Importance of Cybersecurity in Smart Machining and Industry 4.0

Sid Dongre and Hanif Rahbari

(August 15, 2023)

The fourth industrial revolution, Industry 4.0, is mainly characterized by cyber-physical systems, Internet of things (IoT), massive connectivity, and artificial intelligence (AI), supporting automation and monitoring and so is blurring the boundary between digital and physical worlds. It is projected that the next revolution, Industry 5.0, will arrive within the next decade and will reinforce the role of manpower in the smart factories of Industry 4.0 era through new technologies such as augmented and virtual reality (AR/VR). As the manufacturing industry advances into Industry 4.0, many independent manufacturing plants are now connecting to one another to form a global factory and supply chain network each consisting of a large number of connected Industrial IoT (IIoT) devices and monitoring tools. This massive transformation has led to an increase in the frequency of cyber-attacks [1] and cybersecurity has become an important part of smart machining and Industry 4.0, and subsequently, 5.0. However, the skillsets of workers in this industry are currently limited in terms of awareness about common cybersecurity attacks and how to properly configure security protocols to mitigate such attacks.

In this white paper, we provide a brief overview of the skillsets that workers in the smart machining industry need to learn so that they can be better prepared to tackle cyber-attacks. We review known cybersecurity incidents in the smart machining industry and highlight the most critical vulnerabilities as reported by widely renowned cybersecurity firms CyberX [1] and IBM Security [2] [3] [4]. We also review existing cybersecurity standards for manufacturing, such as those developed by the National Institute of Standards and Technology (NIST) [5]. This report can be used to outline the design of a cybersecurity course containing topics that will help workers develop skillsets needed to tackle the clear and present danger of cyber-attacks to the smart machining industry. While implementing new technologies towards Industry 4.0, manufacturing plants must conduct proper risk assessments to understand cybersecurity needs, act on the findings, and implement key security protocols that can mitigate attacks.

Cybersecurity Incidents and Common Vulnerabilities

The NIST blog on Cybersecurity and Industry 4.0 identifies four key areas where cybersecurity risk assessments must be conducted to minimize harm of cybersecurity attacks to workers and equipment. These are cyber-physical systems and *Cobots* – robots programmed by humans to aid in manufacturing tasks, IoT and Big Data, cloud manufacturing, and automation [6]. For example, use of sensors and remote access tools may provide entry points for cybercriminals or industry competitors. Likewise, American Machinist lists four cybersecurity vulnerabilities for machine shops that are most frequently at risk of exploitation [7]. These vulnerabilities include unsecured CNC machines, unsecured internal devices (e.g. flash drives), poor password management, and lack of commitment to cybersecurity. More recently, the Production Machining cites the growing threat of ransomware attacks to the machining industry which is borne out of weak cybersecurity protection making the manufacturers attractive targets for attackers [8].

If not addressed, critical vulnerabilities can lead to devastating cyber-attacks. The most common attack plaguing the manufacturing industry is ransomware. One such attack was faced by Visser Precision in 2020, where the company became a target of the “DoppelPaymer” ransomware [9]. This malware

encrypts files stored on the victim system and demands the victim company pay a ransom in return for the decryption key. Visser Precision did not provide a comment on whether they paid the ransom. Unlike Visser Precision, many manufacturing companies choose not to report cyber-attacks that they have become victims of due to fear of harm to their reputation and loss of their clientele. Nevertheless, the threat of "DoppelPaymer" and other ransomware of its kind, and other types of cyber-attacks still persists.

Although ransomware is the most critical threat to the manufacturing industry, it is only one of the ways by which a manufacturing industry can become a target of cyber-attacks. Cyber risk reports, such as those developed by CyberX and IBM Security, provide a detailed analysis of IIoT systems along with the most common vulnerabilities and attacks plaguing this industry. After combining results presented in several successive reports, CyberX has analyzed over 3000 smart machining networks worldwide and developed a comprehensive Global IoT/ICS Risk Report for the year 2020 [1]. The key findings of the report are listed below:

- 62% of the networks have outdated Windows OS.
- 64% have unencrypted passwords.
- 22% detected indicators of attack (IOA).
- 54% have devices that are remotely accessible via RDP, SSH and VNC.
- 27% do not have a de-militarized zone (DMZ) and are directly connected to the Internet.
- 66% do not auto update their antivirus definitions automatically.

IBM Security has developed a similar report entitled Threat Intelligence Index which provides an analysis of several different types of computer systems and the cyber-attacks that have targeted them. In 2020, IBM Security reported that the manufacturing industry was the second-most targeted after finance and insurance [2] and it took the #1 spot in 2021 [4] and 2022 [3]. In particular, manufacturing businesses and NGOs that were a part of the COVD-19 relief efforts were reported to have become victims of sophisticated and targeted spear phishing campaigns [2]. It was reported that manufacturing industries were most commonly targeted by ransomware attacks, with the "Sodinokibi" strain being the most common in 2020 and 2021 which was displaced by the "LockBit" strain in 2022. Out of all attacks, 20% were attacking the manufacturing industry in 2020, increasing to 23% in 2021 and 25% in 2022 [2] [3] [4]. Other key findings of the IBM Threat Intelligence Index reports are listed below:

- The manufacturing industry fell victim to 33% of all data theft attacks in 2020, and 30% in 2022.
- In server access-based attacks, manufacturing industry faced 7% of them in 2020 and 12% in 2021.
- In 2020, the manufacturing industry also faced 22% of the attacks that exploited the critical path-traversal Citrix vulnerability CVE-2019-19781.

As recently as in 2022, TrendMicro conducted a security analysis of top CNC machine manufacturers and reported security problems with attack demonstrations [10]. Notably, they analyzed CNC machines from four popular manufacturers – *Haas*, *Heidenhain*, *Fanuc* and *Okuma*. Some attacks were demonstrated in all four manufacturers, such as hijacking a machine to change the programming or geometry of the tool, which can potentially even harm the machine. All four machines were also susceptible to attacks that can cause theft of production information, intellectual property and trade secrets. Other attacks that were possible in a majority of the manufacturers' machines include remote code execution, tampering with tool life and ransomware. Most of these attacks were possible through the use of malware that exploited the Microsoft Print Spooler service impersonation vulnerability (CVE-2010-2729) [11]. The report also

suggests countermeasures to mitigate these attacks, such as strong user authentication and authorization mechanisms, and regular operating system and software updates. Table 1 summarizes and lists common vulnerabilities that plague the machining industry along with feasible mitigations.

Vulnerability	Mitigation
Unsecured CNC machines could allow attackers to manipulate machine programming and disable entire machine shops via ransomware attacks	Regular software updates and vulnerability assessments
Data smuggling from unsecured internal devices leading to corporate espionage	Network monitoring and traffic analysis
Poorly managed passwords that are often stored in plaintext	Comprehensive training in cybersecurity best practices Cybersecurity Awareness campaigns Multi-factor Authentication
Upper-level management's lack of commitment to cybersecurity	

Table 1: Common vulnerabilities and feasible mitigations

Based on the findings above, we can clearly identify the most common vulnerabilities threatening the manufacturing industry. We will now review existing standards and frameworks that provide guidelines and cybersecurity best practices for the smart machining industry.

Existing Standards and Best Practices

Modern Machine Shop lists best practices for manufacturing including regular cybersecurity training and auditing, and enforcement of multi-factor authentication as key security measures that can be feasibly implemented to prevent the most common cyber-attacks [12]. Modern Machine Shop further highlights the importance of Enterprise Resource Planning in the CNC Machining Industry and how it is a key part of adhering to the requirements laid out in the Cybersecurity Maturity Model Certification (CMMC) framework developed by the U.S. Department of Defense [13].

NIST SP 800-171 Rev.2

This standard by NIST aims at protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations [5]. It provides guidelines and security requirements for protecting the confidentiality of CUI that is handled by nonfederal manufacturing companies. The target audience of this standard include but are not limited to program managers, contracting officers, chief information officers and auditors. Table 2 below provides a summarized list of security requirements under fourteen families.

Requirement Family	Summarized Requirements
Access Control	Limit system access to authorized users; control flow of CUI, employ principle of least-privilege; limit unsuccessful logon attempts; terminate user sessions after timeouts; monitor remote access sessions; authorize and protect wireless access using authentication and encryption; limit use of portable storage devices on external systems.
Awareness and Training	Ensure that personnel responsible for handling CUI are trained to carry out their assigned information security duties and responsibilities; provide security awareness training on recognizing and reporting potential indicators of insider threat.

Audit and Accountability	Create and retain system audit logs to enable monitoring, analysis, and investigation of unauthorized activity; protect audit information from unauthorized access; limit management of audit logging functionality to privileged users.
Configuration Management	Establish secure configuration settings throughout system development life cycles; employ principle of least functionality; analyze security impact of configuration changes before implementation; monitor user-installed software and employ blacklisting.
Identification and Authentication	Identify and authenticate users, processes, or devices before providing access to systems; use multi-factor authentication; employ replay-resistant authentication mechanisms; prevent reuse of identifiers; prohibit password reuse.
Incident Response	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities; test the organizations incident response capability.
Maintenance	Provide controls on techniques used to conduct maintenance; ensure sanitization of any lingering CUI; ensure testing and diagnostic tool are free of malware before use.
Media Protection	Physically and cryptographically secure and limit access to media storing CUI; prohibit use of portable storage devices prior to establishing identifiable and authenticated ownership.
Personnel Security	Screen individual prior to providing access to CUI; ensure organization systems containing CUI are protected during and after personnel actions such as terminations and transfers.
Physical Protection	Limit physical access to systems storing CUI; monitor physical facility and support infrastructure; enforce safeguarding measures for CUI at alternate work sites.
Risk Assessment	Periodically assess the risk to organizational operations, assets, and individuals relevant to storage, or transmission of CUI; scan and remediate vulnerabilities in accordance with risk assessments.
Security Assessment	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
Communications Protection	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
Information Integrity	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed; periodically update malicious code protection mechanisms.

Table 2: NIST SP 800-171 Rev.2 Security Requirements Summary

As highlighted in the table above, access control, awareness and training, identification and authentication, and maintenance are the most critical security requirements that the machining industry needs to prioritize to prevent the most severe cyber-attacks. Strict access control policies can limit the use of remote access services. Periodic and comprehensive cybersecurity awareness and training can help

educate workers and improve their ability to identify indicators of cyber-attacks. Identification and Authentication policies can help prevent password reuse and enforce multi-factor authentication. Finally, regular maintenance of smart devices is necessary to avoid use of outdated operating systems and antivirus definitions. These security requirements combined can help prevent ransomware attacks that have been cited as the most common threat to the machining industry.

References

[1] CyberX, "2020 Global IoT/ICS Risk Report," 2020. [Online]. Available: https://cyberx-labs.com/wp-content/uploads/2020/09/CYBX_2020_Risk-Report.pdf.

[2] IBM Security, "X-Force Threat Intelligence Index," 2021. [Online]. Available: https://www.cert.hu/sites/default/files/xforce_threat_intelligence_index_2021_90037390usen.pdf.

[3] IBM Security, "X-Force Threat Intelligence Index," 2023. [Online]. Available: https://www.ibm.com/downloads/cas/DB4GL8YM.

[4] IBM Security, "X-Force Threat Intelligence Index," 2022. [Online]. Available: https://www.ibm.com/downloads/cas/ADLMYLAZ.

[5] National Institute of Standards and Technology, "SP 800-171 Rev. 2 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," February 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

[6] National Institute of Standards and Technology, "Cybersecurity and Industry 4.0 - What You Need to Know," 11 May 2021. [Online]. Available: https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-and-industry-40-what-you-need-know.

[7] K. Matthews, "4 Cybersecurity Vulnerabilities for Machine Shops," American Machinist, 17 April 2019. [Online]. Available: https://www.americanmachinist.com/enterprise-data/article/21903040/4-cybersecurity-vulnerabilities-for-machine-shops.

[8] D. Korn, "How Serious Are You About Cybersecurity," Production Machining, 3 May 2022. [Online]. Available: https://www.productionmachining.com/articles/how-serious-are-you-about-cybersecurity.

[9] C. Miller, "Throwback Attack: Visser Precision suffers a DoppelPaymer randomware attack," Industrial Cybersecurity Pulse, 5 August 2021. [Online]. Available: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-visser-precision-suffers-a-doppelpaymer-ransomware-attack/.

[10] Trend Micro, "The Security Risks Faced by CNC Machines in Industry 4.0," 2022. [Online]. Available: https://documents.trendmicro.com/assets/white_papers/wp-the-security-risks-faced-by-cnc-machines-in-industry-4-0.pdf.

[11] Microsoft, "Microsoft Security Bulletin MS10-061 – Critical," 2010. [Online]. Available: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-061.

[12] M. Dandord, "5 Best Practices for Manufacturing Cybersecurity," Modern Machine Shop, 12 October 2020. [Online]. Available: https://www.mmsonline.com/articles/5-best-practices-for-manufacturing-cybersecurity.

[13] M. Danford, "Cybersecurity Becomes a CNC Machining Prerequisite," Modern Machine Shop, 21 May 2021. [Online]. Available: https://www.mmsonline.com/articles/cybersecurity-becomes-a-cnc-machining-prerequisite.

[14] Bureau of Labor Statistics, U.S. Department of Labor, "Machinists and Tool and Die Makers : Occupational Outlook Handbook," [Online]. Available: https://www.bls.gov/ooh/production/machinists-and-tool-and-die-makers.htm.