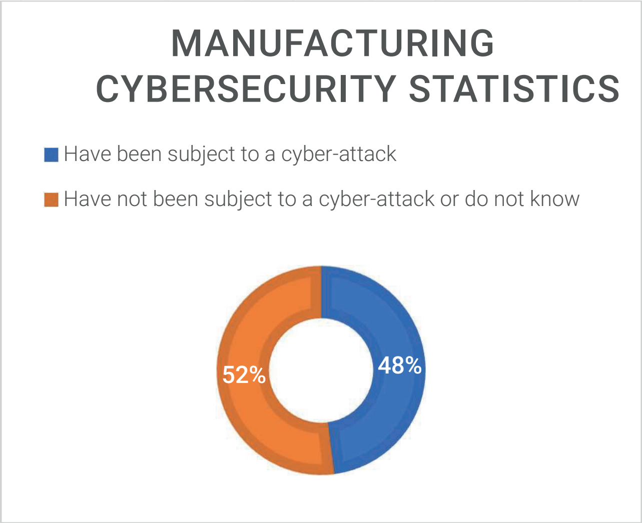
CLEARNETWORK

2019

Cybersecurity: A Manufacturers Guide

Contents

Introduction



Statistics speak volumes. Within the manufacturing industry, nearly half have experienced a cyber-attack (The Cyber Threat Landscape and the Manufacturing Industry).

This statistic coupled with the fact that nearly half of all U.S. businesses have been hacked (InsuranceJournal.com) is a testament to the ongoing concern for cybersecurity across this industry.

The time has come to bolster defenses across the entire manufacturing industry.

Background

The manufacturing industry is under fire from global hacking groups for some very specific reasons. The catalysts for this increase in attacks is due to several factors.

1. Attackers understand that manufacturing operations rely on continued production. Therefore, disrupting or halting operations is almost certain to yield a ransom or payout.
2. Manufacturing data is critical to the company. Trade secrets, formulas, methodologies, and proprietary information are the crux of revenue generation and sustainability. Attackers are hired by competitors to steal such sensitive information to reproduce your product at lower costs. No need for expensive research and development if the attackers can simply steal your data.
3. Manufacturing systems are known to be lacking in security protections and many are running on antiquated operating systems. Cyber-adversaries understand this problem and exploit them heavily. Furthermore, manufacturing networks tend to be relatively flat. No network segmentation means that one system can see any other system, so can attackers.
4. Internet of Things (IoT) devices and Industrial Control System (ICS) are widely leveraged across the manufacturing industry. This leads to a higher surface area for attack and an increased level of externally-exposed systems.
5. Hackers talk to each other. Communication among the cybercrime networks has increased exponentially. When a particular industry is found to be vulnerable, attacks tend to swing towards the susceptible targets. With all things considered, it is not surprising that manufacturers are being targeted by malicious attackers and cybercrime organizations. The time has come for the manufacturing industry to accelerate their defenses and adopt a more inclusive and holistic security posture.

An Effective Defensive Strategy

The most important aspect of heightening the defenses for manufacturers is to first acknowledge and address the statistics that are plaguing the industry. Once your organization has determined that the data held within your environment is in the crosshairs of attackers, the defensive strategy can ensue. It is not merely distant attackers that are seeking to compromise your security, but even internal employees that may be taking your sacred secrets to the competition.

1. Creating Continuity and Recoverability

In the event that insider threats or external attackers were to compromise your manufacturing operations, could you operate in a crippled state? If the answer to this question is no, it is time to consider some options.

1. Have a plan for a disaster (such as ransomware).
2. Create reliable backups.
3. Ensure that backup redundancy is implemented.
4. Test recoverability of such backups.
5. Ensure that speedy recovery operations can be implemented. The overall goal in this exercise is to ensure that when a disaster strikes, the organization can still operate. This should include items such as cyber-attacks, full network compromises, ransomware or malware propagation, or even system/data corruption.

2. Protect the Data

Your trade secrets, formulas, and other proprietary information are the lifeblood of your operations. You must protect this data at all costs from unauthorized disclosure and theft. A sudden competitor that is offering a comparable product at a lower cost will surely raise concerns on the board.

1. Conduct an inventory of all data types. Collect the type of information, location, owner, access granted, and what the level of criticality is for the organization. Rating such data on a criticality scale will enable your organization to implement focused security protocols, saving time, money, and resources.
2. Know who is accessing, modifying, or exfiltrating your data. A Security Information and Event Management platform will enable you to do just that.
3. Encrypt data-at-rest and data-in-transit. Furthermore, protect the keys for decryption.
4. Ensure that sensitive data does not migrate to less-protected systems.

Insider Threats

A study by IBM showed that 60% of attacks are perpetrated by insiders (IBM).

The most important aspect of heightening the defenses for manufacturers is to address the statistics that are plaguing the industry. Once your organization has determined that the data held within your environment is in the crosshairs of attackers, the defensive strategy can ensue. It is not merely distant attackers that are seeking to compromise your security, but even internal employees that may be taking your sacred secrets to the competition. Insider threats do not need to have malicious intent. These are often employees that make simple, yet consequential mistakes that lead to data breaches and network compromises. Insiders already have access to your networks, systems, data, and trust. This is a risky combination that leads to cybersecurity incidents that remain under-the-radar for extended periods of time. Detection of insider threats can be a daunting task. Organizations must first determine what is normal user activity to decipher what are the deviations from the standard behavior. A Security Information and Event Management System (SIEM) can assist with this critical component.

3. System and Network Security Hygiene

Many manufacturing companies have networks that are relatively “flat”. This term is used when a network configuration does not support segmentation of assets. Therefore, from any particular point on the network, an attack can move laterally to compromise other systems without requiring a sophisticated tactic to circumvent security controls

The outdated and otherwise antiquated operating systems that are used within manufacturing organizations also represents an area of high-risk. Malware authors understand that such systems do not have security patches, nor do they support advanced security technologies. Therefore, in creating malicious code, the attackers target specific operating systems to be prime candidates for compromise. Additionally, without the steady influx of security patches available, even if these systems have hostbased endpoint protection, antivirus, or secure configurations, exploitation is as simple as 1..2..3.

The vendors of manufacturing software have been known to deny supporting the latest operating systems. This essentially means that installing such software on new operating systems may render your production lines useless. This places manufacturing organizations in a precarious position. No updates for the systems or software, no network segmentation, no path to migration. Following the steps below will help to protect you in such dire situations.

1. Segment your network. Place vulnerable, outdated, or unsupported systems into their unique zones. Ensure that those risky systems cannot communicate with other sensitive systems. In the event of a breach, you may be able to contain the threat to one segment, rather than a fullnetwork compromise.
2. Put pressure on the software or machine vendor to upgrade their code to support new and supported operating systems. If you place enough pressure on them, the vendors may reconsider their lack of security due diligence.
3. Monitor risky systems. Treat them as if they are already infected. A perfect methodology leverages a SIEM platform to detect suspicious activities or attacks against these systems; enabling your team to respond swiftly.
4. Scan everything for vulnerabilities and patch; quickly!

By the Numbers

A recent study by BitSight showed:

- Over 2,000 organizations leverage outdated and/or unsupported operating systems across 50% of their computers.
- 8,500 organizations have more than 50% of their systems running out-of-date internet browsers, doubling the chances of experiencing a publicly disclosed data breach.
- Running outdated operating systems on the majority of your network nearly triples the chances of a data breach.

Outdated and unsupported operating systems and software can spell disaster f or your organization. Since such systems and software are not supported, security patches and big fixes are not generally released without some special exemptions.
Tackling this problem has been a hurdle for many manufacturing organizations. According to a ClearNetwork affiliate that specializes in incident response, 90% of the manufacturing organizations that were hit with cyber-attacks were running outdated or unsupported operating systems

4. Don't Overlook ICS and Io

The threats to your manufacturing organization do not stop with servers, workstations, laptops, and network devices. There are many other inclusions that are heavily exploited by cyber-attackers. Some of these devices may be more crucial to your operations than you realize. Determining the exposure of your organizational assets begins with a holistic strategy to detect, fingerprint, and discover vulnerabilities on all devices. Some "less traditional" items that hackers heavily exploit are:

- IP-Based Camera systems
- Building Control Systems
- Programable Logic Controllers (PLC's)
- Supervisory Control and Data Acquisition (SCADA)
- Manufacturing Robotics Systems
- Industrial Internet of Things (IIoT) Devices
- Smart Factorie

Many modern factories and manufacturing facilities offer some level of interconnectivity among the devices that produce and the central information technology environment. Attackers currently leverage an online tool dubbed Shodan.io to discover such devices that could be attacked and are exposed to the outside world.

With the recent slew of attacks on manufacturing companies, the trajectory is clear for hackers; steal intellectual property and reproduce cheaper goods. IoT, IIoT, and ICS devices are extremely prevalent within such environments so how should you approach this new interconnected exposure to your business?

1. Inventory all interconnected devices. Determine which devices are exposed to the outside world via vulnerability scanning and discovery. Outsourced Security Operations Centers will perform this feat for you if you are unclear on how to execute.
2. Keep a robust and updated network architecture diagram that describes each individual data path and interconnection. Furthermore, decipher what is critical among such IoT, IIoT, and ICS devices and what they require as far as connections. If such devices do not need to be directed exposed to the internet, remove them quickly.
3. Segmentation again. If possible, removing the ability for such devices to communicate freely with other systems on the IT network can help in limiting the damage of attacks propagated through these surfaces.
4. Monitor the interconnected devices for abnormal activity through a SIEM tool or log correlation engine. The systems may relay activities that are under-the-radar enough to not raise red flags. It is paramount that these systems are seen as digital assets that can be attacked and most likely will be

MANUFACTURING VULNERABILITIES

A recent report by Verizon showed that 86% of cyber-attacks are targeted as opposed to the more opportunistic attacks on other industries where hackers "get lucky" and discover vulnerable targets.

47% of breaches involve the theft of intellectual property (IP). This data theft technique is leveraged to gain competitive advantages and trade secrets are the most common data type breached in manufacturing companies.

- Verizon DBIR

5. Communication

As stated previously, cyber-threats are masters at communication. Long gone are the days of hackers in the basement of their homes. Such hackers still exist however, we are within the age of digital transformation and organized crime.

“Attackers reside within networks, on average, for 146 days before detection”.

“The average cost of a data breach to a company is currently $3.8 million USD”

-Microsoft

Cyber-criminals are organized, well-trained, funded, and in many cases are sponsored by nation-states or larger organizations to conduct their nefarious activities. The attackers have capitalized, communicated, and seized the opportunities in their sights.

The dark web or deep web is used for communication among cyber-criminals. Encrypted communication channels are leveraged to avoid law enforcement and other agencies. Due diligence is taken by attackers to ensure that their devious methodologies are protected. What was once regarded as curious hacking has now turned into a global industry that is expected to be worth a staggering $6 Trillion USD annually by 2021 (Cybersecurity Ventures).

In the past, the worry of cyber-attacks was limited to that of large companies, governments, and military organizations. However, the paradigm has shifted to include all entities; large or small. Communication of our cyber -adversaries calls for an increase in organizational communication, oversight and monitoring. Your security posture should regularly monitor the behavior of individuals, system performance, vulnerabilities, malware, and other infections. Furthermore, communication across all cybersecurity avenues can rapidly change the resiliency of your organization. By staying informed, your organization can stay abreast of cyber-threats. With attackers effectively communicating, your organization should be:

1. Conduct reconnaissance on the web for chatter regarding your company. Using tools such as haveibeenpwned.com and other dark web search engines can relay information if your organization is listed on the dark web as a target or even worse; already breached.
2. Know who is attacking you. This is commonly overlooked as cyber-attacks can be loaded into a single bucket. However, understanding if the attacker’s sources are known nation-states or an apartment complex in downtown Delaware may indicate if you are being specifically targeted by advanced hacking operatives or a rouge teenager with a laptop.
3. Monitor for changes among your employees. Insider threats are very real. Previously loyal employees can be compromised. Money talks and when employees are presented by hackers with an attractive compensation package for stealing your data, they may act. An outsourced security operations center may be able to tip you off if suspicious activity is detected among legitimate users.

> *“You must not fight too often with one enemy, or you will teach him all your art of war”*
>
> *-Napoleon Bonaparte*

Conclusion

Cyber-attackers follow similar paths to exploitation and compromise. However, the micro-level intricacies leveraged in attacks can vary greatly. Luckily for legitimate organizations, bolstering defenses against our adversaries is relatively clear. Based on the number of attacks that have occurred in the past and undergone investigation, a holistic and inclusive best-practices approach to defending manufacturing organizations is recommended.

To Recap:

- **Prepare for impact.** Brace your organization and prepare for the worst-case scenarios. Data destruction, brand damage, cyber breaches, ransomware, data theft, and many more fall into this category. Be ready to detect, respond, and recover.

- **Understand that you are a target.** Your data is precious to you and to cyber-attackers. Inventory, categorize, determine access controls, encrypt, and monitor for unauthorized access, changes, and exfiltration.

- **Take care of your cyber-hygiene.** Network segmentation, vulnerability scanning, system updates, patching, and monitoring via a SIEM tool is a trusted approach. Assume that hackers will get in and when they do, be prepared to slow them down or stop them.

- **IoT, IIoT, and ICS** are likely critical components of your business. Acknowledge that these devices need protection and monitoring. Attackers are finding, exploiting, and using them as conduits for entering your network and wreaking havoc. Determine your external exposure and close any gates that you can.

- **Communicate effectively.** Our adversaries are talking to one another and so should you. Internal communication regarding your cybersecurity posture is the keystone of cyber-success. Measure your risk, conduct your own reconnaissance to determine what may be in-the-wild, monitor your employee behaviors, and understand who may be targeting you. Threats are everywhere from malware, viruses, phishing attacks, vulnerability exploitation, social engineering, and even insiders. Ensure that all bases are covered and keep the lines of communication open with you cyber-sentinels and business leaders.

ClearNetwork Managed SIEM & SOC

Tackling best practices recommendations and staying ahead of cyber-attackers does not require complexity. In f act, the Managed SIEM & SOC solutions provider by ClearNetwork can rapidly elevate your security posture. By employing the Managed SIEM & SOC program by ClearNetwork, your organization can:

- **Security Monitoring:** Scalable security monitoring for every type of infrastructure. AWS, Azure, cloud applications, and on-premises physical and virtual environments.
- **Asset Discovery & Inventory:** Know what you have, all of the time. Monitor for new devices such as cloud systems, workstations, laptops, IoT, servers, network devices, mobile devices, and more. Understanding your environment is key to your cyber-success.
- **Behavioral Monitoring:** Monitoring for insider threats can be daunting. The Managed SIEM and SOC program from ClearNetwork helps to ensure that the human element is monitored for suspicious changes. Don't let malicious insiders or other trusted employees make mistakes or intentionally compromise your organization.
- **Correlate and Log Events:** Take the events from all of your devices and platforms and streamline threat intelligence to detect malicious incidents. Staying in front of such events is critical.
- **Continuous Threat Intelligence:** In the world of information security, your security intelligence is paramount. Attacks are changing every minute. Stay ahead of the newest threats with enterprisegrade threat intelligence.
- **Vulnerability Assessment:** Enable the ClearNetwork Managed SIEM & SOC service to scan your systems and devices for vulnerabilities. Ensure that you have adequate time to patch and mitigate vulnerabilities, flaws, misconfigurations, and bugs before they are exploited.
- **Intrusion Detection and Alerting:** With cyber-attacks lingering for over 1-year on average, don't be late to respond. Know what is happening now so that a response can be formulated quickly to mitigate threats before they become data breaches.
- **Log Management:** Centralization of logs is a critical facet of any information security program. Gathering and combining logs from all sources into a single source is a best practice that expedites security discoveries.
- **Compliance and Reporting:** Simplification of regulatory compliance can be achieved through the use of ClearNetwork's Managed SIEM/SOC. Gathering all of the valuable security intelligence and metrics to be relayed in clear and concise reports can help you to get compliant and remain compliant.

To provide adequate protections in the age of digital transformation and super-interconnectivity, taking appropriate security measures is a basic necessity for sustained cybersecurity resiliency.

If you are uncertain on how to achieve this, contacting ClearNetwork regarding Security Operations Center information and SIEM benefits can be your first step towards achieving this goal.

Sales: sales@clearnetwork.com
Phone: (800) 463-7920
Web: clearnetwork.com

References

https://www.eef.org.uk/resources-and-knowledge/research-and-intelligence/industry-reports/cybersecurity-for-manufacturers

https://www.insurancejournal.com/news/national/2017/09/29/465954.htm

https://www-03.ibm.com/press/us/en/pressrelease/50241.wss

https://www.bitsight.com/press-releases/thousands-organizations-run-majority-of-computers-onoutdated-operating-systems

https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Hacking-the-factory-floorCybersecurity-in-smart-manufacturing

https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/