UNISYS | Securing Your Tomorrow®

Security and the public sector

By Shawn Kingsberry

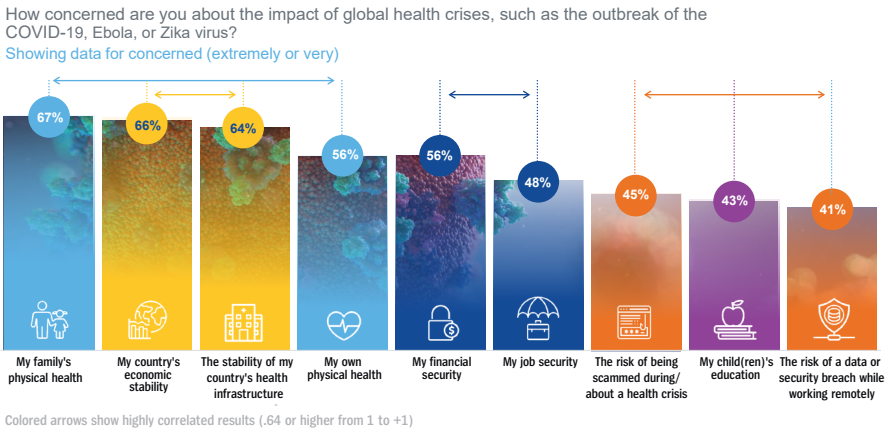
Citizens could not have found a worse time to relax their vigilance over online security.

COVID-19 Worries Pose New Challenges

"It is a development sure to cause consternation among public sector security officials already concerned about ransomware attacks and other threats to their cybersecurity. According to the just-released 2020 Unisys Security Index™, just when agencies were compelled by the COVID-19 virus to send their workers home with little preparation and on devices and networks of uncertain security, respondents were relaxing their concern about internet security."

The Unisys Security Index, the longest-running snapshot of consumer security concerns conducted globally was conducted in March and April in the early months of the pandemic, so it is not surprising that citizens reported increased concern about their personal safety. But they could not have found a worse time to relax their vigilance over online security.

> *Looking specifically at global concerns during the pandemic, 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.*



The 2020 Unisys Security Index surveyed more than 15,000 consumers in 15 countries, gauging attitudes on a range of security-related issues within the categories of national, financial, internet and personal security.

On a scale of zero to 300, with 300 representing the highest level of concern, the global index is now at 175, considered a serious level of concern and tied for the highest level in the 14 years the study has been conducted.

For the public sector in particular, it is a fraught time. In Australia, according to the OAIC notifiable Data Breaches report, health service providers reported the most data breaches, and the education sector is ranked third. Concerns about cyber security in healthcare have further increased during COVID-19 with concerns that everyone from vaccine researchers to hospitals and universities are vulnerable to cyber attacks.

Now, government officials are compelled by the COVID-19 pandemic to send their workers home to work, with all the new risks that entailed. Risks including a vastly expanded attack surface; a network bristling with more endpoints/entry points than ever envisioned by security officials; and a fresh set of attack vectors to exploit workers' heightened worries about health and finances. And unlike many private organisation, many in the public sector were unaccustomed to remote working.

The Unisys Security Index findings hold significant implications for public sector security leaders.

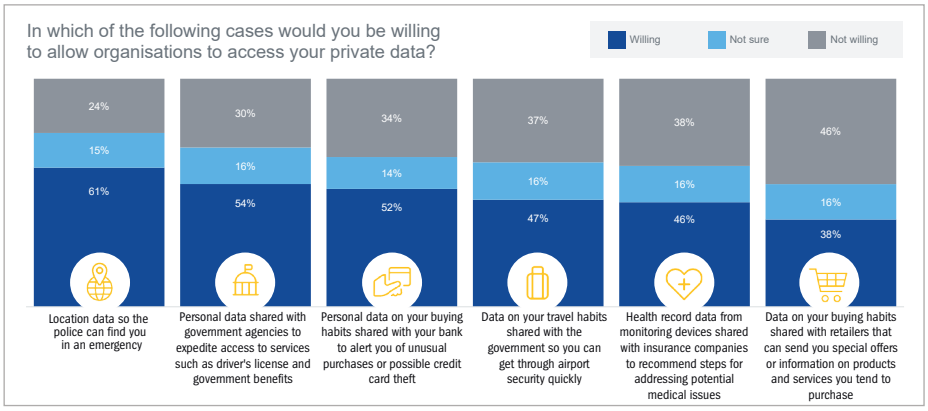
Responses to the pandemic revealed shortcomings of state agency systems and IT capabilities.

1. Make Cybersecurity a Priority – a Core Aspect of the Agency's Mission.

Cybercriminals find the public sector a prime target because of its rich repository of state secrets, citizen private data, and law enforcement information – making it amongst top-five most attacked sectors and underscoring the urgent need to secure data and transition to secure remote delivery.

Citizens need to know if they can trust their governments with their personal data. That trust is easily violated by news that an agency has been breached and their information has fallen into the hands of criminals. The Unisys Security Index was clear on this point:

> *When asked about their willingness to share data with organisations, consumers are clear that both the type of organisation 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.*



Especially because of the COVID-19 pandemic, now that agencies are seeking to collect increasing amounts of personal data to assist with contact tracing, they have the opportunity to demonstrate their commitment and competence in securing this information. Agencies can address these concerns through data protection solutions that leverage technologies such as microsegmentation, encryption and dynamic isolation to limit the access to this data by those who are unauthorised to see it. Public sector agencies must also demonstrate greater competence in protecting citizens against fraud. COVID-19-related fraud has cost citizens millions of dollars of frauds related to scams perpetrated by those who prey on individuals' inattention and/or trust.

Responses to the COVID-19 pandemic revealed major shortcomings of state agency systems and IT capabilities. The CIO of one large state termed his state's identity and access management "woefully inadequate." State web sites crashed.

Secure continuity of operations is now a core aspect of every agency's mission.

The *Washington Post* reported, "A flood of cash-starved applicants overwhelmed states' creaky computer systems and jammed their phone lines. Years of neglect — and technology in some cases that was nearly half a century old — resulted in some Americans waiting months just to collect their first unemployment payments," all while some states were paying out tens and even hundreds of million dollars in fraudulent payments, believed to be perpetrated by an international crime ring.

To restore trust after such high-profile debacles and waste, government should invest in legacy modernisation, digital transformation, and widespread automation, including technologies that deliver real-time analytics for faster and better decisions.

Part of prioritising cybersecurity must inevitably involve a great measure of standardisation. The extensive compartmentalisation of governments, especially at the state level, results in different systems and policies, which make the overall organisation vulnerable – a fact well-recognsed by would-be intruders.

Between the pandemic and the shift in worker attitude, each agency has new security obligations and opportunities, with secure continuity of operations a core aspect of the mission.

2. Prepare as Though Cybersecurity Attacks, Pandemics, and Teleworking Are a Fact of the Future.

Across the broad range of national and state or local agencies, responses to the pandemic were uneven. Some agencies were well prepared with documented policies for working at home including details about device security, data security, and more – and they had practiced putting the procedures in place. They were able to continue operating fairly smoothly with well practiced business continuity plans that enabled them to continue with business and protect their staff.

Others were obliged to scramble to improvise remote work policies paying scant attention to security. The compartmentalisation of many agencies contributed to the confusion. Certain agencies were especially vulnerable, unable to afford the best security technologies, talent and resources and instead depending on developing strategies on the fly, with the resultant impact on business, clients and staff.

Public sector security officials can use the experience of the pandemic to standardise their approach, prepare and practice for the next disaster, and employ the technology that protects devices, networks, data, employees, and the public. That includes:

- Security technology that cloaks endpoints so that hackers don't know they exist, instantly detects an intrusion, and within seconds isolates it via microsegmentation.
- Virtual desktop infrastructure that transfers everything on a worker's desktop, places it securely on the cloud, and allow them to connect to it from their home computer.
- Merged reality that enables an expert at one location to provide real-time, virtual hands-on assistance to a user at another site – especially valuable in a time of social distancing.
- Intelligent automation that could, for example, enable remote employees suddenly working from home to be automatically re-onboarded and reprovisioned with the tools they need to work from home and could also entail artificial intelligence that automatically offers those employees training on unfamiliar processes.

Personal safety has seen the largest increase, rising 9% points to 58% seriously concerned.

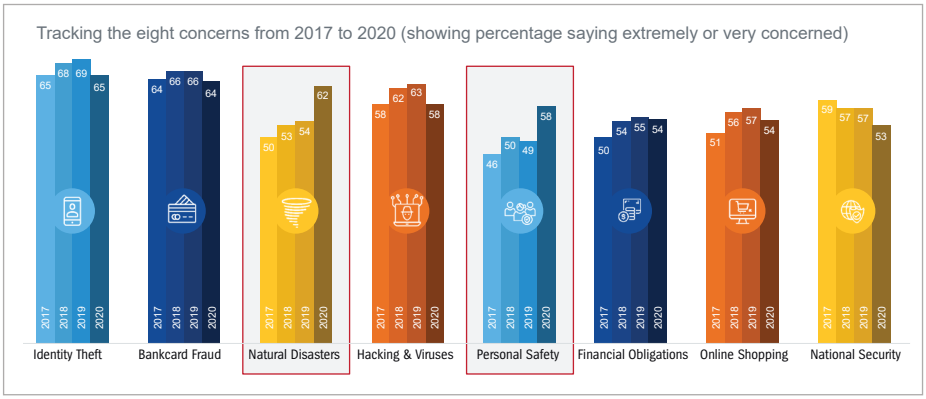
Shawn Kingsberry serves as the Vice President and Director, Global Government Solutions. He works to guide public sector consumers as they adopt cloud computing, data analytics and other digital government platforms. He has a diverse background in government and corporate settings, with extensive experience in large-scale information technology transformation, big data analytics, and enterprise computing, and secure hybrid cloud implementations.

He can be reached at shawn.kingsberry@unisys.com or connect with him at LinkedIn.

3. Adopt Innovation to Address Citizens' Heightened Concern About Personal Safety.

The results of the 2020 Unisys Security Index made it clear that when people are worried about their personal safety, they may well become lax about other security matters.

> *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% 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.*



Subsequent events involving law enforcement, protests, and dangerous episodes of unrest have only certainly fueled those concerns. Ensuring personal safety is one of the most solemn obligations of government, and innovative technology can play a pivotal role.

With that in mind, cities can embrace the concept of "Smart Cities" and use technology, interconnectivity, and the Internet of Things to improve their citizens' lives. Smart Cities become Safe Cities when they use technology as a means of investigating and preventing crime, interacting with citizens, and ensuring their personal safety. Police and other public safety and service agencies can embrace technologies that enable more communication methods and means with the public. Doing so will ultimately drive down criminal activity and improve crime clearance rates as public safety officials receive critical and time-sensitive information via digital means.

The pandemic may have lasting effect on citizens' perception of their safety relative to health, perhaps permanently altering the traditional office buildings that are a core feature of any city and use of city-center real estate and buildings.

It is not an exaggeration to say that the health and wealth of people are inextricably entwined with their sense of security. How cities rise to the current challenges will spell the difference between prospering and declining.

Thanks to rapid technology innovation, compounded by growing recognition that Safer is Smarter, the concept of Smart Cities is moving closer to reality, offering citizens untold opportunities and convenience and a better, safer environment.

For more information, visit www.unisyssecurityindex.com.