AT&T Cybersecurity

AT&T Business | Check Point SOFTWARE TECHNOLOGIES LTD

Manufacturing: A growing target for cyberattacks

Introduction

The manufacturing sector is under attack on numerous fronts. Uncertain trade policies are creating economic imbalances. Sourcing materials overseas is getting more expensive, which makes selling finished products in key markets more difficult. In tight times, it is tempting for organizations to scale back IT budgets, including essential cybersecurity upgrades. However, with today's highly destructive cyberattacks, putting cybersecurity on hold is no longer feasible, and some may consider it reckless. One recent research report validated that manufacturing firms need to stay current with their cybersecurity. Less than 40% of respondents in Sikich's 2020 Manufacturing and Distribution Report said they perform important data breach prevention activities, such as penetration testing, phishing exercises on employees, and assessments of vendors' data security efforts. However, nearly half of respondents said their companies experienced cyberattacks during the past 12 months.[1] "Digital technologies—such as connected devices in the industrial Internet of Things (IIoT), artificial intelligence, and robotics, among others—continue to receive significant attention. These technologies are rewriting the rules of competition for industrial companies, while also increasing their vulnerability to the growing threat of cyberattacks and data breaches."[2]

As "smart" manufacturing continues to expand, the management of cybersecurity risk must become a top priority. Manufacturing is one of the 16 critical infrastructure sectors (CI) underpinning global economies.[3]

In this paper, we explore what manufacturers must consider when updating cybersecurity strategies and offer best practices that can help you prevent a wide range of cyberattacks, and keep your systems and operations running smoothly.

> **"Manufacturing has always been an industry which harnesses technology in order to deliver greater efficiency and productivity. It's a trend which we're set to see increase especially as more manufacturers adopt digital technologies and Industry 4.0 gains traction."[4]**

Manufacturing cyberattack landscape

Manufacturers are under continuous fire from criminal hackers seeking to steal and extort manufacturer's operating funds using banking trojans, phishing attacks, ransomware, and other malware. Likewise, industrial spies —sometimes supported by nation states—are on a mission to steal intellectual property (IP), such as new product designs and customer data.

One report said that an internal network of the U.S.-based National Association of Manufacturers (NAM) was hacked with tools and techniques associated with a foreign nation to gain competitive economic insights.[5]

[1] "M&D Report 2020 Racing Forward," by Jerry Murphy, Sikich LLP, 2020

[2] "M&D Report 2019 Transforming for Tomorrow," by Jerry Murphy, Sikich LLP, 2019

[3] "The European Union (EU) uses the term "Essential Functions" which closely mirrors the U.S. CI sectors. The delineation of essential functions is part of the EU's Networked Information Security (NIS) Directive." As referenced in "Global cybersecurity risks in the manufacturing industry" by Norma Krayem for Willis Towers Watson 2019.

[4] "Jump starting digital transformation in manufacturing," by Ray Watson, Global Manufacturing, February 8, 2019.

[5] "Exclusive: U.S. manufacturing group hacked by China as trade talks intensified – sources," by Christopher Bing, Reuters, November 13, 2019

Malware: Cybercriminals invade the manufacturing process by implanting malware in devices with embedded processors. This preloaded malware is used in "supply chain attacks" that can include distributed denial of service (DDoS) attacks and illicit cryptocurrency miners, among others. File-encrypting malware known as ransomware restricts a manufacturer's access to critical data, contingent on the payment of a "ransom." The now legendary WannaCry and NotPetya ransomware attacks spread rapidly through multiple vectors to paralyze hundreds of thousands of manufacturing organizations around the world.

Some studies cite that destructive malware is on the rise for the industry.[6] Manufacturing firms are an appealing target for attackers because of the critical infrastructure used by the sector.

- Research conducted by IBM's X-Force IRIS incident response team revealed that 50% of organizations affected by cyberattacks in 2019 are in the manufacturing sector.[7]
- According to the report, 60% of manufacturing firms were hit with at least one WannaCry-related attack in the first six months of 2019.[7]

Malware which was once deployed by sophisticated nation-state actors is now being used by common cybercriminals.[8] Manufacturers should think twice before cutting back on IT budgets, as **these attacks cost multinational companies an average of $239 million, destroy an average of 12,000 machines per company, and require an average of 512 hours of work by incident response teams.[9]**

Under Attack

Manufacturers are at risk of attack from:

- Cybercriminals
- Nation states
- Hacktivists

Who are looking to:

- Steal and extort financial assets
- Exfiltrate intellectual property
- Disrupt supply chains
- Protest business practices or influence policies

These high costs impose significant pressure on businesses to quickly pay the ransom to restore business operations.[10] Between the frequency and cost of these breaches, it is safe to say that the sector must protect itself from these costly attacks.

Phishing: Phishing is an increasingly sophisticated form of cyberattack in which cybercriminals use deceptive emails or websites to gather valuable and sensitive information. As they target a manufacturer's critical information for gain, cybercriminals may also seek to steal identity and email address information about manufacturers' partners to launch further phishing and other attacks on them.

[6] "Cyberattacks against industrial targets have doubled over the last 6 months" by Charlie Osborne, for ZDNet 2019.

[7] "Major Attacks That Hit the Manufacturing Sector in 2019", cyware.com, October 10, 2019

[8] "From State-Sponsored Attackers to Common Cybercriminals: Destructive Attacks on the Rise" by Camille Singleton and Charles DeBeck, Security Intelligence, 2019.

[9] Ibid

[10] Threat Intel Report, Kivu, 2019 Paid Ransomware Report

The complexities of the manufacturing environment create an ever-expanding array of attack surfaces.

What makes manufacturers ripe for malicious attacks?

Manufacturers have been involved in a digital transformation for several decades, with successive shifts offering a competitive advantage for those at the leading edge. This transformation, however, must be matched with cybersecurity measures, especially given that manufacturing is currently one of 55 national critical functions at highest risk for a cyberattack.[11]

Each new technological innovation comes with vulnerabilities that cyberattackers can exploit. This is especially true with operating technology (OT), such as software for supervisory control and data acquisition (SCADA), joining with IT technology to become the industrial Internet of Things (IIoT). IIoT connects manufacturer-owned devices to every corner of the globe.

> "Manufacturers should look closely at the IoT devices and partners they're considering to ensure they aren't implementing poorly secured devices or networks. A few approaches to consider are better managing ecosystems and developing more robust data management policies."
> — Rob Mesirow, leader of PWC Connected Solutions/IoT practice[12]

The complexities of the manufacturing environment create an ever-expanding array of attack surfaces.

- The proliferation of IIoT devices increases potential points of contact.
- IT systems are refreshed, on average, every three to five years, OT systems, by contrast, last 10 to 15 years.[13] These older systems may have unpatched vulnerabilities or may not meet updated Wi-Fi protocol standards, thus creating security gaps.
- Increasingly, employees use personal, insecure smart phones to connect to corporate services.
- And at the corporate level, there is new reliance on software as a service (SaaS) and cloud infrastructures for data processing across all parts of the organization.

How, then, should manufacturers address these cybersecurity challenges?

[11] "Global cybersecurity risks in the manufacturing industry" by Norma Krayem for Willis Towers Watson 2019

[12] "2020: Future of Manufacturing Technology," by Peter Fretty, Industry Week, December 2, 2019

[13] "Controlling security within IIoT," by Satish Gannu, TechRadar, August 22, 2019.

Cybersecurity best practices for manufacturers

Typically, manufacturers have accumulated a patchwork of point solutions to:

- Protect their corporate perimeter
- Help secure email
- Protect web usage
- Safeguard other IT services

Early on, IT security added solutions from multiple providers, thinking the differing security technologies would confound attackers. However, this thinking has drastically changed. Using disparate solutions that do not share threat data can leave security gaps and degrade the accuracy of threat detection. This is especially true within SaaS, mobile devices, and virtual environments that are not protected by legacy perimeter-based security devices. In addition, monitoring several security products through their individual interfaces increases the workload volume and complexity for IT and cybersecurity staff. This, in turn, increases the chances of an organization either missing an attack or being overwhelmed by one.

Simplify:

Consolidate your cybersecurity

One answer is to replace point security solutions with a unified security architecture.

When fully deployed, this architecture approach will help protect corporate data centers, cloud and virtual infrastructures, SaaS, mobile-devices, and endpoints simultaneously. Unified security architecture shares threat intelligence across all these environments to plug the security gaps that point solutions leave open. It also provides administrators with complete visibility of all environments through one interface.

This approach makes monitoring alerts straightforward and helps reduce the complexity and cost of cybersecurity operations.

Prevent:

Implement dedicated security for Industrial Control (IC) and SCADA

Many IC/SCADA systems were not designed with security in mind, and no longer receive software patches for vulnerabilities. Malware that targets flaws in SCADA software can result in unplanned shutdowns, and spread through the network, even affecting connected third-parties. Therefore, manufacturers must include dedicated cyber protection for SCADA systems in their security architecture.

Detect:

Employ advanced prevention techniques

An effective security architecture mitigates threats before they enter the manufacturing environment. These elements include threat prevention employing massive threat intelligence to defend against both known, signature-based attacks as well as advanced techniques such as behavioral analysis, chip-level prevention, and artificial intelligence to help stop today’s unknown and polymorphic threats.

Conclusion

In today's complex world of manufacturing, industrial control systems, operational technology, and IT networks are increasingly interconnected. While digital transformation and the IIoT offer tremendous competitive advantage, in the face of this massive connectivity, manufacturers must implement proven practices that help to reduce the attack surface for their critical infrastructure. Development and maintenance of a sound cybersecurity approach is an essential part of their success. Each manufacturer has different priorities influencing their cybersecurity upgrade strategy. Some may choose a so-called forklift upgrade, going from legacy point solutions to a fully consolidated security architecture in a short amount of time. Others may choose a phased rollout:

- Immediately addressing the **most pressing security areas** (such as unprotected SCADA systems, cloud deployments, SaaS, or mobile devices)
- Then building out a **unified security architecture** as legacy solution contracts expire

With today's formidable manufacturing cyberattack landscape, security professionals need to consider all options.

AT&T next-generation firewalls, powered by Check Point Software Technologies, offer network and device-level Industrial Control System (ICS) solutions to help you:

- **Provide for the safety of industrial assets and personnel**
- **Help keep critical industrial processes running** with a choice of active or passive enforcement
- **Gain deep visibility into your OT assets and networks,** facilitating asset inventory and anomaly detection
- **Support compliance** with OT cybersecurity regulations
- **Prevent OT-targeted threats** with virtual patching of vulnerable assets, OT-specific threat intelligence and auto-isolation of infected assets

For further information on how AT&T next-generation firewalls, powered by Check Point Software Technologies, help protect your manufacturing environments, please contact your AT&T representative, or visit cybersecurity.att.com/contact.

AT&T Cybersecurity

AT&T Cybersecurity helps reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our Software-as-a-Service (SaaS)-based solutions with advanced technologies (including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™), and our relationship with more than 40 best-of-breed vendors help accelerate your response to cybersecurity threats. Our experienced consultants and Security Operations Center (SOC) analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.