CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) | BY JOHN DURKIN

SECURE OUR MANUFACTURING TO SECURE OUR WORLD

SECURITY IS A PRIMARY OPERATIONAL CONSIDERATION FOR MANUFACTURERS OF ALL SIZES

Over the past few years, a scourge of cyberattacks has caused extraordinary harm to manufacturers in New York, throughout the U.S. and worldwide: factories have been forced to close as online criminals rendered critical systems inoperable, private data has been breached and held for ransom, and proprietary information has been stolen. In every instance, these manufacturers have faced production delays, suffered revenue losses, and expended untold sums on mitigation and recovery. And the frequency of these attacks on our manufacturers continues to grow.

Technology manufacturers can play an especially impactful role in Securing Our World by implementing security features in their products that are built-in by design.

As manufacturing environments have become more interconnected with and reliant on enterprise networks, public clouds, vendor networks, and other third-party resources to conduct their operations, bad actors have set their sights on exploiting this ever-expanding attack surface. According to IBM Security's 2023 X-Force Threat Intelligence Index, manufacturers were the number one target for ransomware attacks for the second straight year in a row last year, a trend that will abate only when we redouble our efforts to shore up our defenses.

The Cybersecurity and Infrastructure Security Agency's (CISA) office here in New York works with industry stakeholders to provide resources and tools to reduce the prevalence and impact of these cyberattacks and to build resilience into their operations. As October first marked the start of the 20th annual Cybersecurity Awareness Month and the launch of CISA's **Secure Our World** program, there's no better time than now for conversations about cybersecurity.

I'll discuss the objectives of the Secure Our World program and its importance to the manufacturing sector in a moment, but in name alone it should resonate with those in the industry: Security is a primary operational consideration for manufacturers of all sizes – the physical security of offices, plants, personnel, and proprietary information and data is front of mind for every owner and operator. More and more, however, those physical security processes rely on internet-connected systems or networks and that technology plays a role in everything that keeps an organization secure - from communications equipment, security cameras, and access control systems to the very grid networks that power them.

We depend on this technology functioning well to keep our people and our facilities safe. How effective would it be in the event of a cyberattack?

I mention this to underscore the fact that cybersecurity is security. Full stop. A robust and resilient cybersecurity program is foundational to overall security in every organization, large or small.

In an industry steeped in security vigilance, how is it then that cyberattacks against manufacturers continue to grow?

The answer is that cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.

As CISA Director Jen Easterly put it, "The digital threat landscape continues to evolve at an alarming rate, and yet many individuals and organizations have yet to evolve their digital hygiene practices at the same pace."

The **Secure Our World** program aims to bridge that gap and provide individuals and organizations with the knowledge and tools they need to stay one step ahead of cyber threats by driving behavioral change of the most critical cybersecurity habits. Small and medium-sized businesses face unique challenges, so CISA is working to help them **Secure Our World** by offering tools and resources that can help keep our businesses, employees, customers, and ultimately, our communities safer.

For those businesses, driving behavioral change to integrate four key areas of cyber hygiene into day-to-day operations is critical to Securing Our World:

- Using strong passwords.
- Enabling multifactor authentication on all accounts that offer it.
- Recognizing and reporting phishing.
- Updating and patching software.

Remarkably, practicing these simple and straightforward behaviors could prevent the majority of cyberattacks, with phishing being the number one means through which criminals accessed manufacturers' systems in 2021 and 2022, according to the IBM Security report. Additionally, phishing-related data collected during CISA Assessments has shown that within the first 10 minutes of receiving a malicious email, 84% of employees took the bait by either replying with sensitive information or interacting with a spoofed link or attachment, and only 13% of targeted employees reported the phishing attempts.

The good news is that manufacturers are building cybersecurity into their overall security plans more and more. A 2022 Manufacturing Leadership Council survey found that 62% of surveyed organizations had a formal cybersecurity plan in place, nearly double the number reported in 2018. The bad news, of course, is that 38% of surveyed manufacturers are still missing this critical element in their overall security picture.

CISA's Cybersecurity and Protective Security Advisors here in New York are available to provide an array of no-cost services, resources, and assessments to support manufacturers in building cyber threat prevention and resilience into their security plans. As an agency built on collaboration, the organizations who work with CISA do so voluntarily and on their terms, knowing that the

information they provide will be protected. CISA can also develop and conduct tabletop cybersecurity exercises for your organization, provide general cybersecurity awareness training, and our advisors are available to speak to your workforce or security-focused events.

A few actions every manufacturer can take today to Secure Our World:

- Use strong passwords and a password manager. Passwords should be at least 15 characters long, unique to each account and, preferably, randomly generated by a password manager or computer.
- Enable multi-factor authentication (MFA) across all internet-facing accounts and services. Ensure everyone in the organization is using MFA on their accounts and devices, particularly for webmail, virtual private networks, and accounts that access critical systems.
- Avoid social engineering and phishing attacks. Educate personnel to recognize phishing (malware embedded in an email link), vishing (gleaning information to access systems via a phone call) and smishing (malware embedded in a text link) attempts and what they should do if they see something suspicious.
- Keep all operating systems, software, and firmware up-to-date. Enabling automatic updates and timely patching are among the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.
- Use a reputable anti-virus and malware product and keep it up-to-date.
- Ensure devices accessible to the internet are properly configured and that security settings are enabled and kept up to date.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location.
- Maintain a current and tested Incident Response Plan to help quickly mitigate and recover should a ransomware or other cyber intrusion occur.
- Regularly visit StopRansomware.gov for a wide variety of resources to raise your organization's cybersecurity awareness, and to stay up to date on the latest alerts and advisories regarding current threats.

The manufacturing industry is critical to the economic well-being of the nation, and its success in defeating cyber criminals is critical to our national security. Securing manufacturing secures our nation and secures our world.

To connect with your CISA advisors in New York or to learn more about CISA's resources, email CISA Region 2 at CISARegion2@cisa.dhs.gov. Learn more about Region 2 at CISA Region 2.

All organizations should share information on incidents and unusual activity at Report to CISA | CISA or by going to CISA.gov and clicking the "report a cyber issue" button at the top of the page. Alternatively, you can reach CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870, or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Additional Resources:

- **CISA Cybersecurity Awareness Program Toolkit** provides resources for all segments of the community.
- **CISA's Cyber Essentials** is a guide for leaders of small organizations and agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.
- **Critical Manufacturing Sector Resources** CISA identifies, assesses, prioritizes, and protects manufacturing industries with national significance to prevent and mitigate the impact of manmade of natural disasters.
- **Cross-Sector Cybersecurity Performance Goals (CPGs):** CISA developed the CPGs to help critical infrastructure prioritize investments where they are most likely to achieve high-impact cybersecurity outcomes. The CPGs can be especially helpful for healthcare and public health organizations that have gaps in expertise, resources or capabilities.
  - o **Cross-Sector Performance Goals Checklist:** As you get started on the CPGs, look through this checklist to help prioritize and track your organization's implementation.
- **CISA's Cybersecurity Advisors (CSAs)** offer cyber security assistance to critical infrastructure owners and operators and State, Local, Territorial, and Tribal (SLTT) officials. CSAs introduce organizations to various CISA cyber security products and services, along with other public and private resources, and act as liaisons to CISA cyber programs. CSAs can provide cyber preparedness assessments and protective resources, working group support, leadership, partnership in public-private development, and coordination and support in times of cyber threat, disruption, or attack.
- **CISA's Protective Security Advisors (PSAs)** are trained subject matter experts in critical infrastructure protection and vulnerability mitigation. They facilitate local field activities in coordination with other Department of Homeland Security offices and Federal agencies. They also advise and assist state, local, tribal, and territorial (SLTT) officials and critical infrastructure owners and operators, and provide coordination and support in times of threat, disruption, or attack.

Sources:

CISA Insights - Cyber Threats to Critical Manufacturing Sector Industrial Control Systems
NIST - Cybersecurity for the Manufacturing Sector
IBM Security X-Force Threat Intelligence Index 2023 | IBM
Manufacturing was the most targeted sector for ransomware attacks in 2022
CISA Phishing Infographic
Manufacturers Are Getting Tough on Cybersecurity – Nat'l Assoc of Manufacturers

John Durkin is the Cybersecurity and Infrastructure Security Agency Region 2 Regional Director.