CAMA
Colorado Advanced Manufacturing Alliance
BEST PRACTICES

Best Practices - Staying One Step Ahead: Cyber Security for Manufacturers

By Dan Domagala and Gabriel Cineros

EKS&H

EKS&H
AUDIT | TAX | CONSULTING

Cyber-attacks on manufacturing companies are on the rise. In a report released in early 2016, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team documented 97 attacks against the manufacturing sector during fiscal year 2015. This figure represents a concerning near doubling of the number of attacks in 2014, while incidents across all sectors only increased by 20%.

Another reason manufacturers should be concerned is that attacks are becoming more sophisticated in targeting mid-size businesses. For example, hackers are now frequently using a practice known as "spear-phishing," which involves email messages that appear to be from the business owner or CFO sent to others within the company requesting wire transfers or payment distributions.

Manufacturers must understand these new types of attacks and develop appropriate solutions to prevent and respond to them.

Intellectual Property Theft

Challenge: Proprietary information stolen in a cyber-attack could be used to reengineer a company's unique products. Intellectual property (IP) theft might originate from domestic competitors or international attackers. As an alternative to the outright stealing of information, attackers may also gain access to a manufacturing company's computer network and alter its books to cause inaccuracies or confusion. This type of "disruptive" attack is also becoming more common.

Solution: Companies need to look at more advanced defense strategies beyond simple firewalls or antivirus software. Additional security might include a next-generation firewall or network monitoring software (such as Nagios) to provide the business insight into what's happening within its network at all times. In addition to traditional monitoring, analytic solutions (such as Arbor Networks® Spectrum or ProtectWise) record and examine traffic on your network to identify risks sooner.

Attacks on Business Networks

Challenge: Attackers might gain access through a company's distributor or supply networks. These networks are often an integral part of the daily operations of manufacturers, which makes them especially prone to this type of attack. (One trick is for cyber criminals to pose as vendors requesting payment in another type of spear-phishing attempt.)

Solution: To deal with this challenge, vendor management is key. Companies should institute, and *always* implement, technology and accounting security measures. Manufacturers should know their vendors well and make sure they communicate and enforce internal security standards.

Another best practice is to restrict unnecessary business-to-business connections whenever possible. Use an application program interface (API) to transfer data at the application level rather than a traditional virtual private network (VPN).

Human Error

Challenge: Cyber criminals attack at all levels of an organization, from the CEO and down, to gain access to proprietary information. Therefore, *every* employee should know he or she is responsible for maintaining company security. The risk of human error becomes greater when deadlines are involved. In the attempt to bring in raw materials or send out inventory more quickly, employees may fail to take established precautions or bypass security protocols. Examples include sending payments to unknown accounts or setting up unsecured data exchanges.

Solution: Cybersecurity initiatives should be instituted company wide. Two-factor authentication, which requires the use of encryption *and* identity verification for access to information, can help decrease errors. In manufacturing, it's not always obvious what information needs to be protected where, so employee training is key to ensuring appropriate security policies.

When it comes to vendor or supplier payment employees should never bypass normal processes. However, fulfilling orders or providing service sometimes requires customer service over process. In those cases, verifying identity before going to extraordinary measures is the best advice.

Outdated Operating Systems

Challenge: Manufacturing companies often use machines and equipment operated by computers. If those systems are running outdated operating systems (OS) (such as Windows 98, which is no longer supported by Microsoft), they become vulnerable to attack because software providers no longer create security patches for them.

Solution: The ideal solution is to implement a large-scale update of the OS used in primary segments of the company. However, the cost of upgrading the OS can be prohibitive. In these situations, updates can be done selectively to address specific machines and processes. However, inconsistencies in products could result from having different OS running equipment. An alternative might be simply isolating the equipment from the rest of the network to reduce the risk. Many factors need to be considered in determining an appropriate solution, but remember that not upgrading an OS could end up being more costly than doing so.

Misuse of Information Broadcast by Equipment

Challenge: Manufacturing equipment can have its own computer, processing unit, or radio frequency identification. These types of machines, known collectively as the Internet of Things (IoT), sometimes communicate over open networks and broadcast information that could be damaging if intercepted. In addition, products developed by manufacturers for home use, such as surveillance systems, thermostats, and entertainment systems, could also communicate sensitive information.

Solution: Manufacturers need to be mindful of "data in motion" passing from the IoT to the company's network. Once a company determines its vulnerabilities, information should be encrypted as needed. It can be helpful to maintain an inventory of what comes in, what is developed, and the communication security capabilities of each item.

Failure to Implement Regulatory Requirements

Challenge: Some manufacturing companies, particularly those in defense/military and health/medical, may have requirements specifying the type of cyber protections they must follow. These companies may be at greater risk of attack if they overlook, or are unaware of, these specific requirements.

Solution: Manufacturing companies should understand the expectations of government and regulatory bodies and apply the associated best practices, such as installing a certain type of firewall. They should be prepared for random checks by monitoring agencies. International companies may have to follow regulations from multiple countries, which could vary significantly. Consulting an expert can help a company stay up to date on the latest rule changes.

While prevention of attack is certainly preferable, it is also critical for manufacturers to have a plan for continuity of operations if one occurs. Will everything shut down? Will operations continue as usual? Can the incident be isolated from the rest of the company? Manufacturers should create an explicit written plan for what will happen in the event of an attack.

In addition, manufacturers should take stock of all assets and prioritize protection. Assets include both tangible (e.g., financial information and physical products) and intangible (e.g., product designs; software code/firmware; and supplier, customer, and employer information).

Unfortunately, some consequences of a cyber-attack might not be “fixable” no matter what plan is in place, but it’s important to address what can be controlled. Cyber insurance is an option but will not necessarily cover every contingency. Damage control for company reputation should be a component in any post-attack plan.

Conclusion

With the rapid rise of cyber-attacks, manufacturing companies should devote serious time and effort to creating a detailed plan to prevent attacks from occurring as well as determine what to do if one occurs. Having a prevention and response plan in place is the best way for companies to protect themselves from these modern threats to manufacturing.

EKS&H helps manufacturers with a range of issues, including accounting, tax and audit, technology, and talent. We have more than 300 Colorado-based manufacturing clients and partner with many industry organizations, including the Colorado Advanced Manufacturing Alliance, the Colorado Association of Commerce & Industry, and the National Association of Manufacturers.

To learn more about cybersecurity for manufacturing companies, please contact Business Technology Senior Manager Dan Domagala at ddomagala@eksh.com or Manufacturing Audit Partner Kreg Brown at kbrown@eksh.com, or call us today at 303-740-9400.