UNISYS | Securing Your Tomorrow®

# Internet Security Concerns Dominate Survey

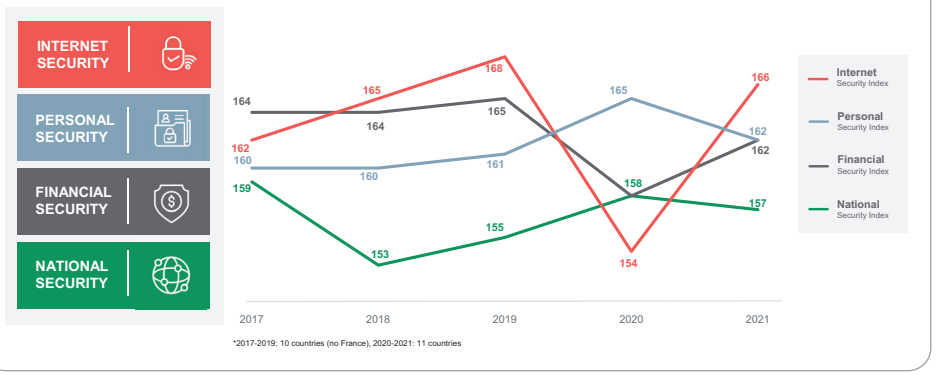
## By Janine Moore


*Reversing a multi-year trend, and driven by concerns about ransomware and remote working risks, concerns about internet security rose by 12 points, moving from last to first in our survey. Viruses, hacking, malware, phishing attacks and employee discomfort regarding monitoring of worker's remote activity were notable examples of cybersecurity concerns.*

The Unisys Security Index™, the longest-running snapshot of consumer security concerns conducted globally, was completed in the summer of 2021, as some workers started transitioning back from remote work to offices as the COVID-19 pandemic initially began to wane. While 2020 showed a sharp spike in concerns about personal security – health concerns being dominant – concerns about Internet breaches and ransomware increased dramatically in 2021. While this phenomenon applied to any industry in which workers could telecommute, the public sector was one of the only employers to largely remain open during the pandemic, and the first to re-open in the spring of 2021, as demand for public services remained unchanged.

**Internet Security Jumps Back to First Place as Pandemic Concerns Drop**

Unisys Security Index component trends




*2017-2019: 10 countries (no France), 2020-2021: 11 countries

The 2021 Unisys Security Index surveyed 11,000 consumers in 11 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 162, representing a slight increase from 159 in 2020 and tied for the highest score in the 15 years since Unisys began conducting the survey.

*Public-sector sites represent ripe targets for cyber criminals.*

## The Public Sector View

As with commercial entities, the threat of state-sponsored cyberattacks looms large; ransomware attacks are not limited to corporations with deep pockets, but, sadly, are often targeted at underfunded, not-for-profit entities such as hospitals, schools or local government sites. Cyber criminals are not deterred by the knowledge that their targets might be helping the public good or that lives could be jeopardized if systems are shut down – they only care about the likelihood of being paid.

Likewise, hacktivists – who seek to disrupt rather than monetize via their attacks – are just as likely to target government systems and sites as their commercial counterparts. In addition, public sector sites offer thieves tantalizing payoffs for data exfiltration: massive amounts of private citizen data; law enforcement details; sensitive or classified information, and financial records such as tax information are just a few examples of targets. Using Advanced Persistent Threats (ATPs), thieves can mine servers for months before being detected and blocked.

## People are Affected

While massive federal breaches, such as the 2020 SolarWinds attack that penetrated multiple U.S. government agencies, are well-documented and are covered as front-page news, breaches of state and local systems can have a disastrous impact on citizens, one that might not seem obvious at first. For example, consider something that might at first seem like a low-impact breach: Benefits for the poor. This isn't the kind of example that will be covered by 60 Minutes or have books written about it, but the sad fact is that many of the underprivileged are deeply dependent on the timely distribution of benefits, and should those be interrupted, they can have a cascading effect.

Specifically, the underprivileged do not have reserve funds, often work multiple jobs, and cannot take personal leave for unscheduled visits to government offices; they do not have personal vehicles, relying instead on public transportation.

More critically, they are faced with desperate decisions regarding their children when the assistance system breaks down: Ff they do not have friends or family to provide free child care, they often rely on subsidized child care, if not SNAP and TANF as well – just to make ends meet.

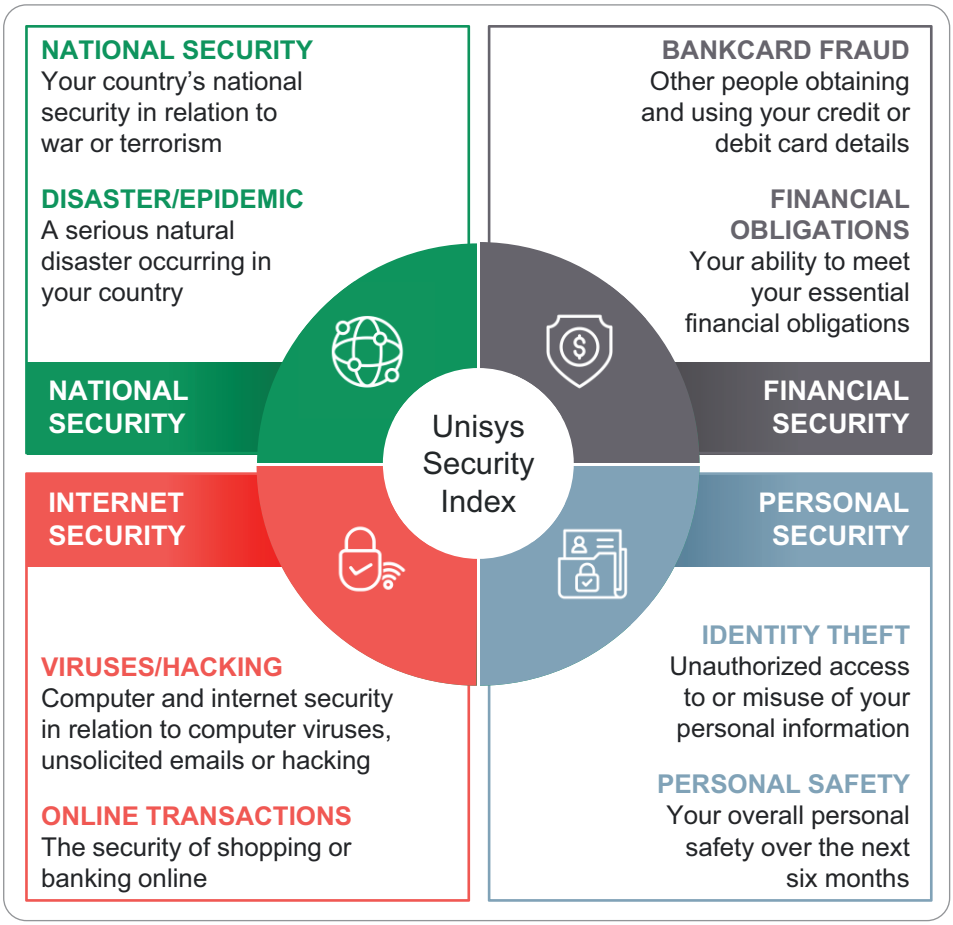
The result is that desperate people do desperate things, especially if they are facing a draconian decision: Pay the rent or pay for my children's food and medicine. So when a hacker takes down the public assistance site, the resulting chaos in the community is severe and predictable.

Along the same lines, those receiving benefits are often less educated and less technologically-savvy when it comes to securing their online personas; they are more likely to fall for phishing, 'SMiShing,' or other attempts to click on malicious sites; and their electronic devices are more likely to be older models without the most current operating system patches. The result is that those who can least tolerate a breach often suffer the most.

*Leveraging the benefits offered by cloud computing can help IT managers reduce risk.*

## Beyond Cybersecurity

Citizens relying on the public sector are also concerned about non-cyber threats. As we saw in 2020 with the COVID-19 pandemic, the ability to shift to a "work from home" model was more difficult for those in service jobs. Those relying on public transportation were less likely to be able to socially distance and those who depend on subsidized health care are more likely to ignore the symptoms. The net result is that these citizens are acutely sensitive to the "Personal Safety" and "Disaster/Epidemic" quadrants of the USI, representing Personal Security and National Security respectively.




### Recommendations

What can IT managers working the public sector do to ensure that their citizens are protected?

1. **Make Security a Priority**, and elevate it to a core aspect of the agency's mission. DHS has identified 16 "Critical Infrastructure" sectors whose protection is considered vital to the United States; attacks on these sectors are deemed to have a "debilitating effect on... public health and safety." While many are defined as commercial entities, several fall into the public, or public/private realm: Energy (including dams and nuclear), emergency services, healthcare and public health, government facilities, transportation and water/wastewater. Each of these sectors requires robust, up-to-date, and reliable security – not just cybersecurity, but physical as well.

**Janine Moore**
As the Senior Director of Social Service Industry at Unisys, Janine provides strategic guidance to Public Sector clients and Social Services agencies to modernize infrastructure, operations, and processes and to prevent fraud, waste, and abuse in benefits programs.

She can be reached at
Janine.Moore@unisys.com

2. **Leverage the Cloud**: Major cloud providers such as Azure and AWS do one thing, and they do it extremely well: They keep their servers running and safe. They employ some of the brightest minds in technology, and have the most powerful security features available. And since they operate at scale, they often represent a significant operational savings when compared with keeping IT on-premise. With limited budgets and staff, government agencies need to streamline wherever possible to keep services up and running.

3. **Preparation**: It's not a matter of "if" but "when" something happens, either from a national disaster such as a weather emergency or terrorist attack, or a cybersecurity breach. Large-scale public enterprises represent ripe targets, and if DHS recognizes that these sectors are of vital national interest, the criminals know this as well. Indeed, this is one of the reasons why cybercriminals target government services or hospitals; they know that their administrators cannot afford to go "offline" for extended periods of time to rebuild their networks. They must run 24x7, or people can die.

4. **Address Citizen Expectations**: One of the side-effects of the COVID pandemic was that citizens got used to doing things online. Amazon and other online retailers reported record revenues, and they were able to scale up to meet demand. Now, citizens expect the same near-instantaneous response from all of their interactions, including the government. Why should I have to physically visit the DMV if I can renew my driver's license online? Why do I have to venture to the courthouse to fill out forms? Citizens are asking these questions, and they are demanding answers. While government administrators scrambled to make most (if not all) of their services virtual, now is the time to take those lessons learned and re-think the public interface modules while keeping security as a key, core component.

5. **Recognize the Citizen's Concerns**: One of the advantages of a large-scale, global survey such as USI is that it touches so many people, from all economic strata and from multiple geographies. When the survey shows a sharp in a specific area, such as the spike in "Internet Security" concerns since last year, the people are speaking. Managers and administrators need to factor these concerns into their plans, tell their citizens "we hear you," and start addressing these fears into planning documents *now*.

## Conclusion

Unisys remains committed to providing secure, innovative, business-driven solutions to government agencies both large and small. We want to help *you* provide the best services possible to your citizens, and help *you* address their concerns.

**For more information,**
**please visit www.unisys.com/industries/public-sector/**