UNISYS | Securing Your Tomorrow®

Cloud and AI Are Transforming Manufacturing, but Employees Lack of Cyber Awareness Creates New Risk

By Stijn Van Impe

2021 Unisys Security Index™ Showcases Consumer Attitudes Impacting Digital Transformation

During the pandemic, a surge in internet use and cloud consumption became a catalyst for fast-increasing cybersecurity concerns, as witnessed by the 2021 Unisys Security Index™, the longest running survey of consumer security concerns. Fueled by streams of reports on cyberattacks across a variety of sectors and organizations, internet security concerns rose nine points and jumped back to the top of the list.

Operating in 'the new normal' of the COVID-19 pandemic drove rapid further digitalization of the workplace, scaling remote work and collaboration. For the manufacturing industry, increases in demand coupled with supply chain interruptions fueled an acceleration in digital transformation. Lockdowns fueled an exponential increase in fast-track product and supply chain digitalization, enabled by cloud and AI.

At the same time, manufacturers went from controllable on-premise locations to thousands of virtual home offices, relying on the security of home networks to protect company information. As manufacturing organizations scrambled to adjust, the expanding digital attack surface provided new hunting ground for malware activists. Cybercriminals leveraged the same digital transformation tools to not only automate their attacks, but to also lower the cost of such threats.

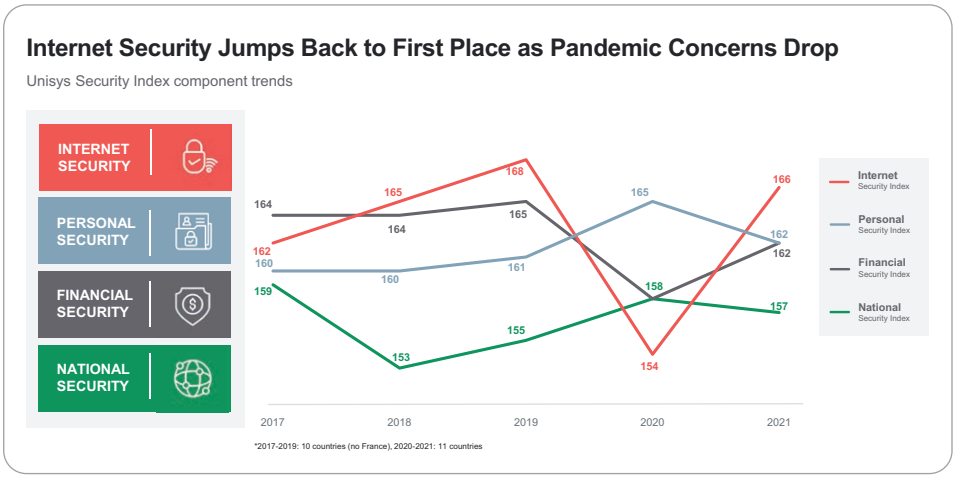
This perfect storm resulted in a 156% increase in cybercrime targeting manufacturing companies. Successful ransomware attacks took down factory operations and customer service availability. These attacks and the associated media coverage likely contributed to the steep rise in internet security concerns measured in the Unisys Security Index. This is a clear sign to manufacturers that digital security will be a key differentiator and enabler in the market.

How Are Manufactures Vulnerable to Internet Attacks?

This year's survey found that two in five consumers are not wary of clicking on links, and 79% are not aware of SIM jacking and more complicated scams. Furthermore, hackers have invested in improving their game and are now much more sophisticated. They use AI, translation engines, and automatic tools and capabilities to get nimble, low cost and versatile as they look for ways in, waiting for the right moment to attack.

Large-scale operating systems, like those found in manufacturing, are highly visible and are increasingly vulnerable for sophisticated internet attacks. These systems take longer to adjust and adapt to attacks, and as a result, need to spend more time, money and energy on malware prevention and cybersecurity.

Internet security jumps back to first place as pandemic concerns drop.



How to Enhance Seamless, Secure Digital Manufacturing Operations

To harden manufacturing systems against the evolving cyber landscape, we suggest four major preventative tactics.

Tested Education: Identity theft is one of the top sources of malware attacks. For manufacturers, employees with manufacturing control access, such as plant operators or IT administrators, are among those targeted by hackers. If an employee's credentials are compromised, a hacker can shut down your plant, ransom hack your data, and extort you for significant amounts money. Manufacturers need to invest in educating and testing plant operators, workers, and managers on how to respond to these sophisticated cyberattacks.

Automated Response: If production control personnel do not know how to respond to cyberattacks, they can inadvertently delay the response or make things worse. Automatic response tools should be put in place as an additional measure to protect against malware attacks. Automatic response systems can be used on a single device or an entire operating system.

Preventive Enterprise Segmentation: Many manufacturing companies operate their security systems in a centralized manner, but using a segmented approach gives IT security teams the ability to react, respond and rebuild more quickly and effectively. Segmentation divides the network into smaller chunks, which are each secured and can talk to each other through encrypted, cloaked tunnels. In the event that a segment is hacked, the damage is limited to only the impacted segment, protecting the rest of the network.

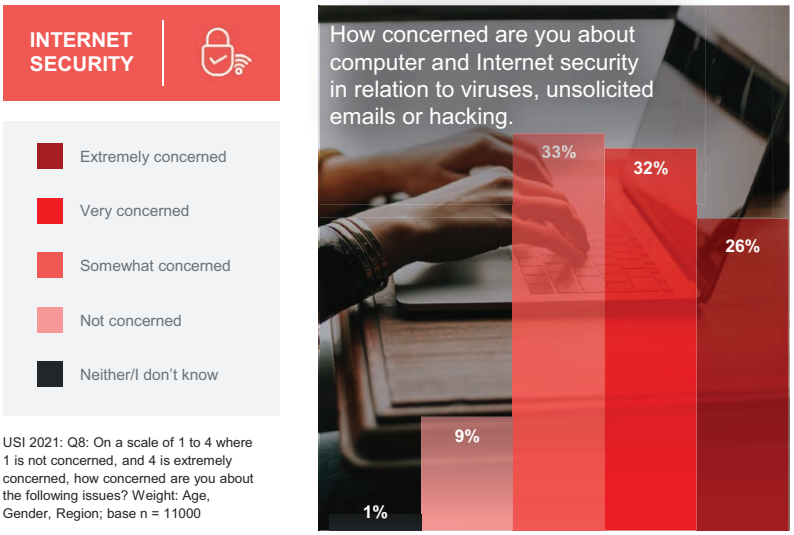
Stijn Van Impe
Stijn is Unisys' leader of EMEA Advisory Services. He is an innovation evangelist and works with Unisys' clients to bring the power of cloud, cybersecurity, and AI to deliver digital transformation programs and improve end-user experiences.

He can be reached at
stijn.vanimpe@be.unisys.com

Biometric Security: While consumers use biometric security on a daily basis, with facial recognition and fingerprints providing access to phones, bank accounts and other personal information, people are still wary of biometrics protecting their workplace. The reality is that identity theft makes up 80% of all cybersecurity incidents. When organizations strengthen identity security, cybersecurity improves. High-volume biometric screening, voice recognition and cameras are the easiest ways to protect employee identity. Globally, 69% of respondents to the survey were not comfortable sharing biometric data, including facial recognition, with their employer – even if it was to ensure safe and healthy access to facilities. In addition, 60% of employees were not comfortable with employers tracking their log in or log out times. Facial recognition and biometrics still have a long way to gain employee trust beyond mobile phones and into the professional atmosphere. However, there is an opportunity here for manufacturers to make that gain and educate their employees on how biometrics not only protects their identity better, but break the traditional trade-off between user convenience and security driving a better employee digital experience and productivity.

Cloud, AI, and Automation Protects Against Cyberattacks

The unfortunate reality is that cybercriminals will only become more sophisticated and prevalent in the manufacturing industry. Manufacturers have the responsibility to stay one step ahead of malware activists and cyber threats. Cloud and AI will help to achieve that. Once implemented securely, cloud and AI will be major competitive advantage enablers for manufacturing companies. These capabilities allow for greater innovation and open the door for manufacturers to be on the leading edge of security and operational scalability.



For more information,
please visit www.unisys.com/industries/manufacturing/

For more information visit www.unisys.com