WHY IS THE MANUFACTURING SECTOR A TARGET FOR ONLINE CRIMINALS?

CYBERCRIME INDUSTRY SNAPSHOT

Manufacturing

CYBER READY

mailguard

Technological innovation and connectedness: Double-edged sword for manufacturing sector

Fueled by the prevalence of supervisory control and data acquisition, industrial control systems and Internet of Thing (IoT), the industry is constantly exposed to security vulnerabilities through machine and process automation.

Software upgrades and security protocols are more difficult to implement and maintain across a physical network comprised of myriad machine types, as opposed to a virtual environment with homogeneous machines.

Every data connection in a manufacturer's network is susceptible. Cyber criminals are constantly scouting for gateways to exploit. According to an IBM analyst, Imaging Computing Server (ICS) nodes might run on outdated operating systems, as they may not be able to update software without triggering equipment malfunction.

Manufacturers' patents and proprietary processes are coveted on the dark web

Ransoms, IP and consumer data theft are the top cited reasons for cyber breaches. The FBI estimates that US$400 billion of IP is drained from the US every year due to cybercrime targeting manufacturing companies.

Verizon's 2017 Data Breach Investigations Report estimates that 94% of cyber attacks on the manufacturing sector are due to espionage, or nation-state attacks. "When you make stuff, there is always someone else who wants to make it better, or at least cheaper. A great way to make something cheaper is to let someone else pay for all the R&D and then simply steal their intellectual property. With that in mind, it will probably be of no surprise that cyber espionage is by far the most predominant pattern associated with breaches in Manufacturing."

Companies in the manufacturing, resources and utilities sector are often part of a long supply chain. It's a numbers game. There are more exploits in disparate—yet interconnected—networks. Data vulnerabilities are amplified in supply chains due to workforce mobility, particularly with mobile devices and unsecured connections as weak points. As many supply chains sub-contract, company data is being handled by secondary, tertiary, and even fourth-degree entities.

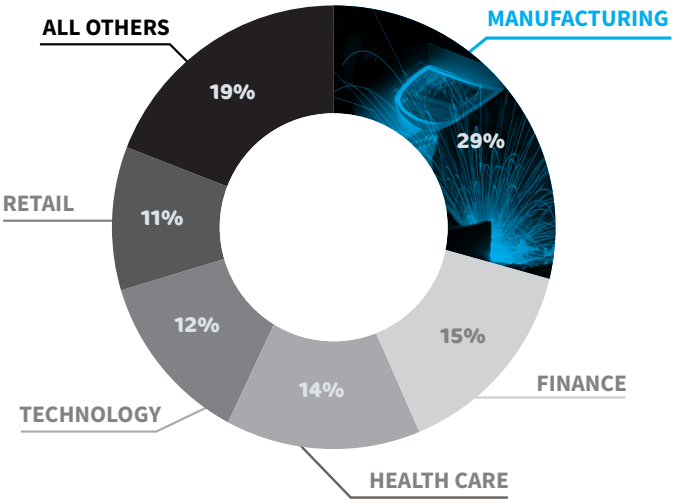
annual revenue of Pharmaceuticals giant Merck

in 2016, a year prior to falling victim to the global NotPetya ransomware outbreak.

lost in misdirected funds in a spear phishing scam

LEONI, one of the world's largest wiring systems and cable technology manufacturers, fell victim to malicous email.

The cybersecurity landscape for the manufacturing sector



PHISHING ATTACKS BY INDUSTRY

Sectors most often impacted by phishing attacks
in 12 months to September 2016

Lack of regulation creates enormous vulnerabilities to cyber attacks

The manufacturing sector is not regulated by compliance standards or legislation, such as in financial services (Payment Card Industry Data Security Standards) or health care (Health Insurance Portability and Accountability Act), resulting in varied cybersecurity mechanisms and safeguards across industry players. This may be the reason why 50% of US manufacturing executives do not feel confident in their cyber-readiness, with 31% of companies having never conducted vulnerability assessments for ICS, according to a Deloitte survey.

Manufacturing—one of the most hacked industry sectors

According to the IBM 2017 Threat Intelligence Index the manufacturing sector is one of the most hacked industries, second only to healthcare. Globally, one third (34%) of all cyber attacks target manufacturers using phishing emails as a common threat. Attacks are scaling exponentially. UK company NTT Security reported that there was a 24% increase in global cyber attacks in Q2 (April-June) 2017 alone.

The three most common attack types on the sector are: reconnaissance (33%), brute-force (22%) and regular malware (9%). We can assume criminals have not only financial motivations but deeper and more devastating intentions such as operational, reputational and physical harm on a mass scale.

MailGuard reporting on recent phishing scams

Cybercriminals impersonate brands that are household names and have large customer bases. The brand recognition, coupled with curiosity or fear, impel unwary recipients to click through to phishing sites, or inadvertently download executable malware. MailGuard has reported email scams purporting to be from government agencies (ATO, the High Court), popular online subscription or free services (Apple, Netflix, Dropbox, Office 365), delivery services (Australia Post, UPS, DHL) and telco / utilities (Telstra, Origin Energy).

Scams bank on human psychology to respond (e.g. tax evasion, traffic infringements, court order, unauthorised account login attempts, overdue bill), reinforced by sophisticated, well-crafted emails and phishing sites (often indiscernible from the mimicked sites). Unfortunately, these campaigns are effective, with 7.3% of targeted recipients successfully phished. The market value of PII on the dark web ranges from USD2,000 for a passport to USD1,065 for a medical record and up to USD400 for a diploma, so a successful phishing campaign can be a boon for cybercriminals.

Manufacturing testimonials

"Email is vital to our success. It provides a simple, cost-effective solution for communicating with drilling teams in remote areas… (MailGuard's) daily reports show all quarantined emails and make it easy to identify any legitimate emails which need to be released… Monthly reports from MailGuard provide valuable traffic statistics and allow our management to pinpoint any issues which may arise."

—Network Administor, Tap Oil

"We recently moved to Office 365 and found their spam filtering (was) not good enough. So, we decided to have MailGuard as an additional layer of security for our emails. MailGuard has solved our Spam problem. The product is solid and their support has been exceptional."

—Systems Administrator, Pilot Pen

GET CYBERREADY WITH MAILGUARD

We identify and stop fast-breaking attacks in real-time, 2-48 hours ahead of the market

Contact your IT service provider now for an obligation-free, 14-day trial

PHONE 1300 30 44 30
EMAIL expert@mailguard.com.au
WEB mailguard.com.au

CYBER READY

mailguard