CISA INSIGHTS

CYBER THREATS TO CRITICAL MANUFACTURING SECTOR INDUSTRIAL CONTROL SYSTEMS (ICS)

The Critical Manufacturing Sector is at risk from increased cyber-attack surface areas and limited cybersecurity workforces related to the COVID-19 pandemic. These trends increase the vulnerability[1] of the Critical Manufacturing Sector to the growing number of ransomware attacks aimed at private businesses by increasing attack surfaces and reducing protective abilities. To mitigate future threats, the Critical Manufacturing Sector should prioritize the management of risks.

BACKGROUND

CISA has identified potential operational vulnerabilities in Industrial Control Systems (the control systems that manage industrial processes) as a result of increased remote-based ICS management and industry adaptation to working conditions in the COVID-19 pandemic:

- expanded cyber-attack surfaces
- reduced network segmentation and securitization
- unauthorized access (both physical and online)

Operational adaptations to the pandemic (such as remote-work adoption) also increase the risks associated with identifying, authenticating, and securing accounts which are now more necessary than in work environments where physical access allows authentication. Managing cybersecurity risks in an ICS environment requires a blend of skills that has become onerous to maintain while facing pandemic-driven changes.

ROBOTIC PROCESS AUTOMATION (RPA)

COVID-19 restrictions on the amount of onsite workers caused more critical manufacturing plants to adopt robotic process automation (RPA)—the automation of critical manufacturing production by employing robots and management through remote operators. RPA already existed in some parts of production, but pandemic-driven uptake is an advancement from previously labor-intensive manufacturing environments.

The shift to RPA addresses pandemic risks of disruption but can potentially introduce new risks when implemented insecurely. For example, RPA requires retraining operators on new processes and strong connectivity to control robots for intricate operations–increasing the operational costs of the transition. RPA requires policies on control, validation, and monitoring to be securely used to mitigate internal risks.

Pandemic uptake of RPA necessitates effective management of remote processes. Remote control, validation, and monitoring must be tailored to support operational needs. Remote control is defined as a function of managing processes in production (such as stopping or resuming production). Validation is identifying what can be successfully performed remotely. Monitoring is a function of connectivity, security, and scenarios to mitigate potential production risks. Challenges with these include bandwidth constraints, identifying favorable remote conditions, and mitigating job losses for the workforce through retraining. Addressing this would enable the critical manufacturing industry to continue unimpeded and provide security analysts remote management access. While RPA can greatly improve the production capabilities and security of manufacturing, it also introduces external supply chain risks.

Industry adoption of RPA helps ensure business continuity during the ongoing pandemic, yet cybersecurity threats

[1] For more information on vulnerabilities to Industrial Control Systems, read the ICS Best Practices

identified by CISA complicate RPA uptake. Shifts to automation and advancements in remote control, validation, and monitoring may be able to increase productivity. These improvements in productivity and manufacturing resiliency could reduce essential critical infrastructure workforce exposure and increase critical infrastructure and community resilience. The uptake of improvements is determined in part by the perceived costs of transitioning manual systems, which can appear artificially high due to cybersecurity costs. Without developing secure automation, the benefits of RPA on future scenarios may be negated by increased vulnerability to cyber-attacks.

CYBERSECURITY WORKFORCE

Historically, cybersecurity services for industrial processes were an operational function performed by plant engineers and operators. However, as cyber-attacks become more sophisticated, the skills needed to detect and respond to threats have greatly expanded. Consequently, organizations must augment their ICS cybersecurity operations accordingly. Unfortunately, these increased requisite skills (such as remote ICS management) expand the knowledge gap between traditional IT security analysts and those required to support manufacturing environments. For example: A Manufacturing Engineer position requires two or more years of managing ICS and vendor/industry-specific certifications, on top of standard IT security experience. This heightened demand for talent also affects the talent pool available to effectively respond to these threats.

If current trends hold, attacks against manufacturing sector infrastructure will continue to increase. Environments previously 'air-gapped' may become more connected to enterprise networks, as well as to public clouds, vendor networks, and other third parties for remote management. This rapid expansion of the threat landscape and attack surface has made it far more likely manufacturing organizations will experience a cyber event significant enough to degrade or impede safety and availability of production. Supply chain attacks or disruptions further complicate manufacturing's need to operate safely. A new threat to manufacturing—ransomware (a prevalent form of cyber-attack during the pandemic due to high IT infrastructure reliance)—has begun to target systems lacking the inherent security controls required to protect themselves. The result can be catastrophic production loss and downtime as well as lost revenues and penalties for production delays.

RISK MITIGATION STRATEGIES

Managing these vulnerabilities identified by CISA requires a long-term and multi-faceted approach. For example: developing cybersecurity and operational knowledge within the shop floor environment is essential, given reduced crew density. Additionally, cybersecurity teams within firms must invest in training for security analysts to be capable of remote monitoring of manufacturing environments. The partnership between production resources and cybersecurity analysts should be developed commensurate with the organization's risk tolerance. For more mitigation strategies, review the CISA Cybersecurity Best Practices for Industrial Control Systems.

CISA'S ROLE TO STRENGTHEN NATIONAL RESILIENCE

Through CISA's efforts to understand and advise on cyber and physical risks to the nation's critical infrastructure, we help partners strengthen their own capabilities. We connect our stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience: in turn strengthening national resilience.

For more information or to seek additional help, please visit the CISA COVID-19 Resource Page or contact us at Central@CISA.DHS.GOV.