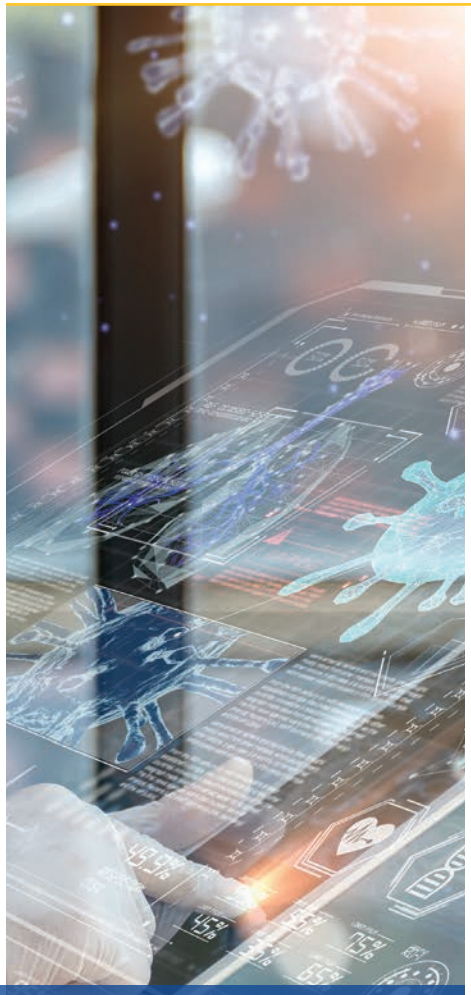
UNISYS | Securing Your Tomorrow®

INTENSIVE CARE NEEDED FOR HEALTHCARE CYBERSECURITY

By Karim Jawhary



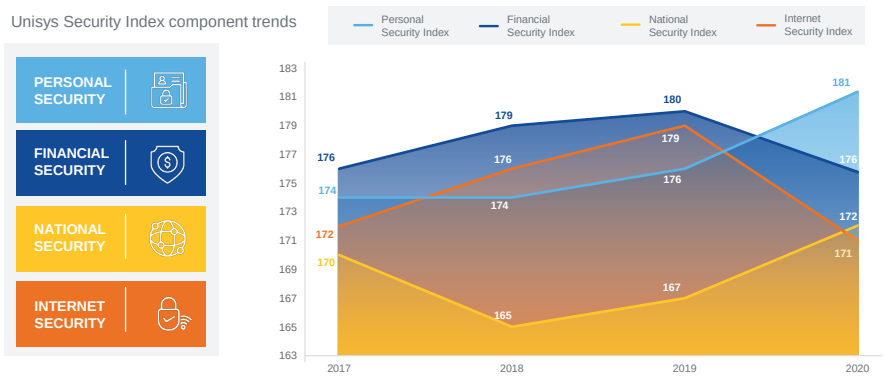
HEALTHCARE WAS ALREADY THE MOST BREACHED INDUSTRY WHEN THE PANDEMIC CAUGHT THE WORLD OFF-GUARD.

2020 Unisys Security Index Reveals Systemic Vulnerabilities

"When the worst worldwide health crisis in living memory brought much of the healthcare sector to its knees, cyber predators never skipped a beat. While they were taking full advantage of the ensuing panic to penetrate chaotic, under-protected healthcare networks, ironically consumers were for the first time in years relaxing their concern about internet security, according to the 2020 Unisys Security Index™. The post-COVID-19 environment places a premium on healthcare adopting essential, available security technologies."

When people say, "COVID changed everything," they are generally right. But when it comes to healthcare, what COVID-19 did and continues to do is amplify, to a deafening degree, what was already reverberating across the sector.

Healthcare was already the most breached industry when the pandemic caught the world off-guard and forced healthcare providers, ready or not, to turn to telehealth, work-from-home, and other expedient measures focused almost exclusively on stopping the spread, caring for the ill, and protecting healthcare workers. In the rush, security protocols often fell by the wayside. At this most inopportune juncture, consumers relaxed their vigilance. According to the 2020 Unisys Security Index (USI):



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.

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

Not surprisingly, the pandemic sparked a rise in consumer concern for their personal safety. But with thousands of workers signing into healthcare networks from home, and patients and providers rushing to handle sensitive matters over the internet, the result was a target-rich environment for cyber criminals who, like the bank robbers of old, know "where the money is." Stolen medical records go for $1,000 on the dark web. Those of the chronically ill often contain data that can become virtual annuity streams via sophisticated insurance fraud schemes.

HEALTHCARE NETWORKS ARE ONLY AS SAFE AS THE WEAKEST LINK.

Internet of Things (IoT) technologies create new vulnerabilities, and healthcare IoT skyrocketed during the pandemic as hospitals sought to free up ICU space and patients opted for remote monitoring and connected devices like heart monitors and pacemakers sending health statistics to healthcare providers for analysis and treatment. Such information is extremely sensitive, of course, and expanded IoT created the potential for new, hidden threat vectors.

Healthcare's supply chains were also thrown into turmoil by COVID-19: drugs, medical supplies, especially personal protective equipment, not to mention the transportation interruptions caused by lockdowns, quarantines, and border closures. A supply chain in turmoil is vulnerable to security lapses as participants and sourcing change or reform.

These developments can serve as the catalyst for the healthcare industry to focus anew on advanced security strategies and technologies, bearing in mind the potentially ruinous costs of breaches and ransomware: loss of customer trust, loss of customers, reputational damage, and hefty fines.

1. Match the Rush to Telehealth With a Rush to Telehealth Security.

Telehealth was already gaining traction for its cost and productivity benefits, but thanks to COVID-19, demand is predicted to soar by 63.4% in the U.S. in 2020. Virtual doctor visits went from about 12,000 a week to more than a million a week. Sick people were afraid of hospitals, hard-hit providers were keeping costs down, and the pandemic drove rural hospitals and clinics out of business, forcing people to seek online care. PHI research predicts a huge shift in demand toward home-care and expects it to be sustained post-COVID-19.

Healthcare networks are only as safe as the weakest link. Many remote care devices lack embedded security, while workers connecting via VPN on their at-home computer systems can pose easy targets for persistent hackers. Systems acquired through M&A may have hidden threat vectors.

Mat Newfield, Unisys Chief Information Security Officer, says, "Hackers are relying on tricks like password spraying, putting our most critical infrastructures at risk potentially from the click of a single working from home employee. Those remote workers are also being targeted by a spike in COVID-themed phishing, spear-phishing, and spoofing attacks – taking advantage of their workers' health concerns and lax security on home networks. They put peoples' lives at risk, as well as their personal health information, and they could lead to ransomware or to penetration of larger networks. Besides possibly being lethal, these attacks could lead to stolen personal health information.

THE PANDEMIC WILL LEAD TO A GENERAL INCREASE IN HOSTILE STATE CYBER-ACTIVITY.

2. Expect a Massive Increase in Cyber Activity From More Powerful Sources.

The high stakes of being first with a COVID-19 vaccine and owning it ensure that hostile nation-states will put their most skillful cyber experts at work, and few healthcare organizations are equipped to deter their sophisticated predations. Imagine the ransom that stolen vaccine secrets could command.

Just a month into the pandemic, prestigious entities focused on finding a COVID-19 vaccine were hacked: the United Nations' World Health Organization (WHO), the World Bank, the Bill & Melinda Gates Foundation, the National Institute of Health (NIH), the Centers for Disease Control (CDC), and a research center in Wuhan, China.

James Sullivan, a former cyber-analyst for the National Crime Agency and head of cyber research at the Royal United Services Institute, the international defence and security thinktank, said, "The pandemic will lead to a general increase in hostile state cyber-activity. It is a new opportunity for intelligence gathering and disruption. We've seen this with disinformation campaigns, cyber-espionage; there's a risk of these all exacerbating political tension and it's no surprise this is happening in an area such as the development of a vaccine."

Nor will the discovery of a COVID-19 vaccine see an end to such attacks. By many accounts, our increasingly hyper-connected world, online and IRL, will remain vulnerable to new and different viruses and diseases, so healthcare organizations will remain prime targets from powerful sources.

3. Protect PHI as It Goes Public.

The most drastic healthcare impact of COVID-19 is that it turned protected health information into a matter of public interest. Now, it is in everyone´s interest to know specific health information about people they have encountered – first-hand, second-hand, third-hand, and beyond.

But, according to USI survey of consumers, "The idea of data sharing and privacy continues to ring alarm bells." As for health information, a mere 40% are willing to share health information even with their insurance companies. Furthermore, USI reports:

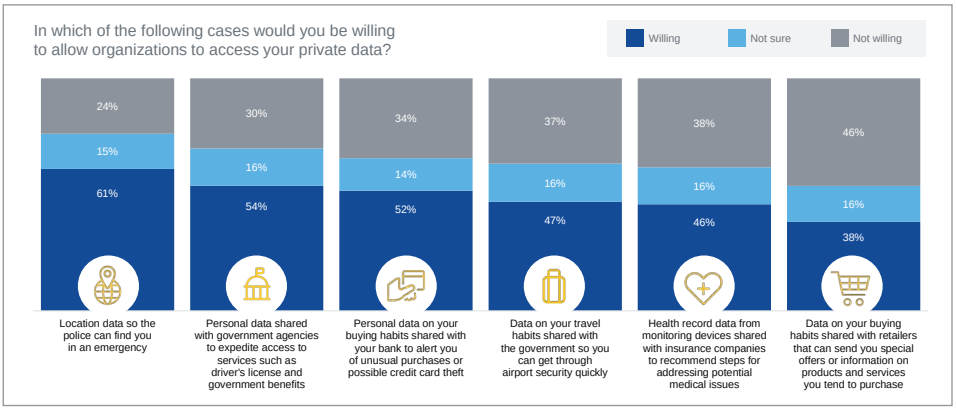
> *The issue of privacy may even have been heightened following specific COVID-19-related tracking measures used in some Asian countries in early 2020 that showed signs of early success in bringing the crisis under control... When asked about their willingness to share data with organizations, consumers are clear that both the type of organization and the purpose of the data collection determine whether data sharing is acceptable. Public sector usage...is considered more acceptable than usage by private sector businesses. Consumers are clear that data sharing is only acceptable if it is for the right reason and with a trusted organization.*

This reluctance to share data collides with what medical authorities see as the best route to containing the virus: contact tracing which requires the extensive use of a variety of information consumers heretofore have always considered private, such as where they travel or whom they dine with.

COVID-19 TURNED PROTECTED HEALTH INFORMATION INTO A MATTER OF PUBLIC INTEREST.

Karim Jawhary
is Senior Industry Director
Life Sciences and Healthcare.

He can be reached at
Karim.Jawhary@unisys.com
or connect with him at
LinkedIn.



Now that temperature screening of employees, customers, patients, congregants, and travelers can impact their participation in public and private life and even their livelihood, healthcare organizations have a tremendous moral and medical responsibility to bridge the gap between the public's right to know and the individual's right to privacy. In doing so, they will walk a fine line between complying with myriad biometric privacy laws and protecting the public's health.

A **COVID-19 Consumer Data Protection Act**, designed to protect citizens' personal health, geolocation, and proximity data collected for COVID-19-related purposes, is under consideration in the U.S. The data of European Union citizens are already covered by the General Data Protection Act.

Next, Urgent Steps

As healthcare organizations seek to improve their data security technologies and practices, they can count on the support of the Cyber4Healthcare initiative, a program designed to offer free cybersecurity services to healthcare providers fighting the COVID-19 pandemic, which Unisys supports with pro bono consultation.

As for the more sophisticated protections, security experts agree that even the most hardened, patrolled traditional security perimeter is vulnerable to breaches. Instead they recommend technology that utilizes software-defined perimeter (SDP) which controls access to resources based on user identity, thereby delivering Zero Trust security with microsegmentation. At its core microsegmentation conceals endpoints, restricts lateral data access from unauthorized traffic and cloaks personal and transactional information even when the system is already breached.

All told, the USI puts a fine point on what healthcare and security leaders have long known – an urgent, concerted focus on securing the industry is paramount.

To learn more visit

www.unisys.com/industries/commercial/life-sciences-and-healthcare

www.unisys.com/offerings/security-solutions

For more information visit www.unisys.com