Press contact:
Marishka Martins
Tel.: +91 9930835325
E-mail: marishka.martins@capgemini.com

More than half of manufacturers expect cyberattacks to increase in the next 12 months but gaps in cyber preparedness persist

Paris, June 30, 2022 – A new report from the Capgemini Research Institute finds that 51% of industrial organizations believe that the number of cyberattacks on smart factories[1] is likely to increase over the next 12 months. Yet nearly half (47%) of manufacturers say cybersecurity in their smart factories is not a C-level concern. According to the Capgemini report, *'Smart & Secure: Why smart factories need to prioritize cybersecurity'*, few manufacturers have mature practices across the critical pillars of cybersecurity. The connected nature of smart factories is exponentially increasing the risks of attacks in the Intelligent Industry era.

Around 53% of organizations – including 60% of heavy-industry and 56% of pharma and life sciences firms – agree that most future cyberthreats will feature smart factories as their primary targets. However, a high level of awareness doesn't automatically translate to business preparedness. A lack of C-suite focus, limited budget, and human factors are noted as the top cybersecurity challenges for manufacturers to overcome.

Geert van der Linden, Cybersecurity Business Lead at Capgemini said: *"The benefits of digital transformation make manufacturers want to invest heavily in smart factories, but efforts could be undone in the blink of an eye if cybersecurity is not baked-in from the offset. The increased attack surface area and number of operational technology (OT) and Industrial Internet of Things (IIOT) devices make smart factories a prominent target for cyber criminals. Unless this is made a board-level priority, it will be difficult for organizations to overcome these challenges, educate their employees and vendors, and streamline communication between cybersecurity teams and the C-suite."*

Organizations face multiple challenges in bolstering cybersecurity at smart factories

The research found that, for many organizations, cybersecurity is not a major design factor; only 51% build cybersecurity practices in their smart factories by default. Unlike IT platforms, all organizations may not be able to scan machines at a smart factory during operational uptime.

System-level visibility of IIOT and OT devices is essential to detect when they have been compromised; 77% are concerned about the regular use of non-standard smart factory processes to repair or update OT/IIOT systems. This challenge partly originates from the low availability of the correct tools and processes, however a significant share of organizations (51%), said that smart factory cyberthreats primarily originate from their partner and vendor networks. Since 2019, 28% noted a 20% increase in employees or vendors bringing in infected devices, such as laptops and handheld devices, to install/patch smart-factory machinery.

People, not technology, remain the top threat to cybersecurity

When it comes to incidents, only a few of the organizations surveyed claimed that their cybersecurity teams have the required knowledge and skills to carry out urgent security patching without external support. One

[1] Smart Factories leverage digital platforms and technologies to gain significant improvements in productivity, quality, flexibility and service. They are powered by three key digital technologies: connectivity (utilizing the Industrial Internet of Things to collect data from sensor technology); intelligent automation (e.g., advanced robotics, machine vision, distributed control, drones, etc.) and cloud-based data management and analytics.

common cause for this widespread inadequacy is the lack of a cybersecurity leader to spearhead the required upskilling program.

When coupled with the scarcity of talent this becomes a significant challenge; 57% of organizations say that the scarcity of smart factory cybersecurity talent is much more acute than that of IT cybersecurity talent. Many organizations said that their cybersecurity analysts are overwhelmed by the vast array of OT and IIOT devices they must track to detect and prevent attempted intrusions. Moreover, cybersecurity executives said they will be unable to respond effectively to attacks in their smart factories and manufacturing locations.

A lack of collaboration between smart factory leaders and the Chief Security Officer is also an area of concern for more than half of respondents. This inability to communicate hinders an organizations' ability to detect cyber-attacks early leading to a higher level of damage.

Cybersecurity leaders take the market advantage

The report found that "Cybersecurity Leaders" who deploy mature practices across the critical pillars of cybersecurity: awareness, preparedness, and implementation of cybersecurity in smart factories, outperform their peers in multiple aspects. These include recognizing attack patterns at their early stage of deployment (74%) and reducing the impact of these attacks (72%), compared to just 46% and 41% of other organizations respectively.

Based on the analysis and insights from the 'Cybersecurity Leaders' identified, the report proposes a six-step approach to develop a robust cybersecurity strategy for smart factories:

- Perform an initial cybersecurity assessment
- Build awareness of smart factory cyberthreats across the organization
- Identify risk ownership for cyberattacks in smart factories
- Establish frameworks for smart factory cybersecurity
- Create cybersecurity practices tailored to smart factories
- Establish governance structure and communication framework with enterprise IT

To read the full report, click here.

Methodology

The Capgemini Research Institute surveyed 950 organizations and conducted in-depth interviews with leaders from different organizations. The global survey took place in October and November 2021. The sectors surveyed include heavy industry, pharma and life sciences, chemicals, hi-tech, consumer products, automotive, and aerospace and defense.

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 340,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.
Get The Future You Want | www.capgemini.com

About the Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think-tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The

Institute has dedicated research centers in India, Singapore, the United Kingdom and the United States. It was recently ranked #1 in the world for the quality of its research by independent analysts. Visit us at https://www.capgemini.com/researchinstitute/