CYREN

10 Steps to Protect Your Manufacturing Business

Solution Brief

Manufacturing businesses of all sizes have become a top target for phishing

Phishing attacks are occuring with greater frequency in the manufacturing industry. According to the 2018 Verizon Data Breach Report, 93% of all breaches of corporate systems begin with some form of phishing, and – true to form – most breaches in the manufacturing industry begin with a well-crafted spear phishing email, containing a malicious link or attachment sent to a company employee

Manufacturing Industry Dynamics Attracting Cyberthreats

Why are manufacturers being targeted, even more than other industries? Among the reasons are:

Manufacturers possess more valuable information than they realize – Even the smallest manufacturing companies have information a criminal can use or sell. Sensitive employee information, such as social security numbers and salary data can garner a criminal thousands of dollars through false tax filings or resale on the dark web. Customer email addresses and login information to supply chain systems are highly sought after. Business plans, intellectual property, and trade secrets are also desireable, since an easy way to produce something less expensively is to let another manufacturer pay for the cost of research and development. Foreign or domestic competitors may use their own cybercriminals to target a manufacturer specifically to steal and leverage their intellectual property – or an independent hacker may target the business simply to make money by reselling the secrets on the dark web. Notably, the highest level of cyber espionage occurs in the manufacturing sector, and most cases begin with a phishing attack.

A high degree of "interconnectedness" – Manufacturing supply chains are connected, integrated, and interdependent. According to research firm Forrester, more than 60% of manufacturing companies grant high-level access to their SCADA/ICS systems to other companies in their supply chain, including outsourced suppliers, business partners, and government agencies. Since protecting the entire supply chain depends on security at every point, including at the small supplier or local factory level, cybercriminals know that in order to access a high-profile target, they simply need to breach the weakest link among any company's suppliers, partners and customers.

Small firms underestimate risk – According to the U.S. Bureau of Labor Statistics, the vast majority of manufacturing companies are small. The 2018 Verizon study reports that small businesses are far more likely to be the target of cyberattacks, with small businesses attacked 58% of the time. Hackers believe smaller firms are less protected.

A Tale of Two Phishing Attacks

Manufacturing employees lose thousands in cybercriminal tax fraud.

In 2016, Seagate Technologies, a manufacturer of precision-engineered data storage technology, became the target of a high-profile phishing attack, when an HR employee responded to a business email compromise scam. Thinking the email was from the CEO, the employee sent hackers highly personal staff information, including social security numbers and salary data for not only 10,000 current and past employees, but also their spouses. Within days of the attack, criminals were filing fraudulent federal and state tax returns for both employees and family members.

Supply chain breach at small HVAC vendor leads to loss of data on 40 million credit & debit cards.

The infamous Target breach – in which 40 million credit and debit cards, and email and mailing addresses for 70 to 110 million people were hacked and compromised – began with single employee at a regional HVAC company opening an email attachment containing phishing malware that captured various system passwords, including those for partners and customers in the supply chain – one of whom was the Target Corporation. The hackers were then able to gain access into Target's systems to steal highly sensitive customer data. This breach ended up costing Target $202 million dollars.

25B
Security Transactions Daily

1.3B
Users Protected

300M
Threats Blocked Daily

10 Steps to Protect Your Manufacturing Business

Solution Brief

Unprotected and unsupported operational technologies – Operational technologies (OT) and control systems like SCADA are increasingly connected to the internet and other corporate systems. Yet many are still running unsupported operating systems, like Windows 95, creating a scenario that makes the entire corporate network vulnerable to attack. Patching vulnerabilities is the first key line of defense. However, today most threats appear quicker than IT or production staff can patch. Further, some operating systems are currently running on unsupported OT, so patching simply isn't an option. A successful cyber attack against OT or a SCADA control system could do significant financial and physical damage to a manufacturing business.

The Business Impacts of a Breach

Data theft – Phishing attacks use spoofed email messages and copycat websites that look legitimate to trick users into sharing valuable information, such as employee data (social security numbers or salary data), customer contact data (email addresses or phone numbers), intellectual property (business plans or trade secrets), financial account information (bank account numbers or transaction data).

Financial fraud – Business email compromise attacks and impostor emails may attempt to divert money to criminally-controlled accounts. Lost revenue can also result in reputation damage and lost customers.

Reputation and loss of business – Manufacturing businesses risk major reputation damage and loss of clients and future business if their company is phished and money or data stolen.

Business interruption – Manufacturing businesses are driven by fixed production and delivery dates to ensure profitability and customer satisfaction. It only takes one phishing or malware attack to have a detrimental effect on an entire production cycle, leading to financial consequences.

What you can do to protect your company, business partners, and customers

1. **Deploy cloud-based email gateway protection from a security provider.** Cloud-based secure email gateways add more advanced security like time-of-click URL analysis and protection from business email compromise.
2. **Deploy a web security gateway.** An effective web security gateway will stop new and zero-day malware downloads, attempts to access malicious URLs, and communications with botnet C&C servers.
3. **Deploy endpoint security with active/behavioral monitoring.** Malware and ransomware evolve quickly and you need to augment traditional AV with next-generation detection.
4. **Employ a defense-in-depth strategy.** A defense-in-depth security approach is recommended by the International Electrotechnical Commission (IEC), the National Institute of Standards and Technology (NIST), and the Department of Homeland Security (DHS). Augment traditional security technologies with next generation detection, including cloud-based web and email gateways and endpoint security.
5. **Use a password management tool and multi-factor authentication.** Password re-use makes phishing attractive for criminals. A breach into one system containing user names and passwords will likely be exploited to access other systems.
6. **Protect against evasive threats with sandboxing.** Today's malware developers are incorporating many different tactics to evade detection by traditional technologies. A cloud sandbox array is a new capability that can sit in-line with an email security gateway to protect from today's evasive malware.
7. **Patch early, patch often.** Outdated operating systems, browsers, and plugins are major vectors for malware infections and breach points into other connected systems.
8. **Create off-site back-ups of important data.** Should a phishing, malware, or ransomware attack happen, off-site back ups can speed up the data recovery process.
9. **Turn off network shares and unnecessary admin rights.** Current malware exploits sharing vulnerabilities and seeks out mapped network drives.
10. **Train users.** Educate users about the social engineering tricks that are used.

Consult us about Cyren's security services:

Email Security | Web Security | Cloud Sandboxing | DNS Security

www.Cyren.com

sales@cyren.com