SECURE YOUR EVERYTHING™

MANUFACTURING:
FEELING THE HEAT FROM CYBER ATTACKS

Introduction

The manufacturing sector is under attack on numerous fronts. Uncertain trade policies are creating economic imbalances. Sourcing materials from overseas suppliers is getting more expensive, making it more difficult to sell finished products in key markets. In tight times, it is tempting for organizations to scale back IT budgets, including essential upgrades to cyber security. However, with today's highly destructive cyber attacks, putting cyber security on hold is no longer feasible, and some may consider it reckless.

One recent research report validated the need for manufacturing firms to stay current with their cyber security. Half of the surveyed respondents in manufacturing environments knew of a data breach or cyber attack involving their computer systems or networks over the previous 12 months. Of these, 11% experienced a major intrusion.[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 cyber attacks and data breaches."[2]

As "smart" manufacturing continues to expand across the globe, cyber security risk must become a top priority for manufacturers. The sector is one of the 16 critical infrastructure sectors (CI) underpinning global economies.[3]

In this paper, as your organization's cyber security executive, we will explore what manufacturers need to consider when updating cyber security strategies. We will offer best practices that can help you prevent a wide range of cyber attacks, and keep your systems and operations running smoothly.

---

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

Manufacturing Cyber Attack Landscape

Manufacturers are under continuous fire from criminal hackers who seek 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 seeking to steal manufacturers' 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.[4]

Threat actors invade the manufacturing process by implanting malware in products with embedded processors. Hackers use preloaded malware in these "supply chain attacks" that can include distributed denial of service (DDoS) attacks, illicit cryptocurrency miners, among others. Some studies in fact, cite that destructive malware is on the rise for the industry.[5] Malware which was once deployed by sophisticated nation-state actors is now being used by cybercriminals in destructive attacks.[6]

> "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."[9]

Think twice before cutting back on IT budgets, destructive malware attacks cost multinational companies an average of $239 million, destroying an average of 12,000 machines per company, and requiring an average of 512 hours of work by incident response teams.[7] With 50% of reported cases of destructive malware reported during the first half of 2019 coming from manufacturing firms, it is safe to say that the sector must protect themselves from these costly attacks.[8]

Cyber thieves seek to steal identity and email address information about manufacturers' partners in order to launch phishing and other attacks on these third-party partners. Manufacturers sit in the crossfire of advanced 5th generation cyber attacks. The now legendary WannaCry and NotPetya cyber attacks spread rapidly through multiple vectors to paralyze hundreds of thousands of manufacturing organizations around the world.

---

[4] "Exclusive: U.S. manufacturing group hacked by China as trade talks intensified – sources," by Christopher Bing, Reuters, November 13, 2019
[5] "Cyberattacks against industrial targets have doubled over the last 6 months" by Charlie Osborne, for ZD Net 2019.
[6] "From State-Sponsored Attackers to Common Cybercriminals: Destructive Attacks on the Rise" by Camille Singleton and Charles DeBeck, Security Intelligence, 2019.
[7] Ibid.
[8] "Cyberattacks against industrial targets have doubled over the last 6 months" by Charlie Osborne, for ZD Net 2019.
[9] "Jump starting digital transformation in manufacturing," by Ray Watson, Global Manufacturing, February 8, 2019.

What Makes Manufacturers Ripe for Malicious Attacks?

Manufacturers have been involved in a digital transformation for several decades. This digital 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.[10] Just-in-time (JIT) manufacturing has roots dating back to the 1970's. Electronic Data Interchange (EDI) as well as automatic identification for supply-chain management and logistics, computer numerically controlled (CNC) machining, robotics, as well as IC/SCADA operating software have made the new manufacturing economy (NME) a competitive advantage for those at the leading edge.

However, each new technological innovation comes with vulnerabilities that cyber attackers can exploit. This is especially concerning with the joining of operating technology (OT) such as SCADA software 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."[11]
>
> *— Rob Mesirow, leader of PWC Connected Solutions/IoT practice*

One survey found that 59 percent of companies are willing to "tolerate medium-to-high risk in relation to IoT security."[12] In regards to system life, "IT systems are refreshed, on average, every three to five years, OT systems, by contrast, last 10 to 15 years."[13] Add to this complex environment, the use of insecure smart phones employees use to connect to corporate services and corporate departments processing their workloads off-site using Software as a Service and cloud infrastructures, and you have a manufacturing environment with a growing collection of attack surfaces.

[10] "Global cybersecurity risks in the manufacturing industry" by Norma Krayem for Willis Towers Watson 2019.
[11] "2020: Future of Manufacturing Technology," by Peter Fretty, Industry Week, December 2, 2019
[12] "Controlling security within IIoT," by Satish Gannu, techradar, August 22, 2019
[13] Ibid.

Cyber Security Best Practice for Manufacturers

Typically, established manufacturers have accumulated a patchwork of point solutions to protect their corporate perimeter, secure email, protect Web usage, and safeguard other IT services. Early on, IT Security added solutions from multiple manufacturers thinking the differing security technologies would confound attackers. This thinking has changed. Using disparate solutions that do not share threat data can leave security gaps, especially in SaaS, mobile devices, and virtual environments not secured with standard cyber security systems. In addition, using a large collection of security products that must be monitored individually through several interfaces increases the complexity and workload of the IT and cyber security staff. This, in turn, increases the chances of an organization either missing an attack or being overwhelmed by one.

Consolidated Cyber Security

One answer is to replace point security solutions with a consolidated security architecture. When fully deployed, the architecture approach will protect corporate data centers, cloud and virtual infrastructures, SaaS, mobile-devices and endpoints all-at-once. Unified security architecture shares threat intelligence across all these environments to plug the security gaps point solutions leave open. Additionally, a unified architecture gives cyber security staff complete visibility of all environments through one interface. This makes monitoring alerts straightforward and reduces the complexity and cost of cyber security operations. There are specific features manufacturers should look for in a consolidated security architecture.

Dedicated IC/SCADA Security

Many IC/SCADA systems not designed with security in mind, no longer receive software patches for vulnerabilities. Therefore, it is imperative for manufacturers to include dedicated cyber protection for SCADA systems in their security architecture to prevent unexpected shutdowns and to keep malware that targets flaws in SCADA software from spreading throughout the network and possibly to partners.

Advanced Prevention

Preventing attacks before they enter any of a manufacturer's environments is a critical feature for an effective security architecture. These elements include threat prevention employing massive threat intelligence to stop both known, signature-based attacks as well as advanced techniques such as behavioral analysis, chip-level prevention, and artificial intelligence to stop today's unknown and polymorphic threats.

Conclusion

Each manufacturer has different priorities under today's challenging business conditions that dictate the best way to upgrade cyber security. Some manufacturers may choose a forklift upgrade from legacy point solutions to a fully consolidated security architecture. Others may choose to upgrade their security through a rollout that starts by immediately addressing the most pressing security areas such as unprotected SCADA systems, cloud deployments, SaaS, or mobile-devices; then building out a fully consolidated security architecture as service contracts on legacy solutions come up for renewal. With today's formidable manufacturing cyber attack landscape, security professionals need to consider all options.

For further information on how Check Point Software helps protect manufacturing environments, please contact your local Check Point representative.

A Case in Point

Learn how this manufacturer was able to prevent ransomware, zero-day, and phishing attacks via network, endpoint, and SaaS applications. Click here to read this customer success story.

"What we've been able to secure with Check Point infinity is fantastic. It's the best cyber security architecture and protection I've ever worked with, hands down."

— David Severcool, Manager of IT Infrastructure and Security, Control Southern

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com