Boxmakers Beware

aiccboxscore.org/2023/03/boxmakers-beware/

M. Diane McCormick March 20, 2023

Boxmakers know boxmaking, not cybersecurity. “You may be an expert in manufacturing, but you probably are not an expert in computer networks,” says Ronald Menold, Ph.D., director of cybersecurity services at COSECURE.
And yet, Menold and industry insiders agree: Cybersecurity is essential to preserving that manufacturing business. Today’s manufacturing is highly vulnerable to cyberattacks that can halt operations, cost huge sums of money, compromise the privacy of employees and partners, or even wipe out the business.

It’s time to prioritize cybersecurity and take the basic steps needed to update systems and policies to prevent cyberattacks before they do their damage.

Tempting Target

In the lingo of cybersecurity, manufacturers offer a “high surface area” for hackers of all types. Their systems house a wealth of information malicious actors can exploit. Hackers might conduct a “drive-by” attack, swooping in when they find a breach, or they could pose an “advanced persistent threat,” waging a constant assault, trying to break in for a purpose.

Manufacturing is vulnerable on multiple fronts. Defunct operating systems—even a computer in shipping running perfectly fine on Windows 7—are no longer automatically updated. A slipup by a connected vendor can crack open the door, like the heating, ventilation, and air conditioning vendor phished into sharing passwords that caused the infamous Target breach of 2013. Operating systems storehouse Social Security numbers, intellectual property, and trade secrets. And of course, they conduct huge financial transactions daily.

Hackers want payouts through ransomware attacks that hold data hostage. They can interrupt service for ransom or competitive advantage. They might want to undermine a rival nation's security by tapping into critical industries. Or they can steal intellectual property for another business to use—without the upfront investment the victim company put into it.

Forget the stereotype of the hoodie- wearing, basement-dwelling hacker, says Menold. Today's hackers sit in cubicles, working 9 to 5. By earning commissions, they are incentivized to "get your money because they get a cut of it," he says.

The Human Element

Business email compromise is the most common form of hacking, constituting 80% of incidents, says Menold. Human error is its driving force when employees are clicking on a compromised link and sharing sensitive information, or visiting infected websites, all of which can set off a chain reaction of cyber compromise.

Once in, hackers often angle their way to the people who control the company's money. With that, they gain access to hundreds of email chains regarding financial matters. By simply duplicating the emails but subtly altering an address—".co" instead of ".com," or substituting a number "1" with a letter "l"—hackers can look like legitimate vendors. They might share the news that they have changed banks to dupe the unsuspecting recipient into sharing electronic fund transfer information or depositing bill payments into a fraudulent account.

"This happens again and again and again to the tune of hundreds of thousands of dollars to millions of dollars per incident," says Menold. "It's instant gratification for hackers because a wire transfer is pretty much immediate and nonretractable after 24 hours. You may be wiring to a U.S. bank, but then it's immediately rewired to a non-U.S. bank."

A business can also be exploited as the vehicle for hackers to spoof other companies. The hacker can seize documents or even find them floating in cyberspace and then send identical versions that dupe the recipient into transferring money or sharing sensitive information. Although such incidents don't always involve or interrupt the company whose documents are spoofed, they can erode trust among partners.

"We have tightened up our controls, especially in finance, because they are very susceptible to these cybercriminals," says Terri-Lynn Levesque, vice president of administration at Royal Containers. "Spoofing is probably one of the hardest to catch, unless you're really diligent. Trust is broken so quickly without you even knowing, until it's too late."

Creating a Cybersecurity Culture

While humans cause most cybersecurity incidents, they are also “the first line of defense,” notes Levesque. “If we become very blasé and lackadaisical about it, that’s when we become very vulnerable,” says Levesque, who serves on the board of AICC and AICC Canada. “Any staff who has a company email address has a key to our cyber front door.”

At Pratt Industries, employees are trained to report any missteps immediately—no consequences—says Juan Merelo, technical services manager. Employees are told, “If you see something, say something.”

“Ninety-nine percent of the time, it’s nothing, but our motto is ‘The bad guys only need to be right once. We have to be right 100% of the time,’” says Merelo.

When a breach is in the news, Merelo’s team creates a teachable moment. They craft the incident in plain language and show how employees’ ties to the hacked entity, such as a social media account or a retailer’s credit card, make their employer vulnerable. “It’s always trying to adapt what is going on to things they can apply in their current day-to-day lives,” says Merelo. “We can provide the perfect playbook, but we are at the mercy of our weakest user.”

At Liberty Diversified International, Chief Information Officer Alla Johnson finds seasonal opportunities to put cybersecurity messaging in a relevant framework, perhaps warning of a fake package delivery message around the holidays. There are several logical times of the year to work in cybersecurity messaging, in addition to regular quarterly trainings and practice phishing campaigns, she says.

Menold warns of a tension between information technology (IT) and cybersecurity. While chief information officers (CIOs) want to keep the network open, chief information security officers (CISOs) are prepared to shut down all or part of the system when needed.

Like many others in manufacturing, Merelo wears both hats but knows when to prioritize cybersecurity. When Pratt Industries opens a new plant, he insists that engineering justify every open system, “and if it doesn’t make sense, it will not be open.”

In her dual role as CIO and CISO responsible for technology and cybersecurity, Johnson leads constructive dialogue among all stakeholders, focusing their solutions on what’s best for the business.

“Most of the time, you can come to a reasonable agreement on what is best for the business and what is best for security,” she says. “Communication is really the key.”

Leadership at the top plays a critical role in creating a culture of awareness and vigilance, adds Johnson, who encourages cybersecurity messages from the CEO, chief financial officer, and top executives of Liberty Diversified's different businesses.

How to Protect

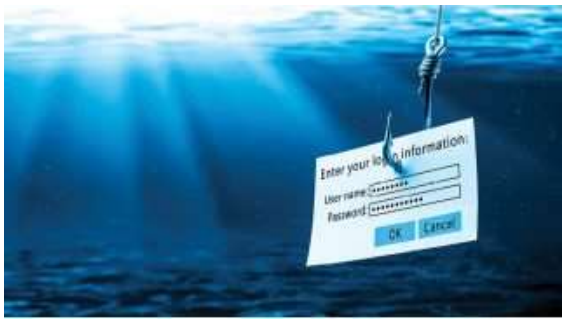
Like fighting fire with fire, keeping hackers at bay requires fighting persistence with persistence. Cybersafety demands consistent application of basic precautions.

Train Employees

Many manufacturers mandate regular training, especially among credentialed employees who send and receive email. Shift schedules and union rules can make it challenging to include factory workers, but it's essential because they touch computer systems, too, notes Menold. Training can address how to spot fakes and why passwords must be revised regularly and never shared.

Send Phishing Tests

Cybersecurity contractors can send regular tests, mimicking messages meant to hack into company systems. Employees who click the links can be referred for extra training, but as Levesque notes, they should not be shamed, rather they should be educated on weeding out the fakes from their genuine emails and texts.



Update or Isolate Operating Systems

The best way to protect production equipment is to isolate it or keep it free of vulnerabilities, says Johnson. Newer robotics equipped with an up-to-date operating system, firmware, and other software are not immediately vulnerable, but they still require continuous monitoring because "they're 12 to 24 months away from being vulnerable," she says.

Any out-of-date operating systems should be updated or, at the least, monitored and isolated from the rest of the network. If isolation is the chosen path, it's important to keep in mind that they remain unprotected, she adds.

Separate IT From OT

Easier said than done at older facilities, but keeping IT apart from operating technology (OT) plants a firewall between the back office and the factory floor. When Pratt Industries' manufacturing equipment must be physically accessed for support or troubleshooting, Merelo's team will create temporary access and carefully monitor the work, denying access if the operator takes any steps outside a strict, predetermined set of allowable actions.

Monitor Alerts and Patches

The U.S. Cybersecurity and Infrastructure Security Agency issues daily bulletins on emerging vulnerabilities and hackers' latest tactics. Security officers must compare such alerts with the status of their own systems, sealing any vulnerabilities. In the case of "zero-hour threats" about vulnerabilities for which there is no solution, Merelo determines if Pratt can live without that supply and, if possible, sever the connection until a solution is found.

And don't assume you can obtain security patches from equipment vendors for any given vulnerability, says Johnson. "They often don't have patches available, or their patches may introduce different problems. If one is available, it needs to be tested thoroughly to ensure there are no interruptions to the business process. From time to time, they have to be reversed, so it's important to have a good back-out plan," she says.

Automate Threat Detection

Your company's security team can't be there 24/7, but managed detection and response (MDR) services can be, applying advanced analytics and threat intelligence to blanket manufacturers in protections. As Johnson explains, an MDR vendor can run millions of transactions through a "secret sauce algorithm" to review transactions, produce alerts, and warn clients of vulnerabilities and unusual behavior.

Involve Tech in Strategic Planning

Good fixed-asset planning and budgeting practices can ward off obsolescence without the need for sudden, significant capital investments. "We're starting to get into a cadence where we plan for these things instead of being surprised by them," says Johnson.

Conduct Cyber Audits

As manufacturers grow, they invest in industrial control systems and expand their networks. Such sophisticated operations could merit a cyber audit by a consultant with expertise in spotting vulnerabilities. Johnson advises companies to conduct regular audits against "a known and trustworthy cybersecurity framework," such as the National Institute of Standards and Technology, paired with regular assessments from outside parties probing for

weaknesses and checking the overall hygiene of the work environment and secure user credentials. Smaller companies might not have room in the budget for third-party audits, but they can conduct internal audits and harden their vulnerabilities, Menold says, perhaps discovering that more employees than necessary are accessing portions of the system.

Limit Vendor Access

For vendors with access to your system, “you want to make sure that their cybersecurity posture is at least to your level,” says Menold. Johnson’s Liberty Diversified uses a rigorous process to limit access to strict need, and anyone with access gets a username and password with multifactor authentication, just like an employee. Those accounts are audited annually. If an outside party needs access to solve a problem, they can access systems with the proper authentication. “While we prefer our systems not to be internet-facing, the reality of running a business is such that we must come up with reasonable controls, which allow our factories to run smoothly and efficiently,” says Johnson.

Create a Response Plan

A plan for responding to incidents and containing the damage indicates a maturity level that earns plaudits from Menold. But few companies follow through by testing them, in which case “it can be kind of useless,” he says. Plans should be reviewed at least yearly and tested via field or tabletop exercises. In particular, the plan’s communication elements should be kept up to date. Who declares an emergency? Are the physical and cyber spaces referenced still part of the organization? Are positions referenced by title or by name (that’s a no-no), and do those positions still exist? Levesque updates her company’s plan frequently, and she keeps a paper copy on her desk and a copy on her cellphone for access to critical phone numbers in case the system is down. Johnson and her team review segments throughout the year, devising scenarios to test the readiness of the plan’s key sections.

Back Up Data

For rapid recovery in case of an attack, always have backup data in off-site locations and in the cloud.

Refer to A Starter Road Map

For companies that need to create a cybersecurity strategy, Menold offers a tip. Insurers have developed complex questionnaires to test the suitability of policyholders for cybersecurity insurance. Get a copy and review the questions (for example, “Do you require

all of your employees to complete a security training course? What about all your contractors?"), and you have a road map to a basic cybersecurity program.

To Levesque, cybersecurity comes down to due diligence. She and her IT team create an annual checklist to keep hardware and systems up to date, but they also remain vigilant each and every day. "Our department will grow as we get bigger," she says. "It has to. We have to remain diligent on keeping everyone educated as the cyber world changes and evolves daily. Preparing for the worst-case scenario is our only option."

Diane McCormick *is a freelance journalist based in Pennsylvania.*