
UNISYS | Securing Your Tomorrow®
2020 Unisys Security Index™
Global Edition

CONTENTS

CHAPTER 01

EXECUTIVE SUMMARY

CHAPTER 02

THE UNISYS SECURITY INDEX: 14 YEARS AND COUNTING

CHAPTER 03

REGIONAL DIFFERENCES LARGER THAN EVER IN 2020

CHAPTER 04

CHANGES IN THE GLOBAL CONCERN

CHAPTER 05

IN A PANDEMIC WORLD, CONSUMERS HAVE TAKEN THEIR FOCUS OFF ONLINE RISKS

CHAPTER 06

DATA SHARING IS DEEMED MOST ACCEPTABLE IN AN EMERGENCY

CHAPTER 07

A CLOSER LOOK AT THE FOUR AREAS OF SECURITY CONCERN

CHAPTER 08

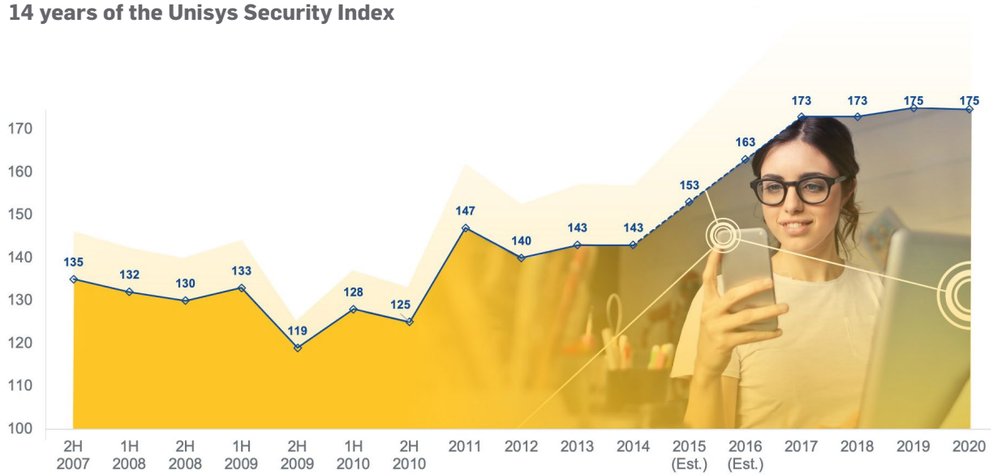
THE UNISYS PERSPECTIVE

CHAPTER ONE

EXECUTIVE SUMMARY

The Unisys Security Index™ has tracked global security concerns for 14 years. Overall, the world remains on edge – global security concerns are at their highest level since the first Unisys Security Index in 2007.

14 years of the Unisys Security Index



With a score of 175 out of 300, the 2020 Unisys Security Index remains at a historical high. Almost all (99%) respondents have at least one security concern out of the eight included in the survey. However, there are notable shifts in focus owing to the emergence of the COVID-19 global health crisis.

Internet Security is now the lowest concern among consumers, after having been steadily on the rise since 2017 and finishing as the area of second-most concern in both 2018 and 2019.

Meanwhile, both National Security and Personal Security have moved up the agenda, driven by a rise in concerns about Personal Safety, which has increased by 9 percentage points to 58% seriously concerned, and concern about Epidemics/Disasters, which not surprisingly has increased by 8 percentage points to 62% seriously concerned.

Consumer worries about all other security concerns fell since 2019.

Personal Safety

58%

seriously concerned

Natural Disasters/Epidemics

62%

seriously concerned

Consumers are narrowing their attention during COVID-19 to their families' health (67% seriously concerned), as well as to their country's economic stability (66%) and health infrastructure (64%). In contrast, Internet Security issues such as the risk of being scammed (45% seriously concerned) or experiencing a data breach while working remotely (41%) are the least concerning risks relating directly to the pandemic. This is despite both a rapid push to remote work for millions of people and mounting evidence that phishing, scamming and hacking are rising dramatically during the pandemic. In this sense, consumers appear to be taking their eye off the ball when it comes to security concerns beyond health and economic well-being, putting themselves and potentially their employers at risk.

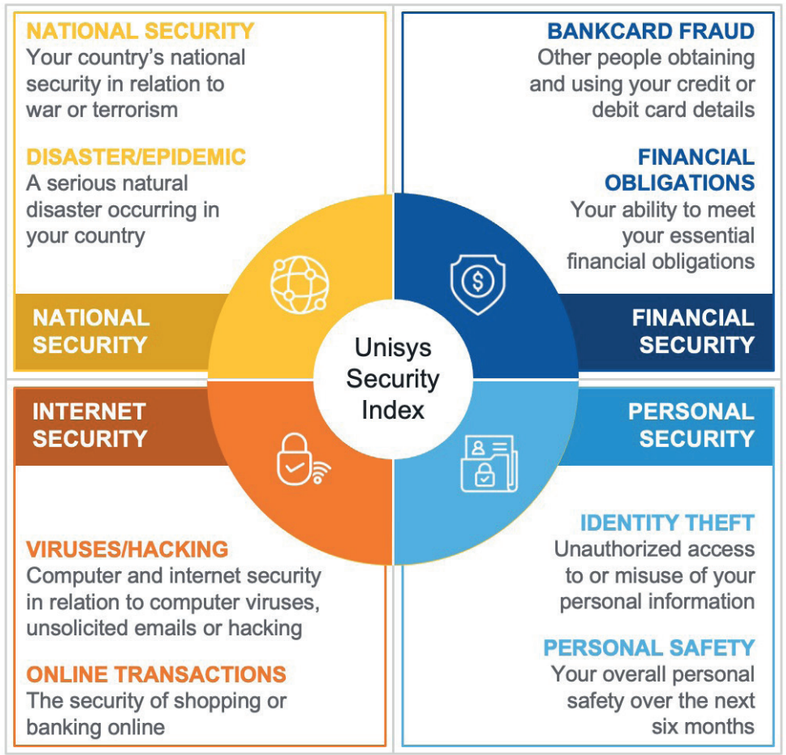
Consumers' change in focus – moving from Internet Security concerns toward those of Personal and National Security – is reflected in attitudes toward data sharing. More than three-fifths (61%) say they are willing to share their location data so the police can find them in an emergency. However, consumers are clear that data sharing is only acceptable if it is for the right reason and with a trusted organization.

For the fourth consecutive year, Identity Theft and Bankcard Fraud are the two most pressing concerns worldwide, despite dropping from 2019 levels. Concern around Identity Theft dropped by four percentage points since 2019 but continues to rank at the top of the eight security concerns measured by the index. Women and young people under 35 are the most concerned demographic groups globally. Six of the top seven countries most concerned about security are developing economies, with security concerns having increased the most in Brazil and Chile since last year.

Scamming and hacking are rising dramatically during the pandemic

CHAPTER TWO

THE UNISYS SECURITY INDEX: 14 YEARS AND COUNTING



Unisys Corporation (NYSE: UIS) plays a prominent role in global cybersecurity through the technology products and services it provides to governments and financial and commercial industries across the globe.

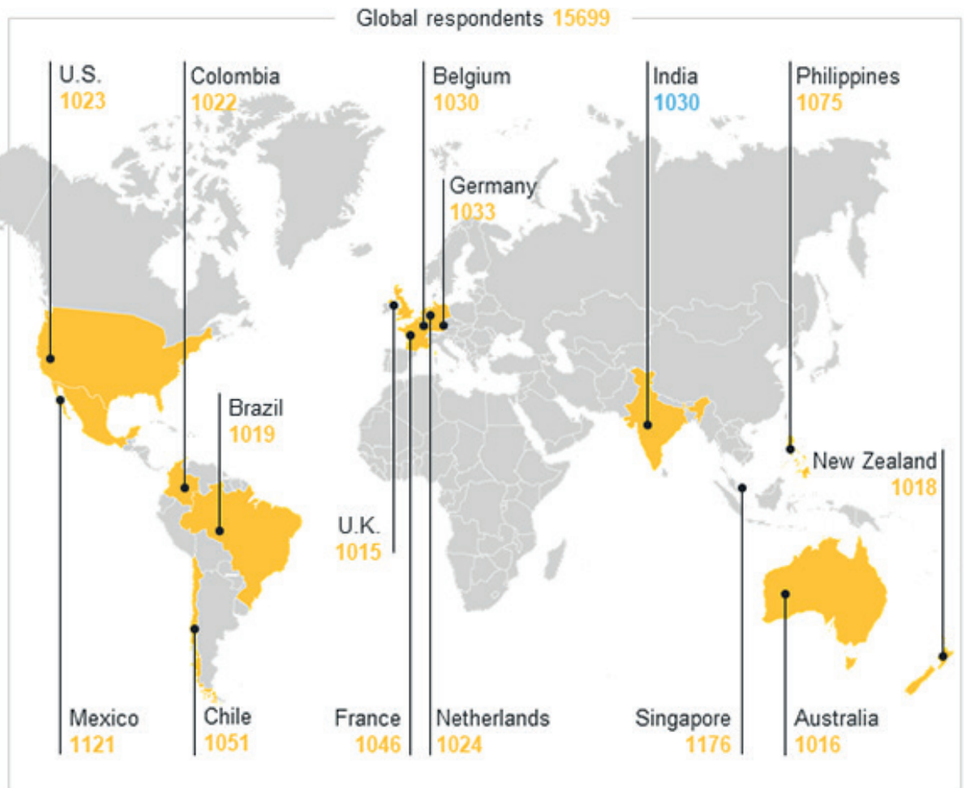
In 2007, the company launched the Unisys Security Index – the longest-running snapshot of consumer security concerns conducted globally – to provide an ongoing, statistically-robust measure of concern about security. The index is a calculated score out of 300[1] that measures consumer attitudes over time across eight areas of security in four categories.

The 2020 Unisys Security Index is based on national surveys of representative samples of 15,699 adult residents from 18-64 years of age. Interviews were conducted online in each of the 15 countries, which were extended in the 2020 survey to include France, India and Singapore. All national surveys were conducted March 16-April 5, 2020.

Importantly, this research was conducted during the onset and spread of the COVID-19 global health crisis. All countries had been affected by either quarantine or lockdown measures at a local or national scale.

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

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 15 countries' security indices. The margin of error is +/-3.1% per country at a 95% confidence level and 0.8% for the global results.

The 2020 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.

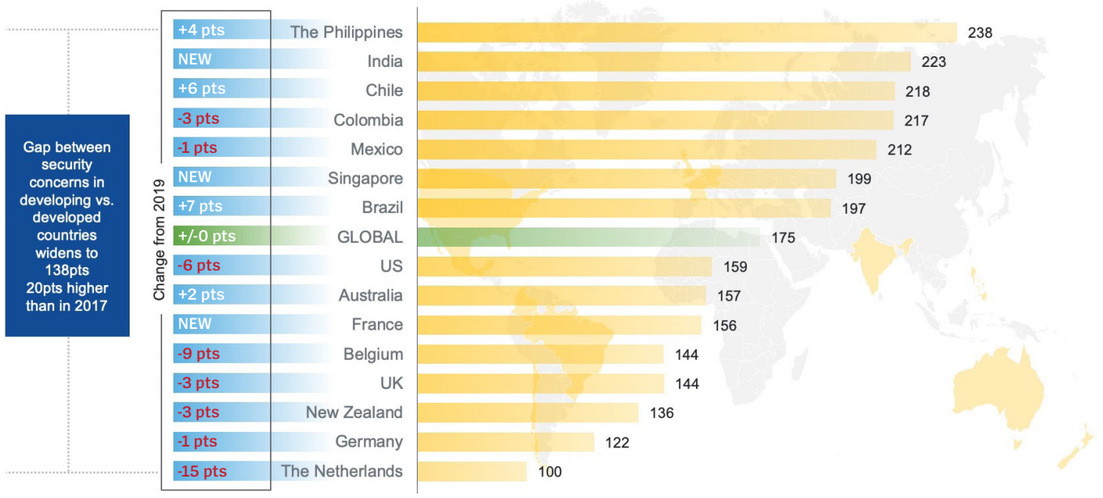
CHAPTER THREE

REGIONAL DIFFERENCES LARGER THAN EVER IN 2020

The 2020 Unisys Security Index score remains at a historical high of 175, the same score seen in 2019 – despite the global health crisis. Almost all consumers (99%) have at least one security concern out of the eight included in the survey.

While the overall ranking of countries' security concerns remains broadly consistent, the gap has widened among the countries feeling the most and least concern. Developing countries tend to be more concerned than developed countries[2], and this distinction has become more marked in 2020. The disparity between the most concerned country (the Philippines, at 238) and the least concerned country (the Netherlands, at 100) has grown by 20 points since 2017.

2020 Unisys Security Index by country



*Developing countries: the Philippines, India, Chile, Colombia, Mexico, Brazil

The biggest increases in concern are in Latin America, where Chile's index score increased by 6 points and Brazil's by 7 points. Financial Security concerns are particularly high in Latin America, with Chile having the highest score (alongside the Philippines) at 236, followed by Colombia (227) and Mexico (220). Financial Security concerns also jumped by 12 points in Brazil, to 203.

Asia Pacific countries also saw an increase over 2019's index. The Philippines maintains its position as the most concerned country, increasing its score by 4 points. India and Singapore, both new to the Unisys Security Index, enter in second and sixth place, respectively. As it relates to Internet Security, the Philippines and India are the most concerned among all the countries surveyed, with scores of 228 and 224, respectively. These countries are also the most concerned about Personal Security, with a score of 251 in the Philippines and 226 in India. Australia is the only developed country to have seen an increase in its score, which rose by 2 points – potentially linked to the country's experience of disastrous wildfires during 2019-20.

With a score of 159, the U.S. is the second-most concerned of the developed countries included in the survey. This is driven by Personal Security concerns, which have risen 4 points to 165 as a result of the pandemic.

In most countries, the top concern during a global health crisis is respondents' families' health (India, the Philippines, Singapore, Belgium, France, the Netherlands, Chile, Colombia and Mexico). However, consumers in Australia, New Zealand, Germany and the U.S. are most concerned about their country's economic stability; and the U.K. and Brazil are most concerned about their country's health infrastructure.

How concerned are you about the impact of global health crises, such as the outbreak of the COVID-19, Ebola and Zika viruses?
Top results for each country

My family's physical health
Top concern in 9 countries

- India
- The Philippines
- Singapore
- Belgium
- France
- The Netherlands
- Chile
- Colombia
- Mexico

My country's economic stability
Top concern in 4 countries

- Australia
- Germany
- New Zealand
- U.S.

The stability of my country's health infrastructure
Top concern in 2 countries

- U.K.
- Brazil

[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.

CHAPTER FOUR

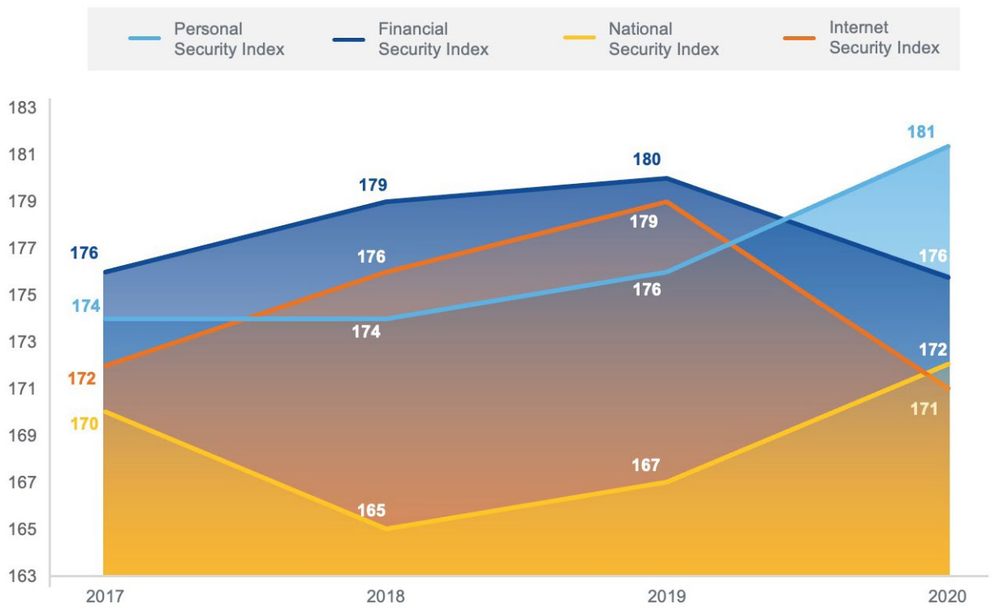
CHANGES IN THE GLOBAL CONCERN

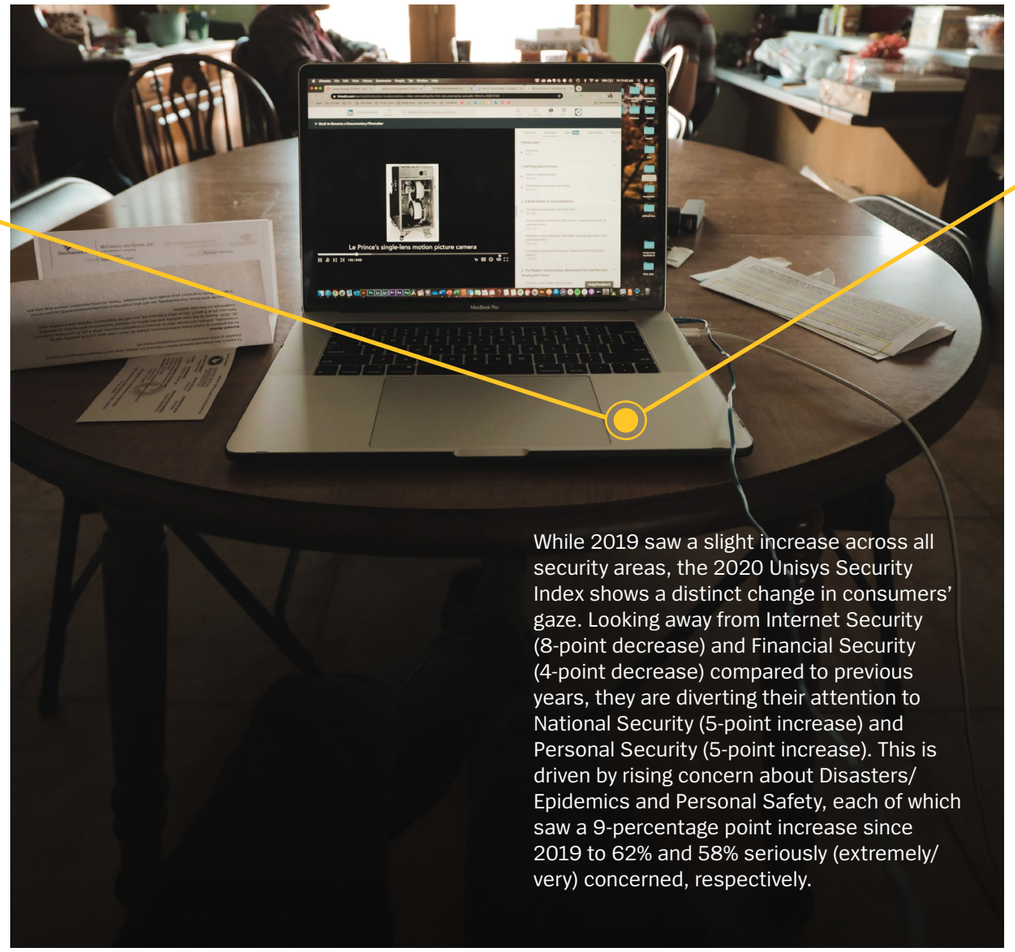
The data behind the 2020 Unisys Security Index was collected during the early stages of the COVID-19 pandemic. All countries were affected at this time, but to differing degrees of severity.

The threat of widespread illness naturally raises immediate concerns around health, safety and economic stability. Given that data collection occurred during what, for many countries, was the early weeks of the crisis, some of the longer-term or less immediately impactful threats – such as long-term employment prospects and the growing risks of internet hacking and computer viruses in a new 'shelter-in-place' world – may not have been front-of-mind.

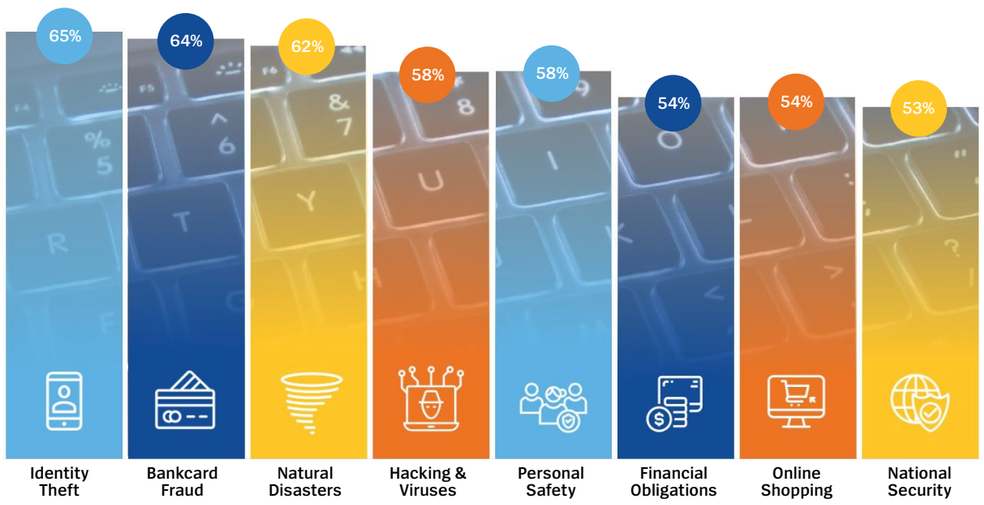
Overall, the 2020 Unisys Security Index score remains consistent with that of 2019. Although security concerns have not increased, they have shifted focus.

Unisys Security Index component trends





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



CHAPTER FIVE

IN A PANDEMIC WORLD, CONSUMERS HAVE TAKEN THEIR FOCUS OFF ONLINE RISKS

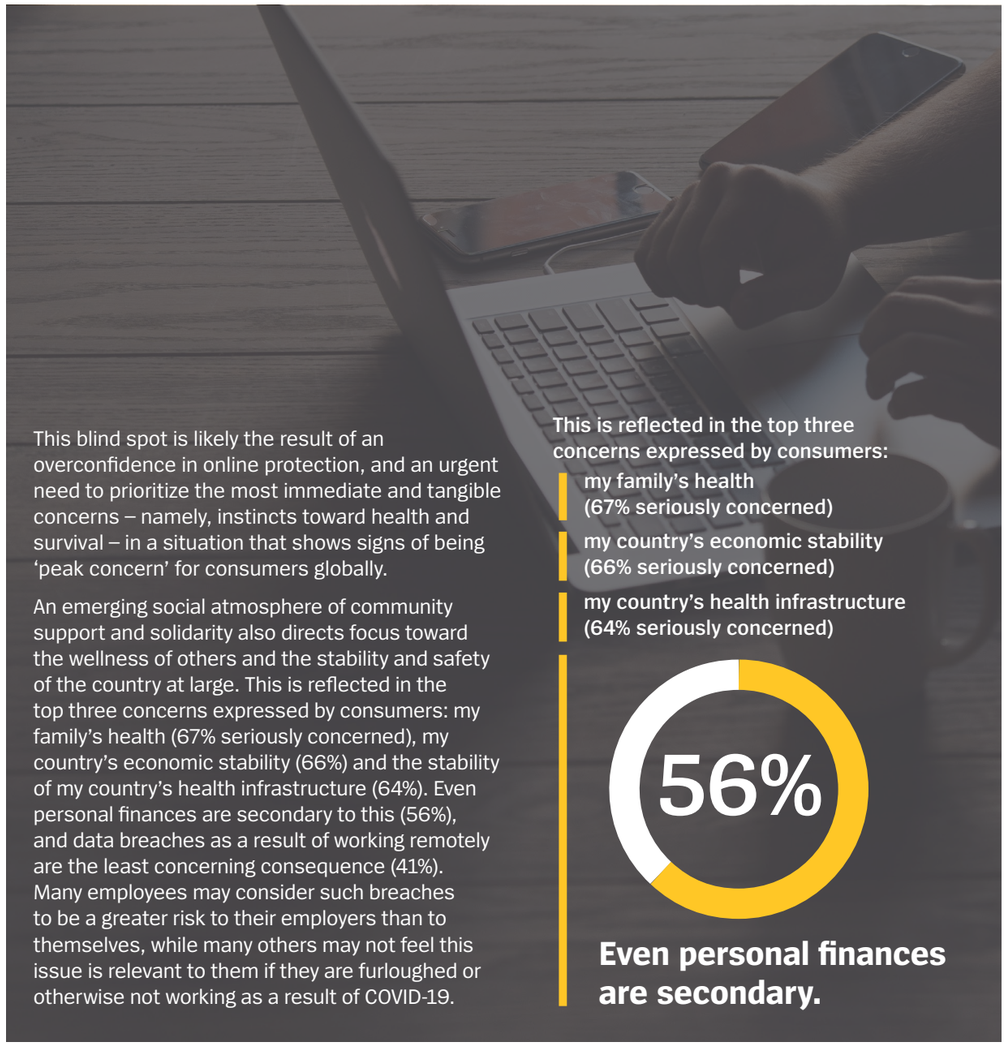
COVID-19 has created an influential backdrop to the 2020 Unisys Security Index. It is already clear that a pandemic on this scale will shape the world for many years to come. Even in the early weeks leading to mid-April 2020, it had changed daily life for millions of people in countries around the world.

Concern about Disasters/Epidemics has, unsurprisingly, jumped into the top three areas of concern, with 62% seriously concerned. And Personal Safety has seen the largest increase, rising 9 percentage points to 58% seriously concerned. Concern about all six other security risks has fallen, including those relating to Internet Security: Hacking & Viruses and Online Shopping. This reflects a false sense of security, given that the risks are now higher, in light of COVID-19, than ever before.

Reliance on the internet has increased dramatically, in a world that now depends on it for remote working and schooling and online socializing, shopping, banking and healthcare. And yet only 41% say they are seriously concerned about the risk of a data or security breach while working remotely, which was the lowest of all the concerns measured globally.

This is despite warnings from the World Health Organization (WHO)[2] and Interpol[3] of increased risk of cyberthreats during the pandemic: Estimates show there have been as many as 192,000 coronavirus-related cyberattacks per week in May 2020 alone, a 30% increase compared to April[4]. In late April 2020, Google's Gmail reported that it saw more than 18 million daily malware and phishing emails related to COVID-19 scams in just one week, and more than 240 million daily spam messages related to COVID-19.

What is more, only 45% of respondents say they are concerned about the risk of being scammed during or about a health crisis. This is worrying given that the vast majority of cyberattacks – 98%, by some estimates – deploy social engineering methods (such as phishing), with the WHO reporting a fivefold increase in attacks since the start of the pandemic.



This blind spot is likely the result of an overconfidence in online protection, and an urgent need to prioritize the most immediate and tangible concerns – namely, instincts toward health and survival – in a situation that shows signs of being 'peak concern' for consumers globally.

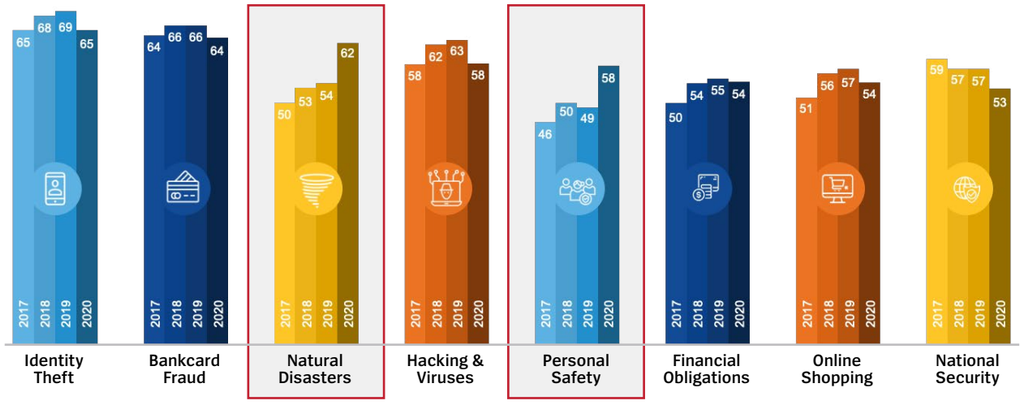
An emerging social atmosphere of community support and solidarity also directs focus toward the wellness of others and the stability and safety of the country at large. This is reflected in the top three concerns expressed by consumers: my family's health (67% seriously concerned), my country's economic stability (66%) and the stability of my country's health infrastructure (64%). Even personal finances are secondary to this (56%), and data breaches as a result of working remotely are the least concerning consequence (41%). Many employees may consider such breaches to be a greater risk to their employers than to themselves, while many others may not feel this issue is relevant to them if they are furloughed or otherwise not working as a result of COVID-19.

This is reflected in the top three concerns expressed by consumers:

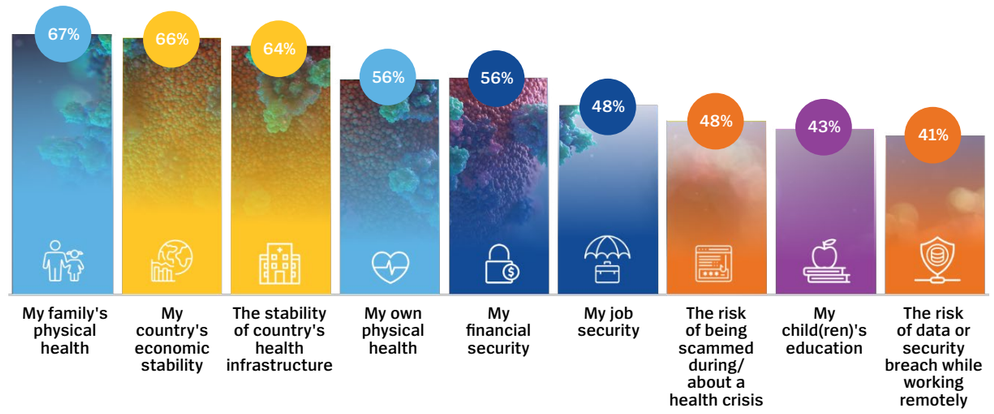
- my family's health (67% seriously concerned)
- my country's economic stability (66% seriously concerned)
- my country's health infrastructure (64% seriously concerned)

Even personal finances are secondary.

Tracking the eight concerns from 2017 to 2020
(showing top 2, extremely or very concerned)



How concerned are you about the impact of global health crises, such as the outbreak of the COVID-19, Ebola or Zika viruses?
Showing data for concerned (extremely or very)



[3] https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/
[4] https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
[5] https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/
[6] https://purplesec.us/resources/cyber-security-statistics/
[7] https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

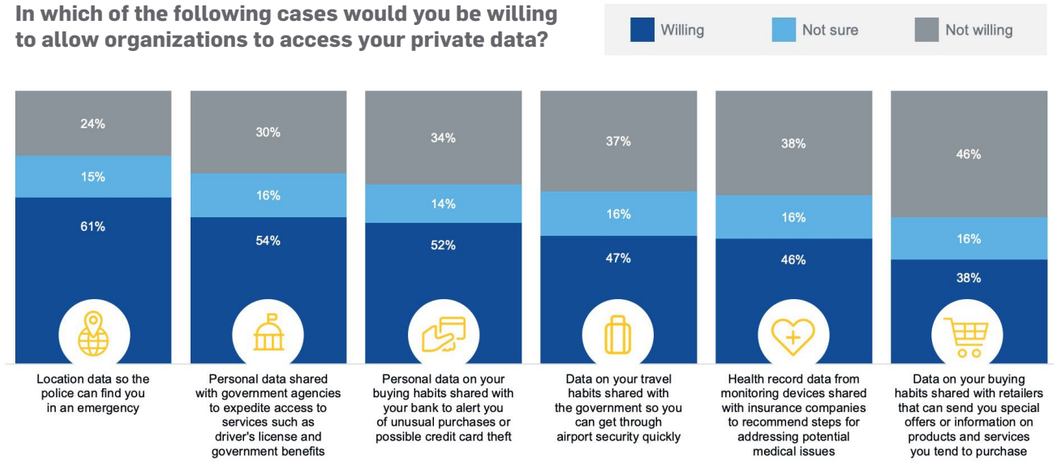
CHAPTER SIX

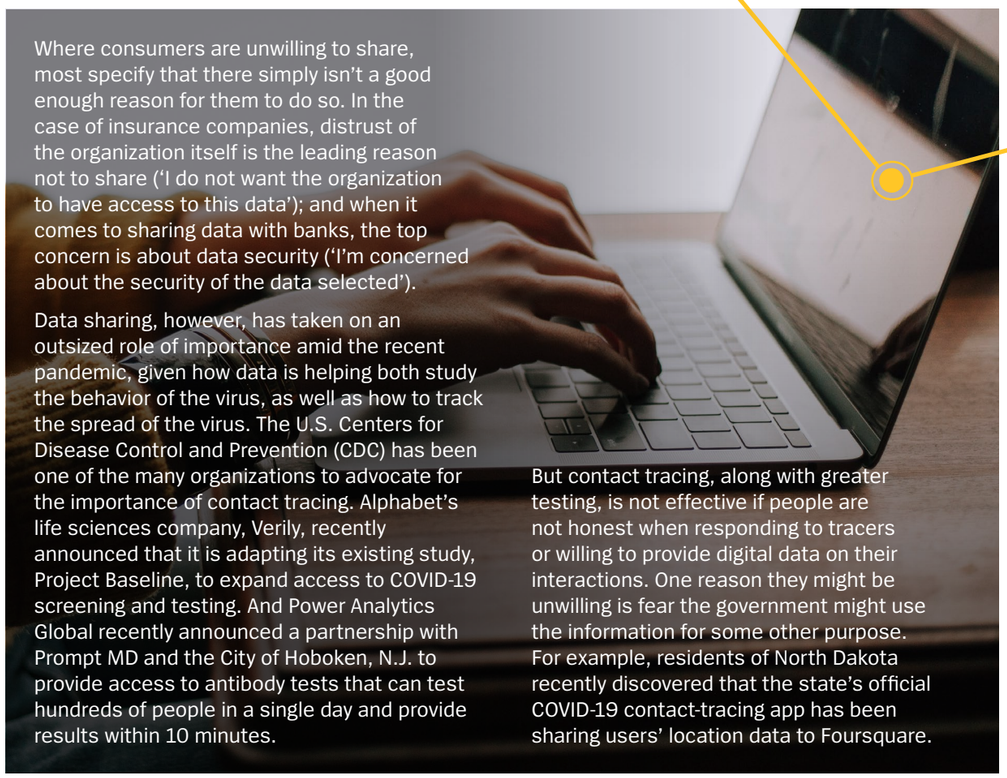
DATA SHARING IS DEEMED MOST ACCEPTABLE IN AN EMERGENCY

Although internet and data security issues have fallen out of focus for many consumers in the midst of a global health crisis, the idea of data sharing and privacy continues to ring alarm bells. The issue of privacy may even have been heightened following specific COVID-19-related tracking measures used in some Asian countries in early 2020 that showed signs of early success in bringing the crisis under control. Faced with the possibility of this type of surveillance being used in their own country, consumers globally are reminded of the trade-off between their own privacy, their own health and the health of their community.

When asked about their willingness to share data with organizations, consumers are clear that both the type of organization and the purpose of the data collection determine whether data sharing is acceptable. Public sector usage, such as the police or government agencies, is considered more acceptable than usage by private sector businesses. And the use of data for emergency assistance or security alerts is less concerning than its use for personalizing special offers, or even for the convenience of speeding up queues through airport security. People are most willing to share data if it is with the police and for the purpose of finding them in an emergency (61% willing); and they are least willing to share data if it is with retailers providing personalized buying suggestions or offers (38% willing).

In which of the following cases would you be willing to allow organizations to access your private data?





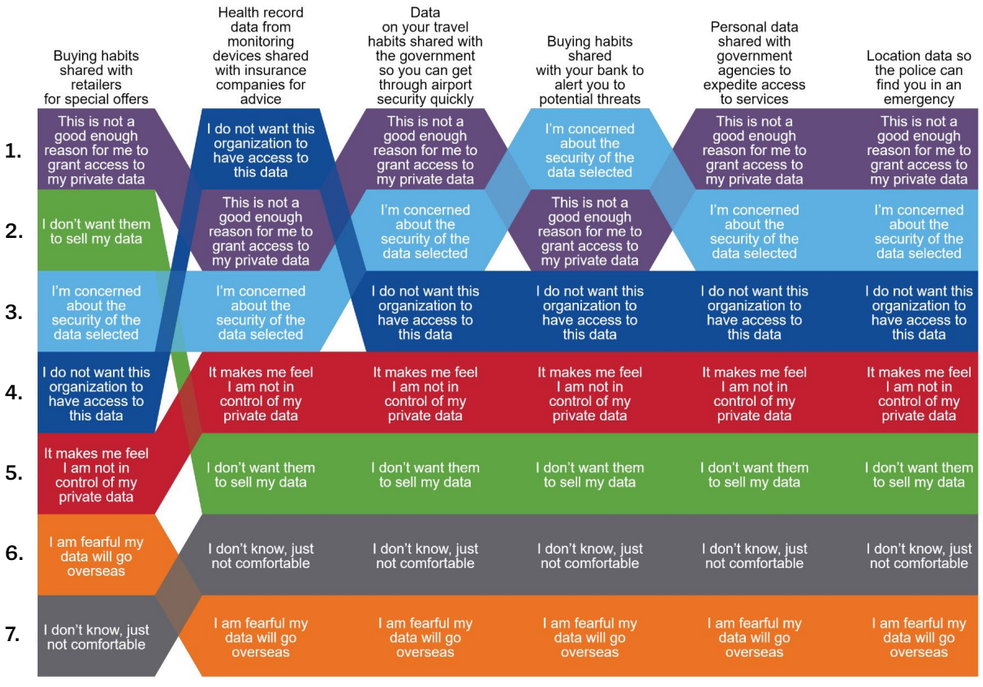
Where consumers are unwilling to share, most specify that there simply isn't a good enough reason for them to do so. In the case of insurance companies, distrust of the organization itself is the leading reason not to share ('I do not want the organization to have access to this data'); and when it comes to sharing data with banks, the top concern is about data security ('I'm concerned about the security of the data selected').

Data sharing, however, has taken on an outsized role of importance amid the recent pandemic, given how data is helping both study the behavior of the virus, as well as how to track the spread of the virus. The U.S. Centers for Disease Control and Prevention (CDC) has been one of the many organizations to advocate for the importance of contact tracing. Alphabet's life sciences company, Verily, recently announced that it is adapting its existing study, Project Baseline, to expand access to COVID-19 screening and testing. And Power Analytics Global recently announced a partnership with Prompt MD and the City of Hoboken, N.J. to provide access to antibody tests that can test hundreds of people in a single day and provide results within 10 minutes.

But contact tracing, along with greater testing, is not effective if people are not honest when responding to tracers or willing to provide digital data on their interactions. One reason they might be unwilling is fear the government might use the information for some other purpose. For example, residents of North Dakota recently discovered that the state's official COVID-19 contact-tracing app has been sharing users' location data to Foursquare.

The following chart shows the reasons why people are unwilling to share their information in different situations, ranked by importance.

Why aren't you willing to allow organizations access to your information?



CHAPTER SEVEN

A CLOSER LOOK AT THE FOUR AREAS OF SECURITY CONCERN

National Security (National Security and Disasters/Epidemics)

In the wake of COVID-19's arrival in most countries around the world, National Security concerns are, not surprisingly, on the rise. Increasing from 167 in 2019 to 172 in 2020, National Security concerns are one of the two security areas to have seen a jump since 2019.

This rise in concern is centered on Disasters/Epidemics, with 62% seriously concerned – an increase of 8 percentage points since 2019. Concerns about National Security specifically – such as terrorist attacks or war – dropped by 4 percentage points to 53%.

Even before COVID-19, people around the world have become increasingly aware of – and many directly affected by – natural disasters, particularly those related to extreme weather. Floods, storms, wildfires or extreme temperatures have affected people in every region included in the survey.

National security concern changes since 2019

↓
- Colombia
- U.S.
- Belgium
- The Netherlands

↑
- Mexico
- Chile
- Brazil
- U.K.
- Australia

The increase in National Security concern holds true for all countries except Belgium, the Netherlands, Colombia and the U.S. The fall in these countries' National Security index score is driven by a reduction in concern about war or terrorism. Concerns about natural disasters and epidemics increased in all cases.

The countries in which National Security concerns fell all experienced an overall reduction in security concerns. In Belgium, the U.S. and Colombia, the only security area to increase in concern was Personal Security – indicating that attention is shifting in these countries from issues of national concern to those of personal safety.

Personal Security (Identity Theft and Personal Safety)

Of the four security categories measured by the survey, Personal Security is now the area of greatest concern around the world – rising from 176 in 2019 to 181 in 2020. It replaces Financial Security as the leading concern globally, which had previously been front-of-mind for consumers since 2017.

Identity Theft remains the top concern of the eight security areas measured, with 65% seriously concerned. However, this is a reduction of 4 percentage points since 2019. The prominence of Personal Security concerns in 2020 is led by an increase in concern about Personal Safety: from 49% in 2019 to 58% in 2020. Against a backdrop of a global health crisis, this is unsurprising.

Personal security concern changes since 2019

↓
- Mexico
- The Netherlands

↑
- The Philippines
- Chile
- Australia
- U.K.
- New Zealand
- Germany

There are minor exceptions to this overall trend toward greater concern around Personal Security. Mexico's score in this area fell by just 1 point, and it remains in the top four most concerned countries when it comes to Personal Safety. The Netherlands fell by just 3 points, a small decrease in the context of overall security concerns in the country dropping by 15 points.

Internet Security (Computer Viruses/ Hacking and Online Transactions)

With attention being drawn to matters of national and personal security, security considerations in the digital world are falling by the wayside. Internet Security concerns are falling in all countries other than Brazil, with an 8-point drop to 171.

This is true even as the world becomes ever more dependent on the internet. Online solutions have become indispensable for countries undergoing lockdown measures to address COVID-19, causing internet usage to increase by up to 50% in some countries[7].

Internet security concern changes since 2019

↓ Mexico
U.S.
Australia
U.K.
Belgium
New Zealand
Germany
The Netherlands

↑ Brazil

The drop in concern is most notable in developed countries, with the Netherlands falling by 32 points, the U.K. by 22 points, Belgium by 19 points and New Zealand by 15 points.

In contrast, Brazil's score has risen 6 points, from 194 to 200. The country continues to be a hot spot for a broad variety of cyberattacks, from phishing and distributed denial of service (DDoS) campaigns to ransomware. The government recorded 19,150 incidents in 2019[8], 3,875 more than in 2018. The implications of COVID-19 for internet security were already being felt in Brazil when the Unisys Security Index data was collected: there had been a 124% rise[9] in cybersecurity attacks during February and March.

COVID-19 has caused internet usage to increase by up to 50%

Financial Security (Bankcard Fraud and Financial Obligations)

Despite Bankcard Fraud remaining a top concern (second only to Identity Theft), Financial Security concerns are, overall, falling. Global scores in this area fell to 176 in 2020 from 180 in 2019.

Both areas of Financial Security concern saw only a minor reduction since 2019. Concerns about Bankcard Fraud fell 2 percentage points to 64% seriously concerned, and concerns about Financial Obligations fell just 1 percentage point to 54%. These issues therefore remain a central consideration for consumers around the world but have fallen in relative prominence due to unprecedented health and safety concerns relating to the pandemic.

Brazil, Chile and the Philippines are exceptions to this, with notable increases in Financial Security concerns. Local political contexts may explain why they are moving against the trend

Financial security concern changes since 2019

↓ U.S.
Belgium
New Zealand
U.K.
The Netherlands

↑ Brazil
Chile
The Philippines

Brazil saw the biggest increase in Financial Security concerns, from 191 in 2019 to 203 in 2020. The country's economic recovery has been slow. Its economic performance[10] over the last decade has fallen behind its peers in the BRICS group (Brazil, Russia, India, China and South Africa), who are associated on the basis of their emerging national economies and significant influence on regional affairs.

Chile has also seen a rise of 7 points to 236, making it one of two countries with the highest Financial Security concerns. Civil protests in the country relating to the increased cost of living and rising inequality suggest that these issues are front of mind for Chilean consumers.

In the Philippines, slow economic growth creates the backdrop for an increase of 6 points. The Philippines now equals Chile in having the highest Financial Security concerns at 236.

[8] https://www.weforum.org/agenda/2020/03/will-coronavirus-break-the-internet/
[9] https://www.bnamericas.com/en/features/why-is-brazil-so-vulnerable-to-cyber-attacks
[10] https://www.zdnet.com/article/coronavirus-related-cyberattacks-surge-in-brazil/
[11] https://www.bbc.co.uk/news/business-48386415

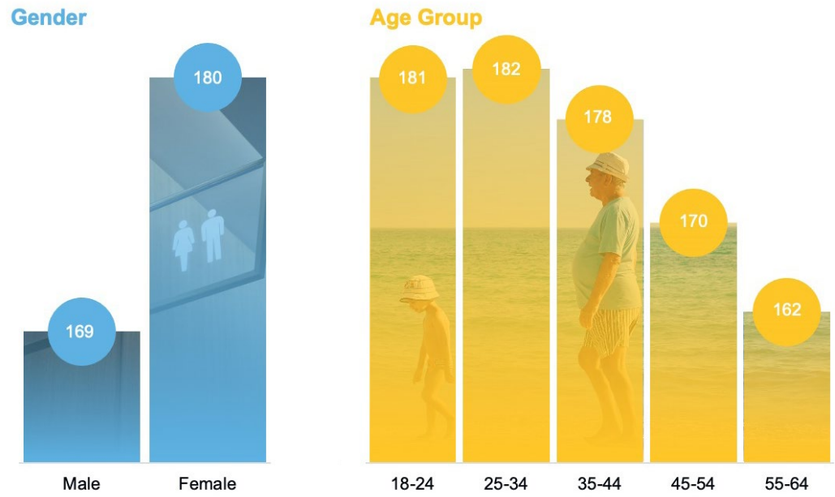
DEMOGRAPHICS

Women are more concerned than men, scoring 180 compared to 169 for men, driven by higher concerns surrounding natural disasters (59% men vs. 66% women) and overall personal safety (54% men vs. 61% women) among women. There is more concern among younger people aged 18-34, with an average score of 182 as compared to 162 for those aged 55-64, with younger people more concerned across every area. Within the context of COVID-19, younger generations tend to focus concern on their family's health, while older generations are more concerned about their country's economy. People on low incomes and those running small businesses are also more concerned, with scores of 182 and 190, respectively, which is not surprising considering the impact that government-imposed shutdowns have had on those groups.

Seriously concerned about natural disasters

Women are more concerned than men, scoring 180 as compared to 169 for men, driven by higher concerns surrounding natural disasters

Unisys Security Index by demographic groups



When it comes to the specific risks posed by the emerging pandemic, lower-income households are more concerned about job security (52% as compared to the global average of 45%) and financial security (62% as compared to the global average of 52%).

The self-employed are highly concerned about both financial security (68%) and physical health (65%). They are also the most concerned about a data or security breach, with 48% of small-business owners and 51% of freelancers concerned as compared to 41% on average.

CHAPTER EIGHT

THE UNISYS PERSPECTIVE

CONSUMER CONCERNS DURING A GLOBAL HEALTH CRISIS

This year's survey was conducted during the outbreak of a pandemic, during which consumers faced heightened concern for the health and safety of loved ones as well as dealing with the possibility of losing employment and the impact of the pandemic on the economy. Given this dynamic, it is no surprise to see consumer concerns rising in terms of national and personal security. However, with more people than ever working and shopping from home – and sharing their financial details with online retailers around the world – it is both surprising and worrying to see that consumer concerns about financial and internet security are decreasing.

When immediate risks are top of mind, consumers may turn a blind eye to longer-term financial and internet risks like identity theft, phishing scams, bankcard fraud and the security of online shopping. However, Unisys Chief Trust Officer Tom Patterson pointed out that *"workers from home need to understand that they are now part of this new expanded attack surface for the critical infrastructure of their entire country."*

Chris Kloes, vice president of Unisys Security Solutions, noted that *"government agencies, security experts and employers need to provide more than just warnings and information. There needs to be actionable recommendations communicated and services signposted to allow individuals to protect themselves, their organizations and their loved ones as much as possible from both physical and digital threats."*

According to Unisys Chief Information Security Officer, Mathew Newfield, there is both a level of apathy and a lack of awareness when it comes to securing the home office environment. *"In my conversations with CISOs, they're saying that when they're testing their own employees at home now, they're seeing double the failure rates on their security tests than they saw pre-COVID."*

"This points to the fact that we've dealt with so many people who bring their computers home from work, but their home networks are already infected. They've already had a breach of their home network. They have never updated their router. They've never rebooted, they've never patched and now they're unknowingly putting their company's data at risk," added Newfield.

A CHECKLIST FOR DIGITAL SAFETY IN YOUR HOME

Newfield shared his tips for consumers to stay safe in the new environment, whether working from home or just sharing and interacting more online.

- **Read** your company's IT security policies and procedures.
- **Update** your passwords on hardware such as cable boxes and internet modems. Even if you've done this before, an update will increase your safety.
- **Ignore** strange calls or emails asking for information.
- **Verify** all hyperlinks. If you have doubts, look at the domain in the URL and use online search engines to verify it independently.
- **Secure** your hardware by updating to the latest firmware and checking the brand and model for security risks. If you're using personal hardware or downloading software for work, get approval from your IT department.
- **Protect** your video calls. Always use new links and make sure meetings are password-protected.

CYBER CRIMINALS ARE READY TO EXPLOIT CONSUMER VULNERABILITIES

While it is understandable that consumers focus on more immediate personal risks in times of crisis, this is also the type of opportunity for which criminals and hackers wait. Ashwin Pal, Unisys cybersecurity director for Asia Pacific, commented that it is no surprise that financial security and internet security concerns decreased this year: *"It's a consequence of people being so focused on health and personal safety. It's distracted them from internet and financial security, which is why they've weighted those concerns lower. And frankly, that's one of the things that scammers count on when launching phishing attacks. They hope they can fly into the right app because people are too worried about their health."*

This is why consumers, workers and employers need to be prepared, by putting in place digital security precautions so they can limit the impact of cybercrime.

Alexis Aguirre, Unisys director of cybersecurity for Latin America, said, *"We live in uncertain times. More than ever, digital platforms are essential for doing business and for connecting with the world. But you have to be careful because information security has never been so threatened. Developing good habits concerning suspicious emails and links should be like buckling your seat belt – necessary but habitual."*

IDENTITY THEFT CONTINUES TO BE VIEWED AS A HUGE THREAT

For the past four years, identity theft has remained the top concern among consumers, despite concern declining since 2019. One reason for this is the high-threat recognition and clear potential impact that identity theft has among consumers.

As Pal explained, *"This is a reflection of what people think is going to impact them most. For example, if I get a phishing email or if I have a remote access breach, a lot of people don't understand what that means. However, if you ask, 'What is identity theft and what's the impact of that on you and how long will it take you to clear your name?', people can tell you: 'Two years, and these are the impacts.' That's what the reflection is – people's perception of the impact of the event. And that's not just identity theft versus things like remote access security; it's also around the health of the family and the health of the economy. It's the probability impact assessment."*

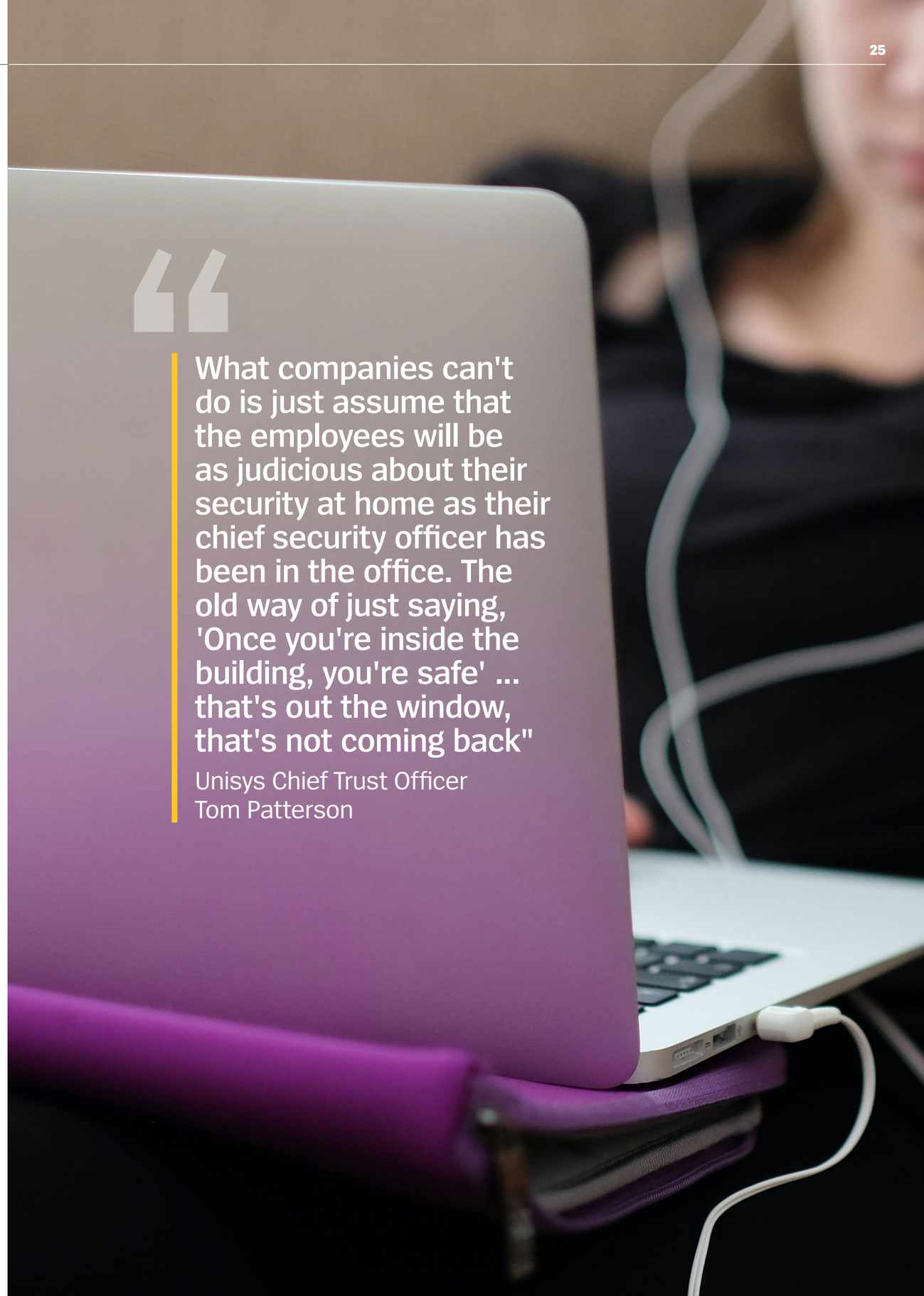
CONSUMERS ARE PREPARED TO SHARE PERSONAL DATA IN EMERGENCIES BUT WON'T THAT BE TOO LATE?

For consumers, willingness to share personal information fundamentally hinges on who they are sharing their information with, and how they expect that information to be used. For example, consumers in New Zealand and Australia are much less likely to share their personal data with financial services organizations. There's simply a lot less trust around financial institutions. There is similar mistrust in sharing healthcare data with insurance companies. As David Chadwick, Unisys director for identity and biometrics, Asia Pacific, said, *"If you're talking about sharing your health information, it's a matter of who you're sharing it with. As soon as people see insurance companies, they say, 'Hang on. They're going to see that I'm overweight and now I'm going to get charged more.' So it's not a matter of sharing your health record data, which is very important data, but rather the fact that you're sharing it with the insurance company."*

However, a large majority (61%) of consumers are willing to share location data to enable the police to locate them in an emergency. *"Consumers want to have their cake and eat it, too,"* Newfield explained. *"What they're saying is, 'I'm going to hold all my healthcare data on a necklace, nobody can have it until I get into an accident and then there's my data. You can use it.' But what if you can't make that decision? What if it happens 30 seconds too late that you try to make that decision?"*

Conclusion

Consumers are paying less attention to internet security, which leads to higher risks for individuals, organizations and employers around the world. Businesses and governments cannot afford to take a back seat when it comes to their employees' and citizens' online safety.



Calls to Action

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

1 Adapt your security for the work-from-home (WFH) era

Companies must make it easier for their employees to be secure when connecting from home, and that means less use of old style VPNs that don't scale and aren't suited for COVID-era WFH security, and more use of Zero Trust processes and technology, including always-on encrypted direct access, identity verification tools and a software-defined perimeter to limit the damage from malware getting in. This model supports the efficiency enabled by containers, cloud and Kubernetes; understands the external and internal threats we all face today; and enables the secure scalability that today's operations demand.

"There has been a massive shift in the workforce in recent weeks as people around the world are being asked to work from home, which can pose challenges to global operations and create unintended security risks," said Vishal Gupta, chief technology officer and senior vice president of Products and Platforms, Unisys. *"Employees today need secure remote access to vital data and applications to perform their work. In a business environment where software-defined perimeters are a reality and enabling remote work is necessary, Unisys believes it is critical to move to the Zero Trust security model made possible by a software-defined perimeter that leverages microsegmentation. Our Unisys Always-On Access™, powered by Stealth™ software makes that possible by dramatically reducing the traditional VPN attack surface and is scalable and easy to deploy and use to support secure access for users at organizations of any size."*

2 Don't lose sight of the human side of both your employees' experience and security

Often overlooked amid the massive shuffle of rapid-scale remote work enablement is the personal toll taken on employees operating today. Now, more than ever, it is important to stay connected to one's employees, both as a way to prioritize their well-being and to make sure they understand the new rules that come with a WFH environment.

"I think establishing regular check-ins, including informal events like a virtual lunch or virtual happy hour is the most important thing all leaders can do for the people they work with, the people they work for and the people that work for them," said Gupta. *"Leaders need to set aside time every day to make phone calls, to make video calls to the people they work with just to check in on them and motivate them. As part of that, from a business perspective, it's also an opportunity to communicate with employees on what platforms are acceptable for business conduct as compared to personal conduct."*

3 Utilize emerging technologies, including biometrics, to extend safety precautions in the age of work from home

It is not just on employees to implement safe practices. It is also on employers to recognize the new risks posed by a remote workforce and to implement appropriate protections. With most people working away from the office, unauthorized access to one employee's laptop could mean access to the whole company.

Firms can equip their employees with additional security controls such as multi-factor authentication — a code from an external device in addition to usernames and passwords — or even biometric logins such as fingerprint scans, which people already use to secure their smartphones.

"In this heightened age of security risks, now more than ever we see the need for more than just the traditional password as the sole method of authentication," said Salvatore Sinno, chief security architect and director of cybersecurity innovation at Unisys. *"Mobile device usage has brought biometrics to the mainstream as more people access their phones via a fingerprint. In today's environment, it makes sense for organizations to have a multi-layered approach to security to achieve continuous identity assurance, both to protect their workers and themselves, and also to address compliance with legislation such as GDPR."*

4 Look beyond "winning" with security and focus on resilience and trust

While most organizations have prioritized cybersecurity and operational resilience, the rapid spread of the COVID-19 pandemic has immediately added a sense of urgency to their importance. As the level of sophistication of cyber threats continues to evolve, an organization is inevitably going to have to come face-to-face with an attack on its network. A proper focus on trust and resilience could be the difference between whether an organization recovers or not.

"If a company aims to build walls around its network and thinks that alone will protect it, it will almost certainly fail," said Kloes. *"At Unisys, we tell companies to focus on the need to take out the catastrophe potential. Through software-defined perimeters, you can create isolated environments, easily overlaid on existing infrastructure. But, with that protection in place, if somebody does get in, they're only going to be able to do a limited amount of damage, because they won't be able to gain access to other pieces of the network. When we talk about resilience, it's about being prepared to take a hit so you are back on your feet quickly, instead of being down for the count."*

5 Be forward-facing – prioritize and implement the adoption of next-generation cyber tools

It has been said that disruption often begets innovation. And one potential benefit to the pandemic is the opportunity it presents to organizations to expand their usage of advanced security automation capabilities, including utilizing artificial intelligence and machine learning to improve their cyber posture. However, proper implementation is more complicated than snapping one's fingers.

"A lot of people think AI is going to be this magical thing," said Newfield. *"People quickly learn that when you deploy these technologies, it's like having a child -- it takes a very long time to get it to a mature state and it's very expensive. However, with the right training, implementation and technical support, AI and machine learning capabilities can be key to identifying discrepancies and to see if there's a problem, such as scanning for irregular behaviors or for malicious users who access documents or parts of the network unrelated to their job."*

About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most demanding businesses and governments. 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; computer viruses/ hacking and online transactions, in the Internet Security category; and identity theft and personal safety, in the Personal Security category. The 2020 Unisys Security Index is based on online surveys conducted March 16-April 5, 2020, during the COVID-19 pandemic. Surveys were conducted with nationally representative samples of at least 1,000 adults in each of the following countries: Australia, Belgium, Brazil, Chile, Colombia, France, Germany, India, Mexico, the Netherlands, New Zealand, the Philippines, Singapore, the U.K. and the U.S. The margin of error at a country level is +/- 3.1% at a 95% confidence level and +/-0.8% at a global level.

For more information on the 2020 Unisys Security Index, visit www.unisyssecurityindex.com.

#SecurityIndex

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

UNISYS | Securing Your Tomorrow®