CYBERSECURITY TURNS URGENT FOR MANUFACTURING

By John Hales

INTERNET SECURITY IS NOW THE LOWEST CONCERN AMONGST CONSUMERS.

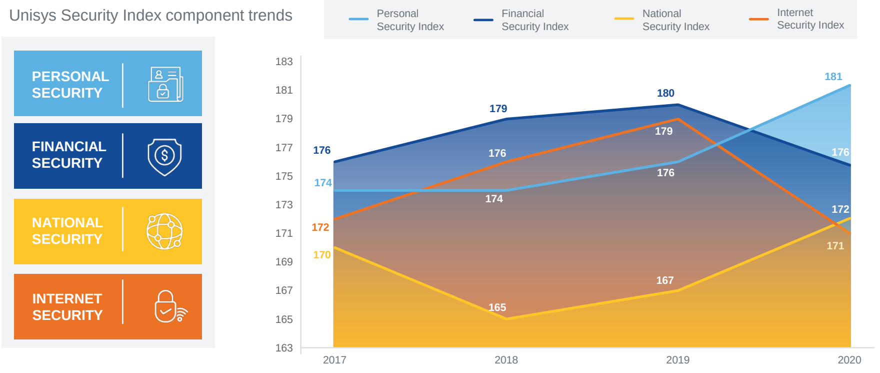
2020 Unisys Security Index Shines a Bright Light through Holes in Security

"Manufacturers are bound to be disturbed by key findings from the 2020 Unisys Security Index™. Conducted during the pandemic, the USI indicates individuals are relaxing their vigilance about security, precisely when hackers are elevating their attacks. Security experts foresee the industry accelerating its adoption of greater automation and proven protective technologies."

As manufacturers rev up their factories again, they already have a lot to contend with – supply chains in disarray, depressed demand for some products, overwhelming demand for others, new COVID-19-related equipment and policies, and geopolitical battles about technology restrictions and reshoring. The last thing they can tolerate is cybercrime.

That is why this this finding from the 2020 Unisys Security Index (USI), the longest running snapshot of consumer security concerns conducted globally for the 14th year, is especially disconcerting:

> *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.*



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.

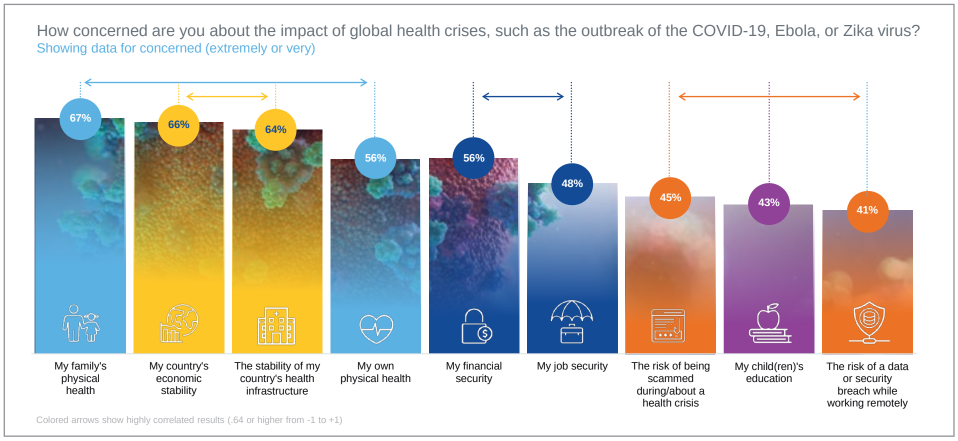
HACKERS NEVER SLEEP – THEIR SOFTWARE TROLLS THE INTERNET CONSTANTLY, AND WHEN IT FINDS AN OPENING, IT POUNCES AND MOVES FAST, INDIFFERENT TO FIREWALLS.

And it came about the same time this headline appeared, surely sending shudders through manufacturing executives around the world: Honda Hit by Ransomware: Attack Follows Major 2019 Data Breach. According to one source, the ransomware "had additional functionality programmed into it to forcibly stop processes, especially items involving Industrial Control Systems (ICS) operations." And that's what happened. It basically brought the operations of a $40 billion multinational conglomerate to a halt only months after the company had suffered the breach of almost a billion records exposing details about thousands of vehicles and their owners. Losses to the firm will easily run to tens of millions of pounds.

The shudders were not confined to manufacturers. The manufacturing industry is, after all, a central player with almost all other industrial sectors – defense, health, energy, transportation, communication, government, and food/agriculture. In the increasingly ultra-connected, online business environment, a security failure anywhere can have rippling consequences everywhere.

The USI report emphasizes the unusual nature of consumers' lessening concern about internet security:

> *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.


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

Colored arrows show highly correlated results (.64 or higher from -1 to +1)

Four Obligations and Opportunities

Unisys security and manufacturing experts have identified four pervasive points of manufacturing vulnerability that can be addressed by proven methods and technologies.

1. Expect Intruders, Have a Rapid Response Plan, and Practice It.

Hackers never sleep – their software trolls the internet constantly, and when it finds an opening, it pounces and moves fast, indifferent to firewalls. The Maersk intrusion took 90 seconds to take out 15,000 computers. In the Honda ransomware attack, it is believed that "the attackers "likely had access to Honda's internal systems for some time before launching the ransomware's encryption function."

With technology that cloaks endpoints so that hackers don't know they exist, instantly detects an intrusion, and within seconds isolates it via microsegmentation, manufacturers can avoid the ruinous financial and reputational loss suffered in large breaches.

I recently asked the security executive at a large firm, "What would you do if you discovered you'd been infiltrated with ransomware." He answered, "In all honesty, we'd have a meeting." Cybercriminals count on that, knowing time is money, and time is on their side.

2. Give Them Less to Pounce On.

It is no secret that manufacturing has a good deal of catching up to do in terms of digitalizing operations. Legacy systems abound, many without embedded security, along with ancient industrial control systems that are hard to patch, maybe no longer supported. But as manufacturers modernize their operations, they end up layering IoT devices – many without sufficient security themselves – on the vulnerable legacy systems – connecting everything to the internet without being aware of attack vectors. The widespread use of mobility expands the attack surface, as does the sudden COVID-19-driven shift to working from home on devices and networks of uncertain safety.

OF SPECIAL CONCERN IS THE FACT THAT HOMEBOUND EMPLOYEES ARE ACCESSING CORPORATE APPLICATIONS VIA VPN.

The first step is to stress-test their own networks, scanning them for vulnerabilities just like the criminals do, become aware of any and all attack vectors, and rapidly address the gaps they find. A frequent culprit is an internet modem that is deployed for temporary access to resolve a particular problem but then is never removed, leaving an accidental backdoor into the core of the network.

A second step is to develop and maintain a full understanding of the organization's overall cyber risk profile. That can be done with always-on SaaS-based software that gives leaders instant visibility into the organization's risk posture and also allows them to run their own risk scenarios, refine them, and understand the benefit of various risk reduction investments.

3. Predict Better and Faster.

Data analytics and machine learning can be wielded to anticipate new potential exploitations before they happen. A supply chain that must be suddenly disrupted for the purpose of reshoring, for example, is an obvious target for planting a backdoor in a product or installing malware. Other predictable sources of new risk would be new mobile devices in the hands of the workforce, or, of course, thousands of employees working from home on networks and devices with lax security.

Of special concern is the fact that these homebound employees are accessing corporate applications and data via VPN. Jack Koons, Unisys Chief Cybersecurity Strategist calls VPNs "vulnerability aggregators." He writes, "Hackers love VPNs because they are relatively easy to crack. They are a door into your network. Once a VPN is compromised, the attack can propagate laterally and at a great pace from server to server within the data center, with no security controls in place to stop the spread....The expanding network means doors – and attack vectors – have grown exponentially. It is next to impossible to ensure that all the doors are locked, or to verify whether everyone coming through those doors has a right to do so."

Manufacturing enterprises can adopt AI and machine learning to predict new vulnerabilities when they make significant changes to hardware and software. They can replace VPNs with technology that utilizes software-defined perimeter (SDP) which controls access to resources based on user identity, thereby delivering Zero Trust security.

DUE TO THE PANDEMIC, CONCERNS ABOUT CYBERSECURITY AND PRIVACY ARE WEIGHING MORE HEAVILY ON THE MINDS OF MANUFACTURING EXECUTIVES.

John Hales
is Enterprise Security Architect.

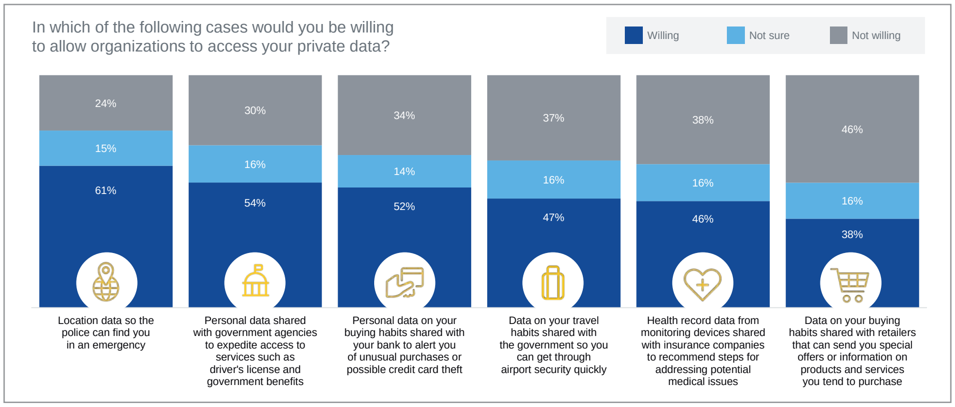
He can be reached at
John.Hales@unisys.com
or connect with him at
LinkedIn.

4. Guard Against COVID-19-Driven Security Issues.

Due to the pandemic, concerns about cybersecurity and data privacy are weighing more heavily on the minds of manufacturing executives. COVID-19 imposed new obligations on all employers, and they come with some significant security implications. Factories with many employees will likely undertake testing for COVID-19, contact tracing, collecting additional information on employee illness, determining employee's readiness to return to work and more activities that before COVID-19 would have been deemed intrusive. They will wish to collect and process such data rapidly and to store it for trend analysis and other purposes. Such information is extraordinarily sensitive, subject to privacy laws and other regulations.

It is still to be determined how employees will react to employers collecting that data. The USI found that consumers' views about sharing their personal data vary widely.

> *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.*



Of special note in this respect is the European Union's initiative, the General Data Protection Regulation (GDPR) which makes every company that processes, collects, or stores the personal data of any EU individual subject to the GDPR's requirements and its penalties. COVID-19-related GDPR considerations for manufacturers have resulted in a steep learning curve for data owners. At the forefront of data owners' minds should be GDPR fines of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. The cost of a cyberattack affecting a production line may be high, but the cost of a cyberattack affecting personal data may be even higher.

As these new COVID-19-related functions involving employee personal data roll out, the software used to support them must be embedded with stringent, GDPR-compliant security features.

Summary

The USI findings can serve as a catalyst for the security improvements manufacturing enterprises have long intended and can now employ – especially in enterprises that are not yet operating at full capacity. As leaders rethink their strategies for risk management, security, and workforce safety, the likely outcome is not only better security but also greater automation and thus greater productivity at a time when productivity is vital.

To learn more visit

www.unisys.com/industries/commercial/manufacturing

www.unisys.com/stealth

For more information visit www.unisys.com