Cybersecurity Best Practices for the Manufacturing Industry

cloud security alliance®

For more information on the Cloud Security Alliance's New Jersey Chapter, visit
https://csachapter.io/new-jersey

Acknowledgements

Lead Authors:

Stan Mierzwa, M.S., CISSP, Director & Adjunct Professor, Kean University Center for Cybersecurity
David Ortiz, CDPSE, CISM, Chief Information Security Officer, Church & Dwight Co.

Peer Reviewers:

Ravindra S Gotavade

CSA Analysts:

Hillary Baron
Todd Edison

CSA Chapter:

Kean University, New Jersey Chapter

CSA Global Staff:

Claire Lehnert (Design)

Special Thanks:

Larry Hughes

Table of Contents

Abstract

The manufacturing and industrial sectors have evolved with the introduction of technologies over the past many decades. Progress in improving processes, techniques, output, quality, and efficiencies have been gained with new emerging technologies, resulting in positive and fortuitous changes for organizations. With the rapid movement towards a modern-day manufacturing environment, new and connected technologies that employ greater cyber-connectedness continue to grow, but at the same time, introduce cybersecurity risks.

Readers of this paper are provided with three main content areas:

1. an historical background of the evolutionary process from so-called "Industry 1.0" through "Industry 4.0."
2. United States and international frameworks for securing the manufacturing sector.
3. a Top 10 list of practical elements that can be rapidly employed to secure manufacturing systems from cyber threats, with a look to the future.

This paper will be of value to those wishing to rapidly learn the background of industrial and manufacturing cybersecurity challenges, and provide a way to begin assessing and addressing potential threats to such environments.

Introduction

Along with the advances and benefits of using information technology solutions also comes the damaging and harmful byproducts of potential cybersecurity incidents.

The area of manufacturing has evolved over the decades. The stages of significant manufacturing advances are coined Industry 1.0, 2.0, 3.0, with Industry 4.0 now in progress. In this continually developing paradigm, increasingly sophisticated smart machines will proactively self-monitor for failures, and suggest or automatically take measures to remediate the problems (Howard, 2018). With growing sophistication in the Cyber-Physical Systems (CPS) manufacturing sector, there will no doubt be countermeasures that can be taken to address associated security issues. Additionally, manufacturing organizations still partaking in pre-Industry 4.0 operations need to address existing cybersecurity risks associated with their implementations.

The Cybersecurity & Infrastructure Security Agency (CISA), under the parent agency of the Department of Homeland Security (DHS), characterizes the manufacturing sector among the 16 critical infrastructure sectors considered vital to the United States and globally. The unavailability or destruction of the manufacturing sector/processes can have a weakening effect on national security, economic security, and the public interest (CISA, 2021). The authors contend that when perusing any of the 16 critical infrastructure sectors, the connection and integration with manufacturing in any of the sectors includes food and agriculture, healthcare and public health, transportation, defense industrial base, and the like.

The authors of this paper briefly outline the evolutionary phases of the manufacturing industry over the decades, to frame out where technology integrations introduced cyber risks. Content related to legacy or manufacturing outfits still uses older technologies but perhaps has been retrofitted to include modern information technology systems, thereby creating cybersecurity challenges. The main section of this paper provides a practical Top 10 list that manufacturers can rapidly use to effectively respond to cybersecurity risks and incidents. Finally, we discuss the business implications of not taking prudent and necessary steps.

A Brief Background, from Industry 1.0 to 4.0

The initial incarnation of Industry 1.0 involved using expanding steam power and mechanization to increase production output (Vinitha, et al. 2020). Put simply, this paradigm empowered the breakthrough from manual labor to machines. The industries that benefited from Industry 1.0 remain in existence today, for example train transportation, textile engineering, and steam power.

Electricity made movement to Industry 2.0 possible. In this paradigm, great advances were made because of electrical power, thereby surpassing water and steam in efficiencies gained (Howard, 2018). Manufacturing began to truly emerge, with enhanced management and building resources to assist with larger mass production of various goods.

Industry 3.0 originated in the late sixties, due to greater advances in process control through **Programmable Logic Controllers (PLC)**. PLCs that led the way to the current Industry 4.0 model (Benias & Markopoulos, 2017).

With the emergence of thriving Internet and communication industries in the 1990s, the world was revolutionized in ways that individuals, systems, and solutions interconnected and exchanged information (Howard, 2018). The manufacturing industry quickly followed how individuals were sharing and obtaining information via the "Internet highway," and continues today to find ways to enhance manufacturing processes using the new medium.

Current Industry 4.0 Technology Advances

Modern and emerging manufacturing systems and factories increasingly use computer networks. The paradigm of Industry 4.0 includes integrating big data analytics, machine learning, computing in the cloud, and inclusion of a large number of sensors and smart devices (Corallo, et al. 2021). Operational Technology (OT), expands the interface edge of information technology to the physical environment. As solutions in the manufacturing world evolve and increase in technology componentry, cybersecurity challenges arise from within the used devices, information systems, and, very importantly, the communication channels.

The variety and realm of industrial-related technologies, and their associated cybersecurity risks, vary based on implementation and local and remote attack surfaces. In general, Industrial Control Systems include manufacturing systems that contain **Supervisory Control and Data Acquisitions Systems (SCADA)**, **Programmable Logic Controllers (PLCs)**, and **Distributed Control Systems (DCS)**. To obtain an industrial factor objective, integration of mechanical, hydraulic, and electrical

components combine to support these industrial control systems (Stouffer, et al. 2017). Crucially, the connection of traditional computing devices, such as PLCs, is increasingly combined with cloud-based and other modern communication and computing systems to provide greater efficiency and automation. Additionally, as with any discipline and industry, a specific knowledge set and glossary may exist. Related to the the Industrial Internet of Things (IIoT), where it is warranted to connect industrial control systems for improved business process capabilities and data analytics, a special vocabulary may emerge, and for this, there is a valuable resource from the Cloud Security Alliance (Roza, et al. 2020).

Existing US Cyber Risk Management Frameworks for the Specific Manufacturing Sector

In May 2015, NIST released Special Publication 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*. It provides specific guidance for establishing secure industrial control systems (Stouffer, et al. 2015). Included are references to other NIST Special Publication documents that provide guidance and significant relevance to the ICS industry.

In October 2020, NIST announced the publication of NISTIR 8183 Revision 1, *Cybersecurity Framework Manufacturing Profile*. The framework is a roadmap for reducing cybersecurity risk for manufacturers. It is aligned with best practices, and meant to enhance current cybersecurity standards (Stouffer et al. 2020). The profile uses the five functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover) as a starting point for defining the risk levels of Low, Moderate, and High (NIST, 2020).

International frameworks and guidelines can also be referenced, such as the ISA/IEC 62443 Series from the International Electrotechnical Commission (Industrial Society of Automation. 2021). It specifies requirements for the Security of Industrial Automation and Control Systems (IACS) which can be used to improve the safety, reliability, integrity and security of IACS using a risk-based approach. Additionally, IEC 62443 can be referred by organizations to track the current maturity level of their manufacturing plants, and then plan their future roadmap to achieve the next targeted maturity level.

Cybersecurity Challenges to Legacy Manufacturing Organizations

As companies approach Industry 4.0, they inherit the risk of cyber-physical designs without cybersecurity in mind. Historically, manufacturing systems were isolated and accessible only physically. Modern manufacturing systems are now equipped with smart devices connected to wireless networks, or direct wiring to other machines and systems. The private industrial networks do not provide adequate protection against cyber threats and make them vulnerable to cyber-attacks (Corallo, et al. 2020).

As manufacturing environments continue to evolve away from isolated systems, unmanned Internet of Things (IoT) devices are introduced. IoT devices bring the requirement for proper systems and information security management with adherence to frameworks that ensure the confidentiality, integrity, availability, and safety of both information technology and operational technology environments (CGI, 2021).

Practical Top 10 List of Items to Quickly Address with Industry 1.0-4.0 Technology Vulnerabilities

As cyber-physical connected systems continue to permeate the manufacturing industry, foundational cybersecurity risk increases. The current practices of securing the manufacturing industry still include critical asset and vulnerability management, network segmentation, secure remote connectivity, proper resiliency, least privilege access, and incident response capabilities. Cyber-physical systems that drive efficiency, automation, and access to cloud-based applications can also lead to amplification of cyber-attacks in manufacturing industries.

A practical approach to reducing Industry 1.0 to 4.0 risks begins with alignment to a cybersecurity framework such as *NIST Cybersecurity Framework Version (CSF) 1.1 Manufacturing Profile*, and the adoption of proper security controls as outlined in NIST Special Publication 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*. An outline of the approach appears in Figure 1.

This proposed approach:

1. categorizes critical assets and data by business priority inclusive of physical and safety priorities;
2. segments the information technology (IT) and operational technology (OT) networks, and further segments the OT network per the Purdue model architecture with consideration of implementing zones and conduits (CheckPoint Software Technology Limited, 2021)
3. restricts remote access to only allowable parties at allowed times with availability of Audit trails
4. applies least privilege access and privileged access management principles
5. enforces access control, on-boarding and off-boarding policies
6. implements a vulnerability management system and patching cadence as per risk determination (where risk = Likelihood * Impact) and informed threat intelligence has robust security threat detection and logging capabilities on systems and endpoints where applicable
7. installs systems with a hardened security baselines inclusive of application whitelisting. and follows strict change management guidelines
8. develops and tests cybersecurity incident response plans
9. uses a mature resiliency approach for business continuity and disaster recovery capabilities
10. provides cyber security awareness training for OT staff.

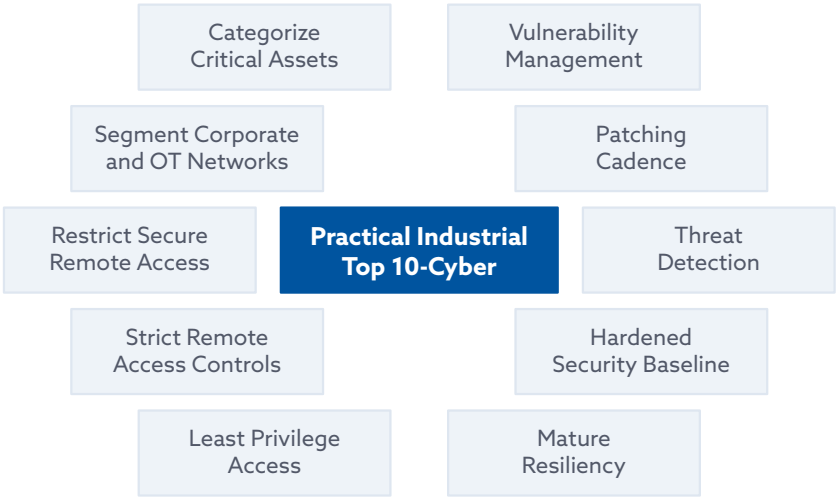

Figure 1: *Proposed Practical Top 10 Security Approaches to Industry 1.0 to 4.0 Technology Vulnerabilities*

Aligning Manufacturing Cybersecurity Efforts with the Business

Ensuring alignment with the manufacturing strategy, mission, and leadership team is key to the success of developing an operational technology-based cybersecurity program. Following business, cybersecurity, and technology alignment, cybersecurity assessments can begin to identify the top manufacturing risks and vulnerabilities, develop a cybersecurity roadmap to mitigate risk, and create a steady-state program. As solutions are chosen with cybersecurity manufacturing vendors, the program can be built, security tooling deployed, and manufacturing cyber operations incorporated into corporate cyber operations. The manufacturing business should be updated upon program build progress and steady-state activities. It should be part of cyber-focused resiliency testing, and made aware of the risk posed to the manufacturing supply chain systems. A steady state can be reached when the rate, value, or amplitude provides very little, or almost negligible change over a set period of time (Stouffer, et al. 2015).

There is no shortage of historical data that cybersecurity is a critical and significant aspect with manufacturing and industrial firms. In one instance, and with no surprise, 65% of firms focusing in manufacturing, oil and gas, utility companies, and mining see cybersecurity as their highest priority for proper governance (Hayes, 2020).

Additionally, cyber-focused resilience requires maturation of OT-specific cybersecurity incident response planning and testing. "Based on my optics from security maturity assessments, incident investigations and strategic consulting work; the OT/ICS environments in most cases are still at quite low maturity with regards to incident response (IR) readiness," Thapar said at the recent OT-ISAC Summit. He added, "IR in OT/ICS also requires a different approach as the threat profile, TTPs as well as level and nature of impact vary significantly from the typical IT environments. Recent attacks have clearly demonstrated a strong need for ensuring deep/wide visibility along with effective automated response across the converged IT-OT-IoT environment."(Industrial Cyber, 2021).

Looking Past Industry 4.0 into the Future of Cloud

The expansion of IoT into the manufacturing sector continues for many reasons, including enhanced automation,and monitoring and intelligence, and digital evidence for use in analysis and investigation, particularly if a cybersecurity incident may occur. The range of IoT evidence may exist in a wide array of devices that may evolve and include cloud-based IoT services (Hou et al. 2020). Enhancement can be made with the help of cloud resources, for example by providing additional storage and compute power. Due to the limited resources of certain IoT devices, information may be short-lived or be overwritten on a device if not sent to a cloud service (Hou et al. 2020).

The integration of IoT, cloud computing, big data and analytics, the Internet, mobile networks, digital twins, including the rise of 5G, will continue to build a sensing environment for all kinds of business, including the industrial sector (Li, et al. 2017). The use of these sensors, with the integration of cloud resources will expand an organization's attack surface. Greater co-reliance within supply chains will be necessary to ensure that cloud integration, as well as the industrial cyber protection strength, remain resilient.

Cybersecurity, manufacturing, and the Internet of Things (IoT) are addressed in the recent US Presidential Executive Order on improving our nation's cybersecurity. Going forward, emphasis on and encouragement of pilot programs will provide better situational awareness on proper security practices and development for IoT manufacturing, with even a component to provide incentives to organizations involved in building such devices (The White House, 2021).

Lastly, another area for consideration specific to the Department of Defense's (DoD) Defense Industrial Base (DIB), is the Cybersecurity Maturity Model Certification (CMMC) framework. The CMMC framework model consists of various levels of applicability that aim to ensure the defense supply chain meets cybersecurity best practices (Carnegie Mellon & Johns Hopkins University Applied Physics Laboratory, 2020). In meeting the CMMC requirements, there will be systems, processes and implementations of manufacturing technology that meet DoD guidelines , creating benefit to all stakeholders.

Conclusion

Industrial automation, manufacturing, and computing continue to evolve, morph, merge, and expand with emerging technologies. The idea that new technologies that can provide improved efficiency, quality, and effectiveness is not new, as has been demonstrated throughout the evolution of Industry 1.0 – 4.0. It is critical to ensure that new security threats are properly dealt with in all attack surfaces and scenarios. Within the industrial sector, the convergence of Information Technology and Operational Technology is progressing. As such,organizations involved in this convergence consider security and cybersecurity a top concern. A recent report from Deloitte provides that 90% of organizations in the OT sector have reported at least one security or cybersecurity compromise to their infrastructure in the preceding two years (Hayes, 2020). With this in mind, it is highly probable that organizations in this sphere will experience a disruption or breach of confidential information within their OT operations.

Although this paper is brief, it does provide a practical framework that can be used as the basis for other frameworks that minimize manufacturing cybersecurity challenges. Cloud computing is rapidly becoming the backbone of digital transformation in all industries, including the industrial sector, and includes the interconnectivity between IoT, artificial intelligence, and data analytics (Akter, 2020). With these ongoing and rapid movements, and potential for greater cybersecurity risks emerging, taking stock with one's industrial technologies to ensure all best practices are followed is a prudent activity. The Top 10 list provided in this paper can serve as the impetus for activities in organizations containing industrial technologies.

About the Chapter

The Cloud Security Alliance New Jersey Chapter is housed at Kean University which enrolls almost 16,000 students and offers more than 50 undergraduate majors and 60-plus graduate options, with four campuses in New Jersey and the only public university in America to have a campus in China. U.S. News & World Report has recently ranked Kean University among the top universities in the northern United States for helping economically disadvantaged students enroll and graduate within six years. Kean is ranked 41st for social mobility out of 170 universities in the region.

Members of the chapter include cloud security professionals, students and those from the manufacturing industry such as Church & Dwight which was founded in 1846 and headquartered in Ewing, New Jersey. It is a multi-billion-dollar company that focuses on Consumer Packaged Goods and is home to many popular brands such as ARM & HAMMER™, Trojan™, First Response™, Nair™, Spinbrush™, OxiClean™, and Orajel™. Church & Dwight includes a Consumer International presence in many areas of the world, including France, Australia, Canada, United Kingdom, Brazil, China, and Mexico.

About the Authors

Stanley Mierzwa is the Director, Center for Cybersecurity at Kean University in the United States. He lectures at Kean University on Cybersecurity Risk Management, Foundations in Cybersecurity, Cyber Policy, and Digital Crime and Terrorism. Previously he was in the role of Lead Application Security for the State of New York MTA Police. He is a member of the FBI Infragard, IEEE, CSA, ISC(2), and a board member of the global pharmacy education non-profit, Vennue Foundation. Stan holds an M.S. from the New Jersey Institute of Technology and a B.S. Electrical Engineering Technology from Fairleigh Dickinson University. He is also Certified Information Systems Security Professional (CISSP).

David Ortiz is the Chief Information Security Officer at the global consumer firm Church & Dwight Co. based in the United States. Previously he was the Chief Information Security Officer and Vice President for Cybersecurity and Infrastructure Security at Bed Bath & Beyond. David holds a degree in Computer Science from the New York University. He is also a member of the New Jersey InfraGard as board member, the Evanta New Jersey CISO Governing Body, and a member of the NJ Cloud Security Alliance. He is also a Certified Data Privacy Solutions Engineer (CDPSE) and Certified Information Security Manager (CISM).

Acknowledgements

This research case study report was self-supported out of great interest in the topic from both a professional and personal perspective, and in the strong interest to outreach to the industrial cybersecurity community. The authors are grateful to their families for providing the time and privacy, during nights and weekends, to help produce this reference publication document.

References

Akter, S., Michael, K., Rajib Uddin, M., McCarthy, G. & Rahman M. (2020). Transforming business using digital innovations: the application of AI, blockchain, cloud and data analytics. *Annals of Operations Research*.

Benias, N. & Markopoulos, A. (2017). A review on the readiness level and cyber-security challenges in Industry 4.0. *IEEE Xplore*. Doi: 10.23919/SEEDA-CECNSM.2017.8088234

Carnegie Mellon & Johns Hopkins University Applied Physics Laboratory. (2020). Cybersecurity Maturity Model Certification (CMMC). Version 1.02. As retrieved from: https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

CGI. (2021). Industry 4.0 and cybersecurity: How to protect your business against cyber risks. As retrieved from: https://www.cgi.com/en/white-paper/manufacturing/industry-4-and-cybersecurity-how-to-protect-your-business-against-cyber-risks

CheckPoint Software Technology Limited. (2021). Purdue Model for ICS Security. As retrieved from: https://www.checkpoint.com/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/purdue-model-for-ics-security/

CISA. (2021). Critical Infrastructure Sectors. Cybersecurity & Instructure Security Agency. As retrieved from: https://www.cisa.gov/critical-infrastructure-sectors

Corallo, A., Lazoi, M., Lezzi, M. & Pontrandolfo, P. (2021). Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. *IEEE Transactions on Engineering Management*.

Corallo, A., Lazoi, M. & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*. 114.

Hayes, R. (2020). Managing the successful convergence of IT and OT. Deloitte. As retrieved from: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-deloitte-managing-the-successful-convergence-of-it-and-ot.pdf

Hou, J., Li, Y., Yu. J. & Shi, W. (2020). Survey on Digital Forensics in Internet of Things. *IEEE Internet of Things Journal*. 7(1).

Howard, E. (2018). The Evolution of the Industrial Ages: Industry 1.0 to 4.0. *Simio: Forward Thinking*. As retrieved from: https://www.simio.com/blog/2018/09/05/evolution-industrial-ages-industry-1-0-4-0/

Industrial Cyber. (2021). Upcoming OT-ISAC summit to focus on shaping security best practices and strategies for OT, ICS environments. As retrieved from: https://industrialcyber.co/article/upcoming-ot-isac-summit-to-focus-on-shaping-security-best-practices-and-strategies-for-ot-ics-environments/

Industrial Society of Automation. (2021). New ISA/IEC 62443 standard specifies security capabilities for control system components. As retrieved from: https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

Kleyman, B. (2021). The IT and OT Convergence: New Benefits and Considerations. *IoT World Today*. As retrieved from: https://www.iotworldtoday.com/2021/09/10/the-it-and-ot-convergence-new-benefits-and-considerations/

Li, Y., Wu, F., Zong, W. & Li, B. (2017). Supply chain collaboration for ERP implementation: an international organizational knowledge sharing perspective. *International Journal of Operations & Production Management.*

Marr, B. (2018). What is Industry 4.? Here's a Super Easy Explanation for Anyone. *Forbes*. As Retrieved from: https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/?sh=5dc3ea0d9788

Roza, M., Ho, W., Khemissa, S. & Washington, D. (2020). Cloud Industrial Internet of Things (IIoT) – Industrial Control Systems Security Glossary. *Cloud Security Alliance*. As retrieved from: https://cloudsecurityalliance.org/artifacts/cloud-industrial-internet-of-things-iiot-industrial-control-systems-security-glossary/

Stouffer, K., Zimmerman, T., Tang, C.Y., Lubell, J., Cichonski, J. & McCarthy, J. (2017). Cybersecurity Framework Manufacturing Profile. NISTIR 8183. Revision 1. As retrieved from: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. & Hahn, A. (2015). Guide to Industrial Systems (ICS) Security. NIST Special Publication 800-82. Revision 2. As retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

The White House. (2021). Executive Order on Improving the Nation's Cybersecurity. Briefing Room - Presidential Actions. As retrieved from: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Tien, J. (2017). Internet of Things, Real-Time Decision Making, and Artificial Intelligence. *Ann. Data. Sci.* 4(2). 149-178.

Vinitha, K., Prabhu, R.A., Bhaskar, R. & Hariharan, R. (2020). Review on industrial mathematics and materials at Industry 1.0 to Industry 4.0. *MaterialsToday Proceedings*. 33(7). 3956-3960.

