VIEW POINT

THE IMPERATIVE OF A CYBERSECURITY-FIRST APPROACH FOR MANUFACTURING ENTERPRISES

Infosys®
Navigate your next

Digitization in manufacturing

The manufacturing industry is undergoing seismic shifts in business and technology. The COVID-19 pandemic has intensified the adoption of digitization, including digital engagement, digitization on the plant floor, and enhanced vehicle connectivity. Manufacturing enterprises need to effect a digital transformation, powered by the Internet of Things (IoT), cloud computing, big data and analytics, robotics and artificial intelligence (AI) to navigate disruption and compete more effectively.

However, digitization poses existential risks through increased vulnerability to data breaches and cyberattacks.

Developing and executing an effective cybersecurity strategy is no longer an option but a business imperative for manufacturing enterprises. A survey of 145 legal and compliance leaders conducted by Gartner, Inc. in April 2020 revealed that since COVID-19, more than 50% of respondents agree that cyberprotection and data breaches are the biggest threat to third parties interfacing with their organizations. Remote work and the increased use of videoconferencing have become occupational hazards.

Cyber-risk in manufacturing

Manufacturers should monitor and address cybersecurity risks in their ecosystem. WannaCry, LockerGaga and other ransomware attacks have targeted manufacturing enterprises and disrupted manufacturing facilities. Such breaches may lead to a complete shutdown of factories and plants. In addition, disruption of IT processes and theft of customer data can damage the credibility of manufacturers and carry reputational risk.

It is not enough to secure the perimeter of the organization any more. Cybersecurity needs to begin at the design level, particularly as the manufacturing enterprise becomes more interconnected.

The evolution in digital technology demands a corresponding pivot to a robust cybersecurity approach. However, a cybersecurity-first approach is challenging, given the velocity of change as well as the specialized skills required.

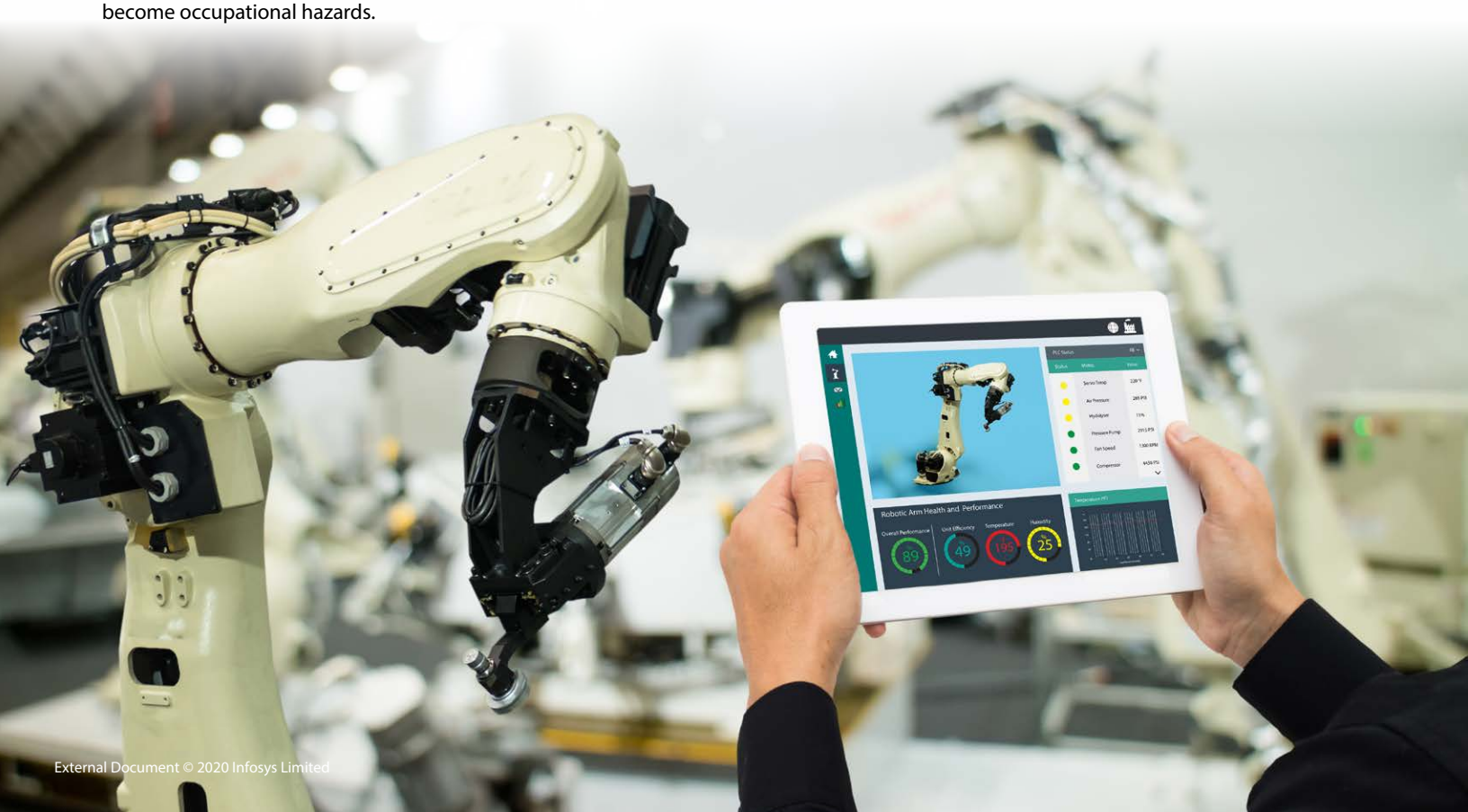
Manufacturers need to address a broad spectrum of cybersecurity risks.

Industrial espionage and secure R&D

Hackers can target a manufacturing business in several ways, including phishing and 'social engineering' tactics that possibly lead to malware infections such as ransomware and Trojan horses.

Hacking and modifying a factory operation targets operations technology (OT) or control and data acquisition (SCADA) management systems. Most manufacturing enterprises have operating technology systems to operate their factories within their corporate IT framework, which are targeted since they are accessible remotely.

Typically, manufacturing businesses have an 'air gap' between OT and equipment and their IT network, but simple methods such as a USB stick have been known to breach the air gap. Consequently, partitioning factories with the air gap network is not an effective measure.



Legacy or unmanaged infrastructure

Manufacturing enterprises use heating, ventilation and air conditioning (HVAC) systems connected to the Internet, but do not have adequate security safeguards. Many third-party applications linked to enterprise systems may lack robust protection, thereby exposing corporate networks to hackers.

Several devices with sensors that link to the Internet for communication, machine failure prediction and inventory management, are vectors that provide hackers with access to sensitive data leading to sabotage and botnet attacks.

Another area of concern for manufacturing enterprises is visibility into assets due to the distributed nature of the OT environment. Comprehensive management, maintenance and protection are nearly impossible without asset visibility and vulnerabilities associated with the assets.

Legacy and obsolete systems operate in the OT environment since the average lifespan of OT systems is 15-30 years. The network becomes vulnerable since the operating systems are possibly out of support. Replacing systems is a challenge since they may be supporting critical production processes in the OT environment.

The SCADA software and PLC firmware were designed for availability rather than security, which was not factored into the design and implementation of these systems. Further, any change in systems such as new additions of controls or patching is difficult since it needs rebooting, which disrupts the production process. Vulnerable and unpatched devices in manufacturing plants can be exploited by hackers to disrupt production.

Connected products

According to The Economic Times, the demand for cybersecurity in the automotive sector is projected to increase by a CAGR of 23.16%, from US$ 1.34 billion in 2018 to US$ 5.77 billion by 2025. While the connected goods sector grows at an exponential rate, there is traction in connected vehicles with significant improvement in electronics. With adoption of cloud-based applications in connected and autonomous vehicles, the emerging modes of mobility are exposed to cybersecurity threats. The integration of automotive electronics at scale and implementation of advanced vehicle technology such as software virtualization, digital twinning of cars / digital twins for everything – healthcare, automotive, shipping industry, connected vehicles, and self-driving vehicles, make modern vehicles vulnerable to cyberattacks.

Vehicles of the future will share data with external data centers to run a variety of applications. The integration of new products and services into the manufacturing process as part of the automation process creates more vulnerabilities. Automotive enterprises building autonomous vehicles need to safeguard owners and users from violation of privacy and infringement of personally identifiable information (PII).

Connected factories

Factories adapt to workflows in real time, with machine-to-machine as well as human-to-machine communication. By connecting all parts of the manufacturing process, a manufacturer can simplify and accelerate the process of building and testing applications across platforms. The connected factory seamlessly incorporates software, data, and processes, both on-site and over the cloud. Business disruption can be avoided by safeguarding data and applications, irrespective of the location of the data repository.

Geopolitical risks

Global threat surveys indicate that modern cyberattacks are caused by geopolitical factors, and governments faced cyber-attacks from state actors in 2018. While geopolitically motivated cyberattacks may seem to be a threat only to government institutions, the private sector is also a target for such attacks. The criticality of the situation is evident from the latest global threat surveys, which revealed that 72% of global CEOs suggested that their business may be affected by geopolitical cyberactivity.

Cybersecurity sensitization

According to a survey conducted by Infosys, 70% of consumers are not aware of cybersecurity threats. This problem is further compounded in the manufacturing industry, where there is a severe shortage of an IT-savvy workforce.

Manufacturers should protect against harm caused unintentionally by ignorant workers as well as by those with malicious intent. Risks from insiders pose a bigger threat as workers have ready access to sensitive information. A cybersecurity culture in the organization requires creating awareness, inculcating best practices, and following stringent protocols and processes.

Navigating to a secure future

Senior leadership should participate meaningfully both during the formulation of the cybersecurity strategy as well as implementation. At the same time, the chief information security officer (CISO) should perform a more prominent role in the organization.

Furthermore, cyberprotection should be an important part across the company lifecycle. Infosys recommends that businesses implement protection at each level, including design and scale, to develop a comprehensive cyberdefense framework.

This demands structural and cultural changes supported by senior leadership and cultivating a security-first attitude by employees. Visibility of assets and OT security monitoring help enterprises assess threats to production and facilitate informed decisions to protect plants from security breaches. Proper segmentation between IT and OT, and zoning of the OT network reduce the threat levels.

A successful cyberprotection program allows manufacturing enterprises to better navigate the digital economy and deliver improved operating efficiency, productivity, and business results.

A comprehensive security governance framework

The manufacturing technology ecosystem has vulnerable components that can be targeted by hackers. Enterprises need to adopt a robust security governance framework to ensure security at multiple levels.

Manufacturers need to develop a cybersecurity strategy to become more standardized and aligned with the manufacturing landscape. Enterprises need to implement advanced technologies, including in-depth defense techniques, and a combination of procedures, processes, and technology to secure process control networks, systems, devices, programs, and data from attacks, losses, delays, unauthorized access, or misuse.

Robust risk evaluation and discovery of equipment requires network assessment, software and safety protocols. The assessment should categorize and list devices across the network, identify the unique risk and sensitivity of data provided by each device.

Zero trust model for secure R&D

A stable network layer demands network segmentation and zero trust. Countermeasures introduce several layers of protection against threats (profound protection) along with operational controls. At a primary level, devices should have security updates on a regular basis.

Network architecture techniques should be enforced with adequate zoning and micro-segmentation, which involves isolation. Networks need to be segmented so that OT devices can be decoupled from conventional IT devices. In the event of a system breach, devices in that section are affected. This zone should be quarantined and remedial measures taken without risking other zones.

Network segmentation to isolate sensitive R&D systems from other systems prevents the lateral spread of malware or attacker access. 'Less privileged access' should be enforced to reduce security hazards.

Artificial intelligence can be adopted to help security professionals focus on detecting and containing cyberthreats.

Unified vulnerability management

Enhanced connectivity increases the number of threat vectors as well as the degree of cyber-risk. OT endpoints, which are distributed globally and often linked to the Internet via protocols, compromise data privacy, confidentiality, and assurance. Enterprises should undertake rigorous security scans and checks to identify new threats and vulnerabilities.

Static and dynamic testing of connected devices should be undertaken to establish a minimum safety baseline. Dynamic testing captures and uncovers code bugs and any underlying system malfunctions or vulnerabilities caused by hardware. It plays a pivotal role in identifying vulnerabilities that are created, particularly when new code is used on old processors.

It should be augmented by security design and coding standards, Safe Code Analysis, App Reverse Engineering and a dedicated fix advisory with a 'Tiger Team ' approach for vulnerability remediation.

Compliance and risk management for the partner ecosystem

An effective partner risk management program safeguards data and prevents attacks across the digital manufacturing landscape. It demands a proactive partner risk assessment using industry-standard safety posture assessment.

Relevant controls and access thresholds need to be designed and deployed for integrated partner systems. Controls should be described based on risk-related partner segmentation. Partner control should be measured using zero trust principles.

Integrated governance and escalation framework (with clear ownership and integrated workflows) are required to mitigate risks. Customized IT and governance mechanisms can be used for efficient risk control by third parties.

Safeguarding customer data

Data protection is a business imperative for the manufacturing industry. Enterprises need to address violation of privacy and infringement of PII. For instance, modern cars relay location data to their company to protect the driver in the event of a breakdown. While this service is useful, the organization should recognize the data as personal information and manage it appropriately.

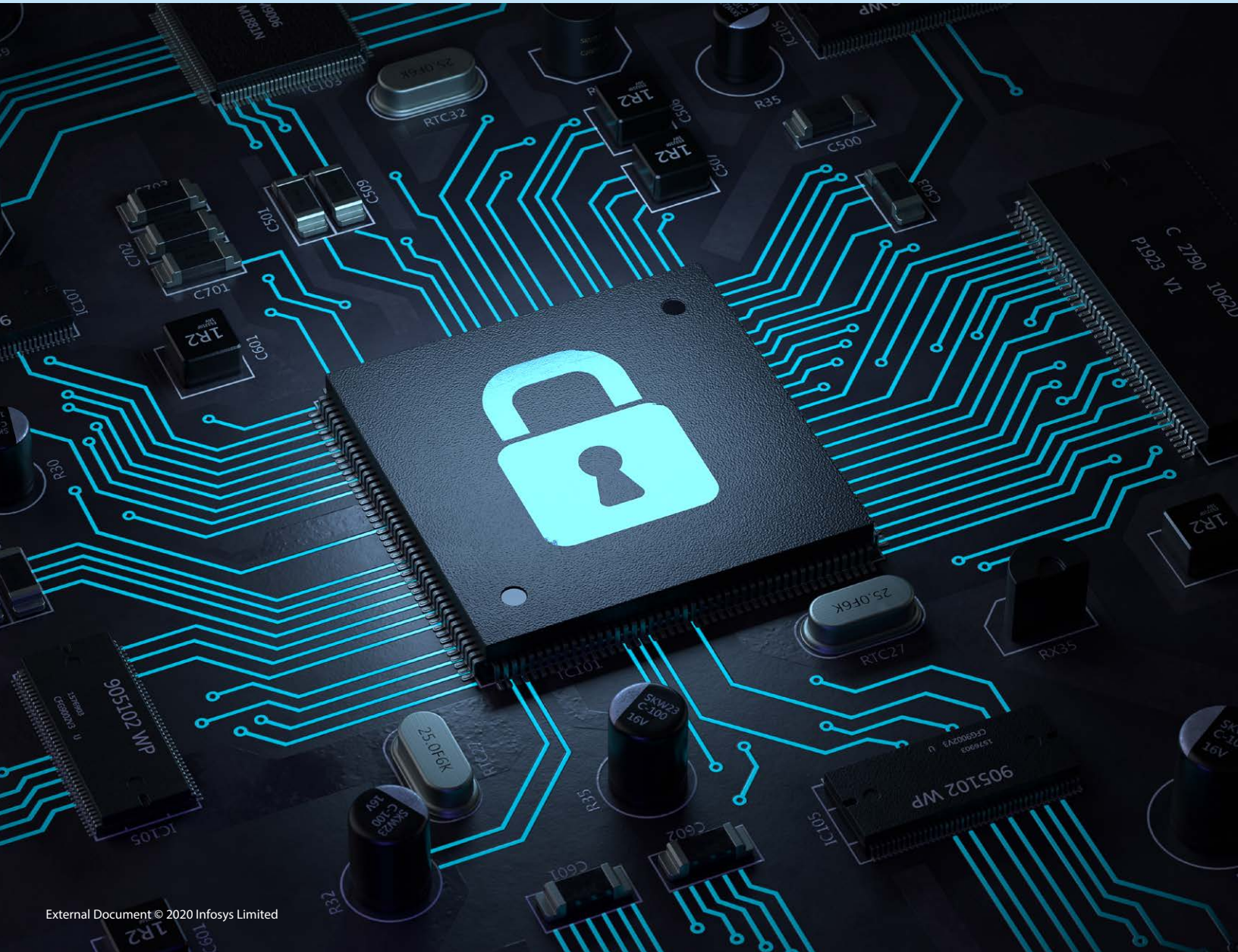
The European Union levies penalties for data breaches in the ambit of General Data Protection Regulation (GDPR). Privacy compliance is also regulated in America by the California Consumer Privacy Act (CCPA).

Companies should enforce a holistic data protection policy and set up a data protection office to manage PII data. Sensitive data should be categorized using data discovery and classification solutions. Risk mitigation strategies related to personal data should be developed and refined continuously. It should be complemented by comprehensive data security tools and software to safeguard personal information.

Managed detection and response

The evolving pattern of threats, technologies, and processes make cybersecurity a business priority for manufacturing enterprises. It demands domain experts to implement threats-detection technology, access management, risk and enforcement governance. Enterprises should prepare for rapid identification and recovery of IT to boost stability in the event of security breaches. Well-defined playbooks should be developed for early detection and prompt response.

Behavior-based anomaly detection and sandboxing can be used for threats that cannot be identified using signature-based systems. AI and automation can be incorporated into security incident management and response systems to reduce false positives. It should be complemented by constructive hunting risks.



Prioritizing cybersecurity

Infosys advises manufacturing enterprises to become secure by design. We need to develop a cybersecurity culture at a very early stage of the product and company lifecycle. Enterprises should develop frameworks, technologies, and strategies to ensure that protection is deeply ingrained across the ecosystem.

Infosys is committed to developing a resilient cybersecurity program to help manufacturing enterprises work at scale, while increasing operational performance and reducing costs. With our dedicated team of security experts, indigenous best practices, automation, deep knowledge and responsive intelligence, business versatility and predictable delivery of operations through global cyberdefense centers, Infosys is prepared to scale up the digital journey of manufacturers and ensure 'secure by scale'.

Our CyberNext Platform suite and accelerators are provided as managed security services from our six global CDCs (Cyber Defense Centers). We reinforce our capacity to execute at scale with access to the finest talent by leveraging our partnerships with Ivy League universities, such as Purdue, to reskill and upskill employees.

Infosys' tools, such as CyberGaze, based on the proprietary Infosys SEED (Security Management System, Enterprise Layer, Evolve & Turn, Detect & Respond) architecture, have evolved from the National Institute of Standards and Technology (NIST). It provides the CISO with an end-to-end view of cybersecurity initiatives and enables prompt decision-making by:

- Offering a single pane view of security metrics across the cyber landscape
- Enabling both visualization and drilling down of metrics (e.g. by position or technology)
- Enabling trending of how metric values shift over time

Infosys, a managed cybersecurity services organization, partners with global manufacturing enterprises for holistic security programs to significantly reduce costs, increase visibility, and protect enterprises against breaches.

Authors

Shridhar Iyengar, *Vice President, Automotive, Americas, Manufacturing, Infosys*

Shridhar has helped global clients in their journey across the technology landscape over the last two decades He has worked with leading automotive companies and nurtured long-term relationships.

Balamukund Sripathi, *Director, Cybersecurity, Infosys*

Bala has 24 years of experience delivering IT, risk management services and cybersecurity services for manufacturing enterprises. He has managed cybersecurity transformations and operations for global clients.

Contributors

Suhas Anandrao Desai, *Industry Principal, Cloud Security, Cybersecurity, Infosys*

Nilby Jose, *Principal Consultant, Cybersecurity, Infosys*

Prashanth P Pai, *CISSP | Lead Consultant – MFG Domain Consulting Group, Infosys*

Bhavya Devaraj, *Senior Project Manager, MFG Value Design, Infosys*

Manasi Shetty, *Associate Consultant, MFG Value Design, Infosys*

REFERENCES

https://www.helpnetsecurity.com/2019/05/23/connected-devices-growth/

https://www.manufacturingglobal.com/technology/cybersecurity-making-manufacturing-secure

https://www.infosys.com/services/cyber-security/documents/transport-logistics-industry.pdf

https://www.infosys.com/about/knowledge-institute/insights/overcoming-healthcares-cybersecurity.html

https://www.marketsandmarkets.com/PressReleases/cyber-security-automotive-industry.asp

https://besttechmagazine.com/automotive-cybersecurity-market-to-reach-usd-5-77-billion-by-2025-report-2/

https://ukmfgreview.com/sponsors/irwin-mitchell-cyber-security/

For more information, contact askus@infosys.com

Infosys®
Navigate your next