, more than half (51%) support facial recognition for airport security, and nearly a third (32%) support its use at voting stations.
**U.S. Consumers Trust AI for Cybersecurity but Not Driving**

When asked their opinions on the use of AI, two in three (67%) Americans support its use for identifying suspicious online activity such as hacker attacks. But less than half support AI replacing human interactions, with just 44% supporting its use for health diagnoses and 37% for self-driving cars or taxis.

<table>
<thead>
<tr>
<th>Application</th>
<th>Strongly Support</th>
<th>Somewhat Support</th>
<th>Neutral-Neither Support or Oppose</th>
<th>Somewhat Oppose</th>
<th>Strongly Oppose</th>
</tr>
</thead>
<tbody>
<tr>
<td>For cybersecurity software to automatically identify suspicious online activity such as possible hacker attacks.</td>
<td>29%</td>
<td>38%</td>
<td>23%</td>
<td>6%</td>
<td>4%</td>
</tr>
<tr>
<td>For border agents to rapidly assess the risk of travelers coming into the country based on their backgrounds and past behaviors.</td>
<td>27%</td>
<td>31%</td>
<td>26%</td>
<td>10%</td>
<td>6%</td>
</tr>
<tr>
<td>To automatically analyze surveillance video on city streets to identify possible criminal behavior.</td>
<td>22%</td>
<td>34%</td>
<td>28%</td>
<td>10%</td>
<td>6%</td>
</tr>
<tr>
<td>For home appliances and devices to adjust themselves, such as thermostats that automatically adjust temperature or refrigerators that warn when perishables are going bad.</td>
<td>19%</td>
<td>33%</td>
<td>31%</td>
<td>10%</td>
<td>6%</td>
</tr>
<tr>
<td>For health care workers to diagnose patients’ symptoms without immediately consulting a doctor.</td>
<td>15%</td>
<td>29%</td>
<td>29%</td>
<td>17%</td>
<td>10%</td>
</tr>
<tr>
<td>Self-driving cars or taxis.</td>
<td>13%</td>
<td>24%</td>
<td>26%</td>
<td>17%</td>
<td>20%</td>
</tr>
</tbody>
</table>
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 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 sort of waking up now and saying, ‘My personal information actually is really important, and people can do really bad things with it. I’ve gotten notices from the Internal Revenue Service that my account has been hacked. I didn't know that was going on. This really affects me directly,’” said Jeff Livingstone, Unisys vice president and global head of Life Sciences and Healthcare.

“In the world of healthcare, for example, concerns related to data security are increasing tremendously,” Livingstone continued. “And it's largely because, up until two years ago, you did not have these highly-publicized attacks and releases of private information. The other thing is that, slowly but surely, people are becoming aware of the problem that financial and billing systems at healthcare organizations have great lags of time between the healthcare activity and the actual billing or financial process. This gives hackers a large time window in which to do terrible things. They are using this healthcare information to set up personas online, and therefore it's far more valuable than, say, the classic financial information. The value of healthcare information on the black market is actually exponentially increasing. So these two things have come together in sort of a perfect storm for 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., we’ve set up fusion centers to cover 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 personal relationships. 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 bank card, 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 bank card,” 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, because you believe that the biometrics will make it easier for public safety officials to target the bad actors. Along those same lines, privacy advocates are most concerned about false positives. And the good news is that improved technology – including biometrics – can help reduce the number of false positives. So, this all can be mashed 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 harping on 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 these fears, 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 is 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 the right people involved as well. We see this, for example, with border security technology, which often includes a strong data analytics component but lacks the ability to communicate threats to somebody who could actually do an interdiction. 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](http://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.