How to Improve Cybersecurity in Manufacturing

With the rapid increase in the number of connected IIoT devices within a manufacturing environment and across an enterprise, the opportunity for risks of cybersecurity in manufacturing facilities increases with each new node. It is paramount to identify and mitigate as many potential cybersecurity risks as possible. The overall corporate risk will increase in proportion to the total number of connected devices within an IIoT framework. However, a dedicated review and framework plan will work toward defending against cybersecurity risks.

Attack Surface

Each new device inserted into the network increases the threat opportunity for the overall area known as the “attack surface”. This is the total sum of all the entry nodes within a network that may potentially provide unauthorized access to confidential data. There are several key risk areas of cybersecurity in manufacturing that must be addressed as part of the larger IIoT infrastructure. The larger the number of people who can access information, equipment and data, the broader the attack surface opportunity will be for potential threats. Each login, hardware node, and access credential offers an entry point into a network that can be compromised. (Kassner M.)

Threats can come from all reaches of the globe as well as internal to the organization. Companies of all sizes, both large and small are potential targets. Large companies such as Merck, Tesla and SunTrust Bank have all come forward publicly in recent years claiming to be victims of cybersecurity breaches which significantly adversely impacted their operations. Smaller manufacturing organizations may be at comparatively more risk due to their relatively smaller staffing for IT security management. (Huelsman T.)

Exfiltration

It is important to protect the intersection where information technology (IT) and manufacturing operational technology (OT) converge. This can be the most vulnerable point for potential data exploitation. Operational technology to support manufacturing should be limited in their access to broader corporate information technology and have finite interactions that are defined and available only for limited access.

People are at the core of all cyber-attacks. This means that threat origination may not be limited to the external of an enterprise but could also come internally. Compromised employees by third parties or simply those with vindictive malice may have sufficient incentive to thwart operations from the inside. (Hatchell D.) Similarly, humans and human processes are also the largest defense against threats.

Data exfiltration is defined as unauthorized transfer of information, either by a human or directed machine. These are some of the top methods of exfiltration (Forsyth E.):

- Phishing – extracting credentials from unsuspecting authorized employees, usually through email
- Removable Media – This is an ‘old school’ type of data exfiltration, but their use can insert viruses and act a means to remove proprietary data from a database. Encryption is a method to mitigate this.
- Misuse of protocol – The activity occurs when an employee intentionally circumvents security guidelines by using a back-door access or installing unauthorized 3rd party software.
- Using weak or reused passwords without 2nd factor authentication provides an easier means for attackers to gain access to data. This opens the door to identity theft.
- Drive-by downloads – This occurs when an unsupported application or browser allows an unintentional download of viruses or malware due to security holes within the software.

However, it should not be viewed as a daunting task to mitigate the cybersecurity risks within your manufacturing environment and launch a control plan to initiate them for protection of your corporate assets. There are primary actions that companies small and large can take to secure their data.

An excellent way to protect digital assets from many of the threats is to adopt an explicit cybersecurity practice at your enterprise. The most widely known openly available plan is the NIST 800-171 Cybersecurity Framework. (Forsyth E.) It provides a first point of defense for your company to initiate relatively easy affordable steps toward achieving a higher level of security protection.

Discover and Define

Discover and define the understanding for all the organizational complexity needed to manage security systems for cybersecurity aspects of the business within manufacturing. This includes the location of proprietary manufacturing information, customer data, trade secrets, financial data, order patterns, supplier data and system capabilities. All access points should be clearly understood. Interdependencies between information technology (IT) and operational technology (OT) should be vetted at all intersection points. The minimum required human authorization credentials should be identified for each interface opportunity within the manufacturing environment. Databases should be segregated based on access needs.

Each hardware node insertion into the network, whether a sensor, gateway or other wireless repeater, should be security hardened for resistance to tampering. If one entry point can be spoofed, then it has the potential to become a pathway to gain unwarranted access to data and information. Hardware should make use of a public key exchange for a secure boot process. This will allow detection of a spoofed device and permit blacklisting of devices to quarantine suspected equipment. At the least, corrupted data at the entry point can cause unwanted chaos within the confines of the manufacturing operation.

Protect and Defend

Enact appropriate safety measures to defend against attacks and ensure that mission critical services within the operation are protected. There are myriad of human safeguards that can prevent a compromise of security. Encryption of data that is stored as well as transmitted should be mandatory. Physical USB drives and other methods of data extraction should either be disabled or have forced encryption. A 2nd factor authentication for login access also prevents a simple identity theft of credentials

Filter down the human access points to the essential required staff that must have access. Employees that have changed roles or have left the company and no longer need access to key information should be removed from the approvals list. Adding employee access should require escalated approval review to be certain of requirements. Employee permissions within the network should be exclusively defined to only the areas of influence that are needed with well-defined segregated areas sectioned off to control access across boundaries. (Hannigan R.)

Identify and Take Action

It is important to detect when a cybersecurity breach occurs. Otherwise, containment actions cannot begin, and the situation may only get worse. Alerts and triggers should be established to bring immediate awareness to the unauthorized access with an attack and begin the measures for containment, and recovery. A thorough plan, established in advance, should detail the operations schedule to set in motion once an attack is identified, including personnel, network activities and backup measures. The plan should predict the most likely scenarios with the appropriate response to the events and the proper remediation action.

Restoration Plan

Any impacted data area should be able to be quarantined to prevent further virus infiltration or damage. A review of the impacted areas of the operation should be assessed to determine the scope. A perpetual back-up must be maintained to avoid total loss of information that could impact any area of the business. Eventual root cause of the issue should be identified from a thorough investigation with an appropriate closure of the security hole, whether technical or human related.

Cybersecurity risks may be increasing in manufacturing with the growth of information networks that bridge the divide between IT and OT infrastructure. Enterprises should not turn a blind eye to the impact a data breach could have on their operations. However, with an appropriate planning phase and partnering with IIoT specialists, the identification of the highest probable infiltration areas is the first step. By following a dedicated cybersecurity framework, mitigation across all aspects of the organization can provide a valuable defense for protection of the company's proprietary data.

Sources

Forsyth E., 2019 *The 5 Most Common Cybersecurity Threats to Manufacturers*
https://www.nist.gov/blogs/manufacturing-innovation-blog/5-most-common-cybersecurity-threats-ma

Huelsman T., *Cyber Risk in Advanced Manufacturing*
https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html

Hannigan R., 2019 *Why the Manufacturing Sector Finds Cybersecurity Challenging*
https://www.mbtmag.com/security/blog/13249322/why-the-manufacturing-sector-finds-cybersecurity-challenging

Hatchell D., 2018 *Cybersecurity Trends for Manufacturers*
https://industrytoday.com/article/cybersecurity-trends-for-manufacturers/

Kassner M., *Why Manufacturing Companies Need to Up Their Cybersecurity Game*
https://www.techrepublic.com/article/why-manufacturing-companies-need-to-up-their-cybersecurity-game/