The Urgent Cyber Threat To U.S. Manufacturers

A PRACTICAL INSIGHTS GUIDE FROM HUNTINGTON

Manufacturing companies are some of the biggest targets for cyberattacks. The events that grab headlines are the spectacular ones, like the 48-hour shutdown of Honda's Sayama plant in Japan during 2017. But being a smaller target affords little protection. The viral nature of cybercrime technology means it's fast and easy to mount thousands of attacks. Cyberthieves are eager to find companies with weak defenses—which are often those with small or overworked security staffs.

25%

of manufacturing executives surveyed said lack of trained personnel is a major obstacle to adopting advanced security processes and technology[1].

What they're after varies. It may be money, through a ransomware attack that paralyzes your systems until you hand over funds to restore control. Or, it may be an attempt to steal intellectual property (IP)—like your unique manufacturing process. It may be data, such as confidential customer, employee or vendor information. Or, it may simply be an attack out of malice—digital vandalism that uses malware to destroy or disrupt your systems.

As the 2018 IBM X-Force Threat Intelligence Index found, manufacturing was the second most attacked sector, behind information and communications technology[2]. In one 2017 Cisco Systems survey, more than a quarter of surveyed U.S. manufacturers reported lost revenue from cyberattacks in the previous year[3].

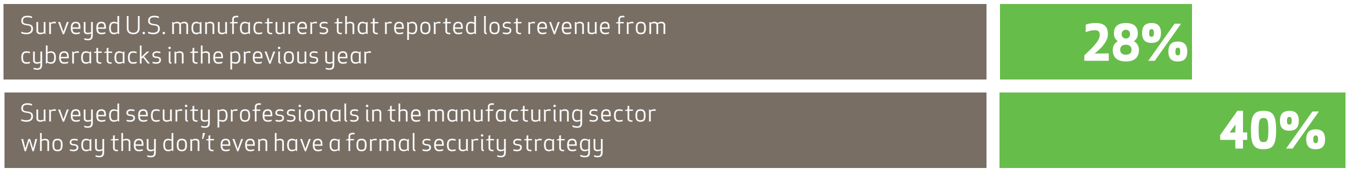
IN THIS REPORT:

5 KEY STRATEGIES FOR HELPING TO REDUCE CYBER-SECURITY RISK

1. Determine what you are trying to protect.
2. Conduct a detailed cyber risk assessment.
3. Initiate regular cyber awareness training.
4. Protect and segment your networks.
5. Develop a response and recovery plan.

Despite this alarming trend, Cisco reported that 40% of surveyed security professionals in the manufacturing sector say they don't even have a formal security strategy[4].

Many manufacturers are aware of the problem, however.



Don Boian, chief information security officer at The Huntington National Bank, says he sees many small to mid-sized manufacturers moving past the "denial" phase and into the "acceptance" phase, where they're ready to take a more methodical approach to security.

FRAMING THE DISCUSSION.

It's time to think of cybersecurity as the new plant safety challenge. Just as manufacturers have developed a robust physical safety culture over the past 30 to 40 years, they now have to build the same kind of awareness and protocols around cybersecurity.

"We're trained in factory environments not to step across the yellow line," says Marty Edwards, managing director of the Automation Federation. "We need to start thinking about a thumb drive being stuck into a computer as a safety violation."

Eugene Spafford, executive director emeritus of the Purdue Center for Education and Research in Information Assurance and Security in West Lafayette, IN, agrees.

"The rule of thumb for anybody managing a business is to assume that their systems have been penetrated," says Spafford. "Especially when it comes to the protection of IP, a lot of organizations don't think about security. Today, security must be a part of the original design."

Manufacturing has unique vulnerabilities, particularly around technology that operates plant equipment. Separating the networks for information technology (IT) and operational technology (OT), such as machine control boards, becomes more difficult as modern equipment comes into plants and the Internet of Things (IoT) evolution takes hold. Managing these more complex networks in the age of IoT makes security a daunting task, particularly for companies that don't have staff dedicated to it.

To help kickstart a more proactive approach to security, we developed this guide—a checklist outlining five basic steps to understanding and reducing risk—for manufacturers like you.

48%

of cyberattacks on small to mid-sized companies surveyed were initiated by phishing attempts or other attacks on employees[5].

$120k

Estimated average cost of a targeted attack on a small or medium business[6].

1 Determine what you are trying to protect.

Nothing brings a threat into focus like considering what you have to lose. Begin by identifying your company's crown jewels—perhaps a manufacturing method, or a hard-won relationship with a customer who relies on components that you supply.

"If it takes you three weeks to restore your operation, what's three weeks worth of sales going to cost you?" asks Marty Edwards of the Automation Federation. "Based on those numbers, you have to look at how much you want to invest in cybersecurity to bring the risk of that occurring down to an acceptable level."

One sobering statistic: Kaspersky Lab estimates that the average cost of a targeted attack on a small or medium business is $120,000[6].

In addition to the immediate cost of a shutdown there is the price of remediation, workforce disruption and harm to your reputation. Also there could be additional costs if you don't have data properly backed up, and a response and recovery plan in place. Then there could also be the cost of new security technology and practices that, if you'd invested in them earlier, might have prevented or minimized the attack in the first place.

While many manufacturers have someone on staff responsible for tech, they don't always take the time to fully evaluate the cost of a potential cyberattack. Once you've seen what an attack could cost your organization, it'll be easier to justify the investment in the next preventative steps, including hiring a consultant to investigate your vulnerabilities, training staff in cyber awareness, and segmenting your IT and OT networks.

2 Conduct a detailed cyber risk assessment.

Because most mid-sized manufacturers often lack dedicated cybersecurity staff or budget, it's important to prioritize which threats to tackle first so you get the most bang for your buck.

$155

average four-year cost per stolen record from a data breach in the industrial sector[7].

Collecting a detailed and actionable understanding of your vulnerabilities is typically the work of an IT security consultant, who will do things like scan your external facing connections to check for malware and other attacks, review your system configurations and look for any software flaws. The consultant will then give you a report and help you develop strategies to patch your systems and watch for network vulnerabilities like unused network ports exposed to intruders. In some cases, you may hire the same consulting company to do routine follow-up checks of the network, or to train your internal IT team to do the updates and monitor work.

For a small or mid-sized manufacturer, this kind of assessment and a follow-up plan should cost about $15,000. If that seems costly, remember that a typical attack can cost more than $100,000[6].

When searching for a consultant, executives need to understand the level of complexity their company can handle, and have the consultant offer a program that will work for their company's sophistication and resources. For example, says Rob Westervelt, a research director within the Security Products group at International Data Corporation, if you're not technically savvy, you don't want to get a huge detailed report on every single software vulnerability in your environment. For many, the crucial component will be guidance on where to begin.

QUESTIONS TO ASK YOUR CYBERSECURITY CONSULTANT:

□ What are the highest-risk parts of my environment?

□ What are the most cost-effective ways to invest in security?

□ How much should I spend on security equipment and staff to mitigate my biggest risks?

□ Can you offer a program that is tailored to my company's level of sohpistication and resources?

Some questions executives should pose to the consultant include: What are the highest-risk parts of my environment? What are the most cost-effective ways to invest in security? How much should I spend on security equipment and staff to mitigate my biggest risks?

3 Initiate regular cyber awareness training.

The human component is critical in cyberattack prevention, and companies of all sizes will benefit from staff training. In fact, according to the Ponemon Institute, the single biggest cause of data breaches is negligent employees or contractors[8].

Training often includes a class on how to spot suspicious phishing emails as well as a review of basic cyber hygiene, such as password management, and teaching staff which kinds of devices they can connect to the network. For people who work remotely, changing the default password on their home Wi-Fi router is the sort of detail easily overlooked. Staff also must learn to see unauthorized thumb drives as a source of risk.

“Someone can plug a USB drive into a computer or machine and infect the plant. It could be that someone’s kid is a gamer, and they picked up a virus on the drive,” says John Nicholas, a professor and the program director for Cybersecurity and Digital Forensics at the University of Akron. “It’s a matter of practicing continuous cyber hygiene.”

20%

of publicly recorded security incidents in 2017 were caused by employee error and mishandling of technology[9].

Chuck Peirano, chief fraud and security officer at Huntington, says manufacturers also have to set clear policies about office use of social media, because Facebook, Twitter and the like can be entry points for hackers. Companies should also decide whether or not they let workers send emails from home to work or work to home.

“You may have a great system inside, but someone can introduce malware from their home PC… so that’s another way of bringing problems into the company,” Peirano says.

Peirano adds that even the HR department needs to get up to speed on risk, and take steps like scanning or quarantining incoming PDF or Word resumes.

Racine Metal-Fab, a 60-employee precision sheet metal and fabrication service company based in Wisconsin, hired a consultant to do a security assessment a couple of years ago. As part of the exercise, the consultant phished the company’s employees with fake emails, then used the results in a follow-up presentation.

PERSPECTIVE

> ***“Most importantly, response plans need to be tested and practiced. The first time you run the response, it will not go smoothly. You want to discover any hiccups long before a real incident.”***
>
> *—Marty Edwards, managing director of the Automation Federation*

Surprised employees learned how many of them had not only been fooled, but had actually offered up usernames and passwords to the might-have-been cyberthieves.

Dean Popek, CFO of Racine Metal-Fab, who also serves as the IT manager, says the company now runs a phishing exercise once a year, followed by a brief review.

Building a cybersecurity culture takes a commitment from top management, and mutual understanding that employees are the first line of defense. Nothing happens unless the staff takes ownership of cybersecurity. It’s management’s job to reinforce and update the training and keep security awareness top-of-mind.

"The other thing I do," Popek says, "is any time I read an article about security… I'll send it out to everybody in the company and just say, 'Hey, folks, here's a reminder about the risks out there today.'"

DOS

- Do start thinking about cyber safety with the same attention you give to plant safety.
- Do conduct a thorough risk assessment to figure out the real cost of a cyber incident.
- Do consider hiring a cybersecurity consultant to prioritize your vulnerabilities.
- Do create a cyber training plan for all employees.
- Do take steps to help protect your OT just as you do your IT, with firewalls and controlled network access.

DON'TS

- Don't ignore your IP or client IP in your risk assessment.
- Don't overestimate your company's resources and sophistication in creating a cyber protection plan.
- Don't forget about departments like HR in your cyber training and policies.
- Don't assume your manufacturing equipment has the latest patches and updates.
- Don't wait until you've had an incident to test your response plan.

4 Protect and segment your networks.

Smaller manufacturers are at an important technology crossroads. As they replace old equipment with new machines that are connected to the Internet—now that manufacturing is well into the IoT era—and as more pumps, valves, hand tools and even helmets come with wireless radios, it's increasingly difficult to separate the IT and OT networks.

For years, manufacturers created what became known as an "air gap" between IT and OT, where the systems were on physically separate networks. (In truth, it was never a foolproof strategy: All it took was inserting a thumb drive with bad code for the gap to be jumped.) As these new, networked equipment and IoT products come into the plant, often joining the company's IT networks, they introduce a cyber vulnerability manufacturers simply haven't had to deal with before.

State-of-the-art machinery often includes security features that mitigate risk, but that level of equipment may be cost prohibitive to smaller manufacturers, who need to find ways to secure older, vulnerable equipment.

"One of our biggest risk areas are the controllers on some of our older manufacturing machinery," says Peter Losiniecki, information technology leader at R&B Wagner Inc., a 155-employee metalworking company in Milwaukee, WI. "We can't even get a lot of the equipment manufacturers to upgrade their computer systems. There's at least one machine that's still on Windows XP. They will not provide a more current operating system or controller."

The problem is that small and mid-sized companies have put far more money into equipment than into IT, but now the two areas overlap, says John Nicholas, computer and cybersecurity professor at the University of Akron. "Manufacturers are going to have to start investing in IT personnel and people who offer services to keep their systems secure," Nicholas says.

CYBERSECURITY RESOURCES

The National Institute of Standards and Technology (NIST) provides guidance around cybersecurity standards for manufacturers. There are also free resources, published by universities and tech companies.

NIST Manufacturing Extension Partnership
https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance

NIST Self-Assessment Handbook
https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf

NIST Cybersecurity for IoT Video
https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

MForesight: Alliance for Manufacturing Foresight, Guide for Manufacturers
https://cra.org/ccc/wp-content/uploads/sites/2/2017/10/MForesight-Cybersecurity-Report.pdf

Center for Education and Research in Information Assurance and Security, Purdue University
https://www.cerias.purdue.edu

Deloitte and MAPI Video on Cyber Risk in Advanced Manufacturing
https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html

The first step in helping to protect the network should be installing firewalls that identify and block vulnerabilities in industrial environments, says Bryan Tantzen, senior director of industry solutions at Cisco Systems. Plants also need a secure method of remote access, so equipment vendors can communicate with their installed machines to troubleshoot problems and maintain the systems.

Manufacturers rolling out new equipment should work with their networking provider to isolate or segment the part of the network the new machines run on. They can also install tools that offer visibility: the ability to monitor network performance and identify potential security issues in all segments of the network. Tools are available that provide the same sort of visibility in OT networks that network managers have had for years in IT networks.

The best bet for small and mid-sized manufacturers: Even if you anticipate that it'll take three to five years to upgrade to IoT equipment, start creating a security plan for introducing it now, so you're ready as your old, vulnerable machines need to be replaced.

5 Develop a response and recovery plan.

Response and recovery plans are essential to any security program because it's more a matter of *when* you are going to be hacked than *if* you will be hacked. You don't want to be caught off-guard.

A response and recovery plan is another cybersecurity tool a consultant can help develop. It should detail step-by-step processes and responsibilities for incident response, including who will do the hands-on work of analyzing the scope of the attack and restoring lost systems and databases, as well as when to notify the company's attorney, law enforcement and, possibly, the local media.

Companies may want to publish the step-by-step plan in the company manual or at least create redundancy in responsibilities, so if the IT person is out sick or on vacation, somebody else can get started on crucial steps like unplugging infected computers or machines and calling legal counsel.

While most manufacturers will first concentrate on their office IT systems, it's also important to include OT systems in the plan.

Marty Edwards, of the Automation Federation, says many manufacturers neglect to make regular OT backups. He says this can become a real problem, pointing to a recent ransomware case in which a Midwest hospital resorted to paying more than $50,000 ransom because it just didn't have the mechanisms in place to restore its systems.

"I would ask them, 'Why is a ransomware infection on your system any different than a fire or some other disaster?'" he says. "You should have a plan to recover from that."

Most importantly, he adds, those plans need to be tested and practiced. The first time you run the response, it will not go smoothly, so you want to discover any hiccups long before a real incident. For example, Edwards says, "If you've done these backup tapes for years and years, when's the last time you took one off the shelf and actually tried to restore it?"

CYBER RISK MANAGEMENT: HOW HUNTINGTON CAN HELP.

As risk-management leaders, CFOs, treasurers and other executives must help protect corporate data and systems without handcuffing the technologies that improve speed, efficiency and connectivity of plants and overall businesses. To do this, they need to work with their boards of directors, IT and OT managers—and, importantly, with their financial institutions.

"Cybersecurity should be viewed in conjunction with an overall business continuity strategy, and your financial institution should be helping your business operate and be successful," said Don Boian, chief information security officer at Huntington.

We work closely with businesses to provide tailored, actionable insights that help them mitigate risk and manage uncertainties. By leveraging our collective expertise, we can help navigate the risks associated with cyberattacks to help better protect your company and your customers. Talk to a local Huntington Relationship Manager about managing and mitigating the impact of cybercrimes on your company.

About Huntington

Huntington Bancshares Incorporated is a regional bank holding company headquartered in Columbus, Ohio, with $104 billion of assets and a network of 966 branches and 1,848 ATMs across eight Midwestern states. Founded in 1866, The Huntington National Bank and its affiliates provide consumer, small business, commercial, treasury management, wealth management, brokerage, trust, and insurance services. Huntington also provides auto dealer, equipment finance, national settlement, and capital market services that extend beyond its core states. Visit huntington.com for more information.

References

1 *Cisco Systems. Cisco 2017 Midyear Cybersecurity Report.*

2 *IBM Corporation. X-Force Threat Intelligence Index, 2018 Report.*

3 *Cisco Systems. Cisco 2017 Midyear Cybersecurity Report.*

4 *Ibid.*

5 *Ponemon Institute. 2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB).*

6 *Kaspersky Lab. On the Money: Growing IT Security Budgets to Protect Digital Transformation, 2018 Report.*

7 *Ponemon Institute. 2017 Cost of Data Breach Study, Global Overview.*

8 *Ponemon Institute. 2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB).*

9 *IBM Corporation. X-Force Threat Intelligence Index, 2018 Report.*

The information provided in this document is intended solely for general informational purposes and is provided with the understanding that neither Huntington, its affiliates nor any other party is engaging in rendering financial, legal, technical or other professional advice or services. Any use of this information should be done only in consultation with a qualified and licensed professional who can take into account all relevant factors and desired outcomes in the context of the facts surrounding your particular circumstances. The information in this document was developed with reasonable care and attention. However, it is possible that some of the information is incomplete, incorrect, or inapplicable to particular circumstances or conditions. NEITHER HUNTINGTON NOR ITS AFFILIATES ACCEPT LIABILITY FOR ANY DAMAGES, LOSSES, COSTS OR EXPENSES (DIRECT, CONSEQUENTIAL, SPECIAL, INDIRECT OR OTHERWISE) RESULTING FROM USING, RELYING ON OR ACTING UPON INFORMATION IN THIS DOCUMENT EVEN IF HUNTINGTON AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF OR FORESEEN THE POSSIBILITY OF SUCH DAMAGES, LOSSES, COSTS OR EXPENSES.