SPECIAL REPORT:

CYBER SECURITY

PROTOCOLS FOR MANUFACTURERS DURING COVID-19

WHAT'S IN THE REPORT:

- 7 types of threats manufacturers should watch out for
- Strategies to secure equipment and networks
- Best practices for training staff
- What to do in the event of an attack
- Free cyber risk assessment

NAM CYBER COVER

AHT INSURANCE

SPECIAL REPORT:

CYBER SECURITY

PROTOCOLS FOR MANUFACTURERS DURING COVID-19

In addition to the health and safety concerns surrounding COVID-19, manufacturing companies also must stay vigilant regarding cybersecurity. With so many employees now working remotely, businesses face a dramatic increase in the risk of cyber threats. A data breach or malicious attack can lead to safety risks, downtime and disruption, loss of reputation, damage to customers, impact to your bottom line and more.

By securing your systems and following best practices, you can protect your network, company, employees and customers while keeping your business up and running. Use this special report to help you safely connect your remote workforce, minimize your cybersecurity risk and mitigate the impact of any incidents.

CYBER THREAT LEVEL

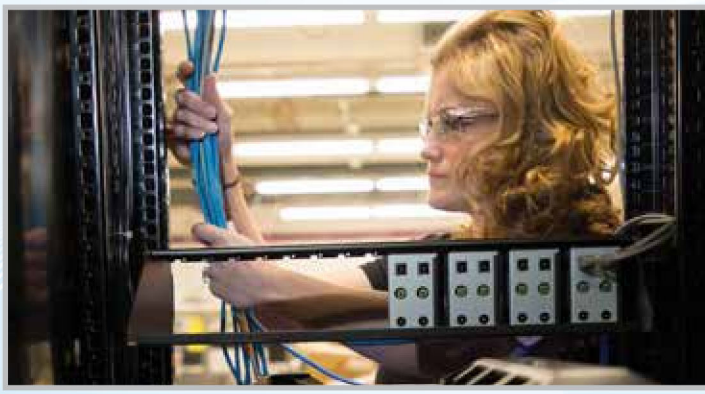
86% of cyber attacks against manufacturers are deliberate and targeted[1]

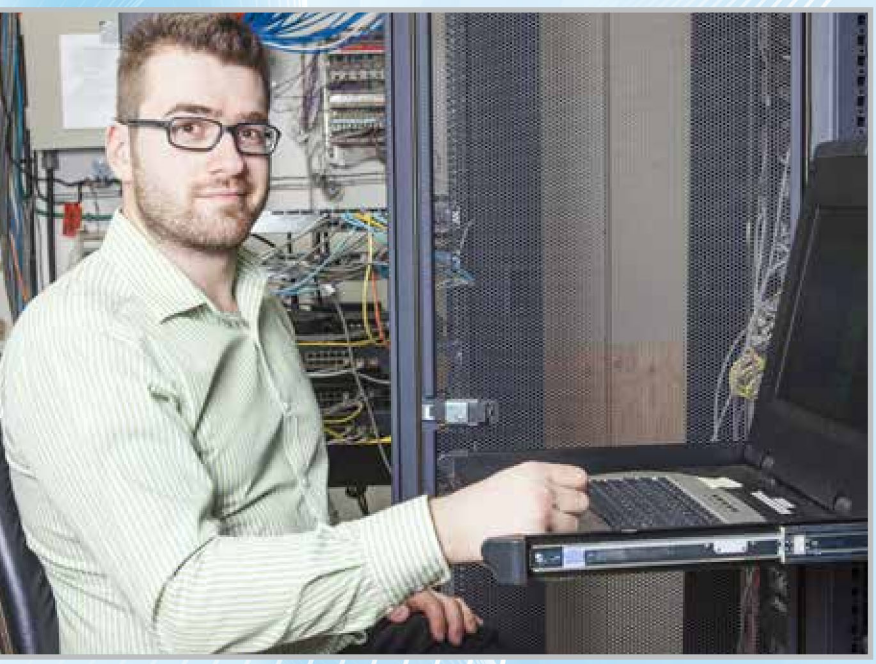
39% of manufacturers experienced a breach resulting in losses of $1 million to $10 million[1]

78% increase in supply chain attacks in 2019[2]

40% of all ransomware claims result from exploitation of remote access services[3]

1. Symantec Internet Security Threat Report 2019
2. Varonis “110 Must-know Cybersecurity Statistics for 2020”
3. Coalition cyber insurance provider





CYBER SITUATION DURING COVID-19

Why the increased risk during the pandemic? Much of the U.S. workforce is working remotely, and cyber actors and hackers are feeding on this opportunity to exploit vulnerabilities. Home networks are typically not as secure as business networks, yet your remote employees still handle sensitive information—financial records, employee data, intellectual property, control of your automated facilities and more. The increase in online communication and interaction increases the potential for problems.

THREATS TO MANUFACTURERS

Threats to your company, employees, processes and data take many forms, and new threats emerge almost daily. Here are a few current threats to be aware of:

Data breaches—loss or theft of confidential information such as employee Social Security numbers and personal information, passwords, bank account numbers and more

Intellectual property theft—theft of proprietary company and product information that could be valuable to competitors or those seeking to harm your company

Ransom—an unsavory party locks down your systems and demands money to release them, taking away access to your company data, communication channels and the control of your facilities

Phishing scams—emails or documents posing as legitimate communications designed to steal personal or company information

Hacking or hijacking—a hacker accesses your networked production equipment and takes control of your plant, perhaps destroying equipment and products while posing safety risks to your on-site workers

Zoom bomb—hackers infiltrate your videoconferencing platform and display disturbing and disruptive graphic content

Disinformation campaigns—efforts to spread discord, disrupt markets, and influence policy development through false information

HOW TO PROTECT AGAINST THREATS

The best way to bolster your cybersecurity is through a combination of secure equipment and best practices, including employee training.

DEVICES AND NETWORKED EQUIPMENT

If a device or piece of equipment is Wi-Fi enabled and connected to your network, it's vulnerable to outside attacks—and it makes your entire network vulnerable. (Hackers in the newsworthy Target data breach of 2013 entered Target's system via the networked HVAC system, for example.) Ensure all equipment, from employee mobile devices and laptops to automated production equipment, has up-to-date firewalls plus anti-malware and intrusion prevention software installed. Teach your employees to update their home routers so they do not use default network names and login credentials.

VPN NETWORK

A virtual private network, or VPN, creates a secure, encrypted connection between your remote employees' devices and a company server connected to the internet. A VPN effectively shuts down your network to outside traffic.

NETWORK SEGMENTATION AND ACCESS CONTROL

Another way to enhance security is to divide your network into multiple segments that are not connected to one another. This way, if you experience a security breach in one segment, your entire business is not affected. For additional security, set up user-based permissions that limit an individual's access to only the segments or subsegments they need.

BEST PRACTICES FOR SECURE EQUIPMENT

> Update anti-malware software
> Create a virtual private network
> Segment networks
> Control access for each user
> Require multi-factor authentication
> Use proactive monitoring and threat detection

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication can strengthen your cybersecurity by requiring multiple credentials to access a system, application or device. For example, you can require a user to log in to your intranet or company email program using a password as well as a code sent to their mobile device.

PROACTIVE MONITORING AND THREAT DETECTION

Enable system monitoring and threat detection with alerts so you can be aware of any issues and take action as soon as possible to minimize damage and disruption. Another proactive strategy is to enlist professionals known as ethical hackers to seek out vulnerabilities in your system. Consider also hiring dedicated cybersecurity personnel whose focus is to protect your network from the latest threats.

ENHANCE PASSWORD PROTOCOLS

Passwords such as 12345 or ABCDE are all too common, leaving your accounts and network vulnerable to hackers. According to the U.S. Department of Commerce's National Institute of Standards and Technology, the current best practice is to increase password length, not necessarily password complexity. NIST suggests passwords of 16-64 characters. Additional best practices include regularly updating passwords and never using the same password for more than one account.

RESPONSIBLE WI-FI USE

Discourage employees from using unsecured public Wi-Fi without a VPN when accessing work-related accounts and materials. If public Wi-Fi must be used, train staff to look for a green padlock at the top of the web browser to ensure a trusted internet connection.

EMAIL BEST PRACTICES

Discourage your staff from sending sensitive information or documents via email. Instead, share documents via a secure cloud-based platform. You should also increase the sensitivity of your email program's spam filter as a precaution against phishing attacks.

BUSINESS CONTINUITY PLANS

Ensure your business continuity plans and emergency response plans have been updated to account for your remote workforce. Does everyone know what their role is in the event of a disruption? Additionally, establish an acceptable use policy for remote access to company servers and systems.

STAFF TRAINING

Train staff on how to securely access your system, how to look out for new threats and scams, and how to use trusted sources for the latest information. Run drills and practice scenarios. One company sends dummy phishing emails to employees; anyone who falls for the "scam" is required to take a brief cybersecurity awareness course. Also make sure everyone knows how to contact your IT support team or cyber incident emergency response team. Because cyber threats are constantly changing, implement a system for keeping staff up to date on any new risks, disinformation campaigns, or best practices to minimize disruption.

INCIDENT RESPONSE AND MITIGATION

Despite your best security efforts, cyberattacks and data breaches can happen. Enlist the help of professionals to respond to a cyber incident quickly to minimize damage and downtime. Consider purchasing cyber insurance to help you reduce the severity of any financial losses.

BEST PRACTICES FOR TEAM TRAINING

> **Publish** contact info for IT support and cyber incident response team

> **Distribute** an acceptable use policy for remote access

> **Update** your business continuity plans for remote workforce

> **Establish** an alert system to keep your team informed

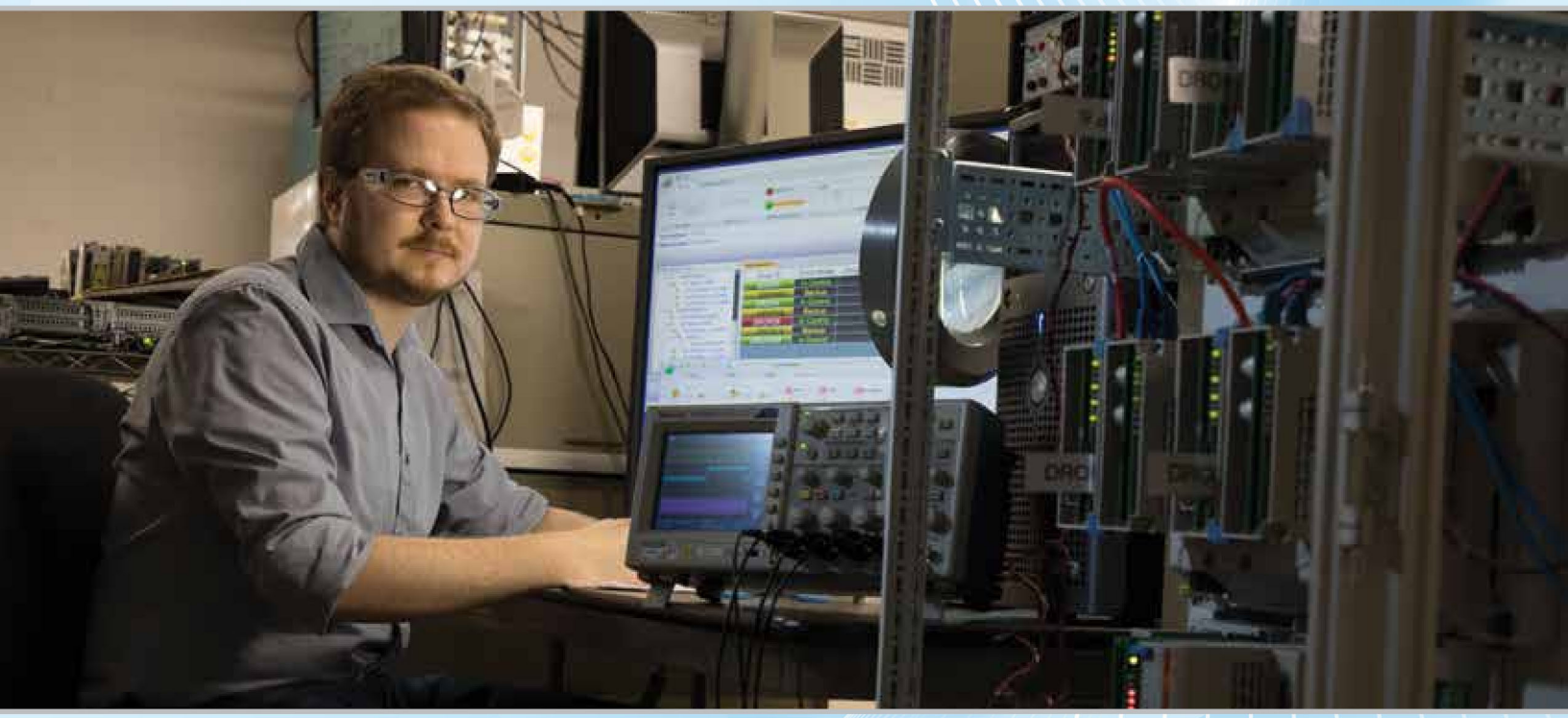
> **Create** protocols for updating passwords regularly

> **Educate** staff on responsible use of email and public Wi-Fi

> **Run** practice drills and offer cybersecurity awareness courses

HOW TO STAY SECURE

Throughout the COVID-19 pandemic, you have likely learned that nothing is certain and things change rapidly. Cybersecurity during this time is no different. Be aware that no single cybersecurity solution is sufficient to protect your business from an attack. Using multiple protocols and best practices will help you maximize the security you have in place and anticipate emerging threats.



ADDITIONAL RESOURCES

CYBER FRAMEWORKS

Standards, guidelines and best practices to manage your cybersecurity risk. Published by the U.S. Department of Commerce's National Institute of Standards and Technology.

GET THE FRAMEWORKS

RISK MANAGEMENT FOR NOVEL CORONAVIRUS

A quick resource to identify potential risks of COVID-19, including cybersecurity issues, and what you can do to protect your business. Produced by the Cyber and Infrastructure Security Agency, a division of the U.S. Department of Homeland Security.

GET THE FACT SHEET

NAM CYBER COVER

A program from the National Association of Manufacturers to identify, protect and manage the unique cyber risks that face manufacturers. Includes insurance and proactive cybersecurity tools.

LEARN MORE

FREE CYBER RISK ASSESSMENT

What is your company's risk level for cyberattacks during COVID-19? Find out with a free Cyber Risk Assessment.

GET AN ASSESSMENT

REMOTE ACCESS THREATS

Learn more about the one technology responsible for more than 50% of all ransomware events. Get the technical details on the Coalition cyber insurance blog.

READ THE BLOG

NAM CYBER COVER

Identify, protect and manage the unique cyber risks that face manufacturers. This program combines the power of a leading cyber insurance provider, Coalition, with a nationally recognized broker, AHT Insurance.

PROGRAM BENEFITS

Manage risks
Mitigate severity
Respond quickly
Recover from an attack

HOW THE PROGRAM WORKS

Simply request to be contacted by a NAM Cyber Cover specialist. They will be in touch promptly with your free Cyber Risk Assessment and quote.

Learn more at namcybercover.org.

Cyber insurance and risk mitigation for manufacturers