What Manufacturers Need to Know About Cyberattacks

By George Thuo
Director of Cloud
Global Shop Solutions

We simplify your manufacturing.™

Data breaches and cyberattacks are one of those things small to medium size manufacturers think **it won't happen to me**. Yet, according to the Verizon 2023 Data Breach Investigations Report, 43% of all cyberattacks are conducted against small businesses. If that doesn't grab your attention, consider this fact: manufacturing ranked 4th in the number of cyberattacks by industry, topped only by the public administration, information and finance industries. Denial of service, an interruption in an authorized user's access to a computer network, had the most attacks in the manufacturing industry, with ransomware a close second. Ninety-six percent of cyberhacks in the manufacturing sector were motivated by money.

Clearly the manufacturing industry is under siege from highly skilled hackers who are constantly developing new ways to achieve successful data breaches that yield substantial amounts of money. Yet, hackers pursue more small and medium manufacturers for a variety of reasons. Why do so many manufacturers receive so much attention from cybercriminals and face higher risks? And how do you protect your data, finances and business from the evil doers?

What Do Cyberattacks Look Like?

Cyberattacks are a malicious disruption of a company's systems and/or network. Hackers use harmful code to compromise your computer system so they can steal or hold your data hostage. They have many different types of cyberattacks to deploy. These include:

- Ransomware
- Identity theft, fraud and extortion
- Malware, phishing, spamming, spoofing, spyware, trojans and viruses
- Stolen hardware, such as laptops or mobile devices
- Intellectual property theft or unauthorized access
- Denial of service attacks
- Breach of access and "password sniffing"
- System infiltration and website defacement
- Instant messaging abuse

The type of attack deployed depends on what the hacker is seeking. Ransomware attacks are motivated purely by money. Identity theft, fraud and extortion attacks seek money, but often the hacker is looking for sensitive data that could lead to more successful data breaches and a higher financial return. Regardless of the type, cyberattacks involve a clandestine effort to gain access to your data and digital assets undetected, thereby putting the hacker in control of your company's system.

Why Smaller Manufacturers are Prone to Cyberattack

Small and medium size manufacturers are targeted by cyberhackers for most of the same reasons as other small businesses. The primary attraction is that manufacturers don't have the technology or resources that larger companies do. Most can't afford the best protections or trained cyber security personnel to protect their systems and data. Many fail to adequately train their employees on how to prevent phishing and other types of attacks that take advantage of naive individuals who don't respond to emails with a careful eye.

Cybercriminals understand the vulnerability of manufacturers and target their businesses accordingly. In many cases, penetrating a manufacturer's security proves to be less of a challenge than larger companies. If hackers fail to penetrate a targeted manufacturer, they typically move on to the next small manufacturing business that has its guard down.

Even though small to mid-size manufacturers lack the financial assets of larger enterprises, ransomware is still a favorite of cyberhackers because manufacturers often pay the ransoms. Small cyberassaults can have large financial and data repercussions, and the larger the extent of the breach the more likely the manufacturer will pay the ransom. Cyberattacks can also create devastating damage by targeting critical plant equipment, and supply chain disruptions can create ripple effects that shut down production lines for several days or more, thereby throwing production goals and distribution targets into disarray and confusion.

Data Breaches Also Popular with Hackers

A data breach is defined as a security incident in which unauthorized intruders access sensitive or confidential information. The information can include personal data, such as Social Security numbers, bank account numbers, healthcare data, corporate data from customer records, intellectual property and financial information. Data breach and cyberattack are often considered equivalent terms. However, data breach refers only to security breaches in which someone gains unauthorized access to data. Hackers acquire unauthorized access to data in many ways, including:

- Weak and stolen credentials
- Backdoor and application vulnerabilities
- Malware
- Social engineering
- Excessive permissions
- Ransomware
- Denial of service attacks
- Improper configuration and exposure via application programming interface (API)

Data breaches typically provide the fuel for ransomware attacks that result in large payments from the manufacturer. However, they can also yield extremely valuable information that opens the door for the hacker to hold other companies or customers at ransom.

Minimizing Damage from a Cyberattack

Keeping cyberattack damage to a minimum requires quick response with a plan of action worked out in advance. Be prepared to implement these six steps as soon as possible.

1. **Identify the attack.** Identifying the type of attack will help you determine its severity and the measures needed to mitigate the damage. Some common types of cyberattacks include ransomware, phishing, denial of service, and malware.

2. **Isolate the affected systems.** Once you've identified the type of attack, disconnect the affected systems from the internet and your internal network to prevent the attack from spreading to other systems in your network. Complex networks may require more sophisticated isolation measures.

3. **Contain the attack.** Determine the scope of the attack by identifying the systems and data that have been compromised. Identify any vulnerabilities that may have been exploited to carry out the attack.

4. **Notify internal and external affected parties.** These include your senior management, IT department, and third-party vendors or service providers that may be affected. Contact law enforcement officials if evidence of criminal activity exists.

5. **Recover and restore your systems and data.** Use backups to bring systems and applications up to date with the latest security patches. Conduct a comprehensive review of your security policies and procedures to identify weak points in your security infrastructure.

6. **Learn from the attack.** The final step involves researching and analyzing the attack to uncover any gaps in your security technology and procedures. Provide all employees with hands-on training for recognizing and responding to cyberattacks. Bring your systems and data back up as quickly as possible while minimizing the damage in the process.

How to Protect Your Shop from a Cyberattack

No defense is perfect, but implementing these 12 steps can significantly reduce the odds that hackers will be able to penetrate your data and systems.

1 Employee awareness and training.

Cyber hackers frequently send phony emails expecting some unaware user will take the bait. These often seem legitimate to untrained employees, making it easy to fall into the hacker’s trap. Train your employees to always:

- Check links before clicking them
- Check email addresses from received emails
- Use common sense before sending sensitive information
- If an email request seems odd or suspicious, call the person and verify the source and the request

2 Use patch management.

Cybercriminals are professionals at exploiting system weaknesses to gain access to your network. Patch management is a process of applying updates to software, drivers, and firmware to protect against vulnerabilities. Designed to manage all your software and system updates, patch management also boosts productivity by ensuring optimal operating performance of your systems.

3 Protect all your endpoints.

Endpoints consist of desktop computers, mobile devices, servers, embedded devices, and other physical devices that connect to and exchange information with a computer network. They also provide access paths to security threats but can be protected with endpoint protection software and anti-virus programs running on all computer systems.

4 Build a firewall.

With so many sophisticated data breaching techniques, protecting your network with a firewall is essential. A computer network security system that restricts internet traffic within a private network, a firewall provides a highly effective defense against cyberattacks.

5 Use of two factor authentication.

Two-factor authentication (2FA) is an identity and access management security method that requires two forms of identification to access data and resources. Enforce it on email and other commonly accessed applications.

6 Perform penetration testing on systems.

Engage an Independent Cybersecurity company e.g. once a year to perform penetration testing on all internal systems to identify vulnerabilities or points that need better protection.

7 Back up your data in remote locations.

Data hacks of full backups can result in significant down time, loss of data and devastating financial loss. Back up your data on a regular basis and store it in different locations in case your onsite backups are compromised.

8 Control physical access to your systems.

Without a reliable perimeter security system someone could walk into your facility and infect your file or gain access to your entire network by inserting a hardware key that identifies an authorized user. Be very careful about who has access to your systems and how they get in.

9 Don’t overlook wifi security.

With thousands of wifi enabled devices in the world, the risk is any device can get infected by connecting to a network. An infected device that gets connected to your business network puts your entire system at risk. Securing your wifi networks is a vital safety feature for your systems.

10 Use separate personal login accounts for all employees.

Every employee needs their own login for every application and program they use. Ensuring every staff member has separate logins helps reduce the number of potential attacks. Users should log in only once a day with their own personal set of logins.

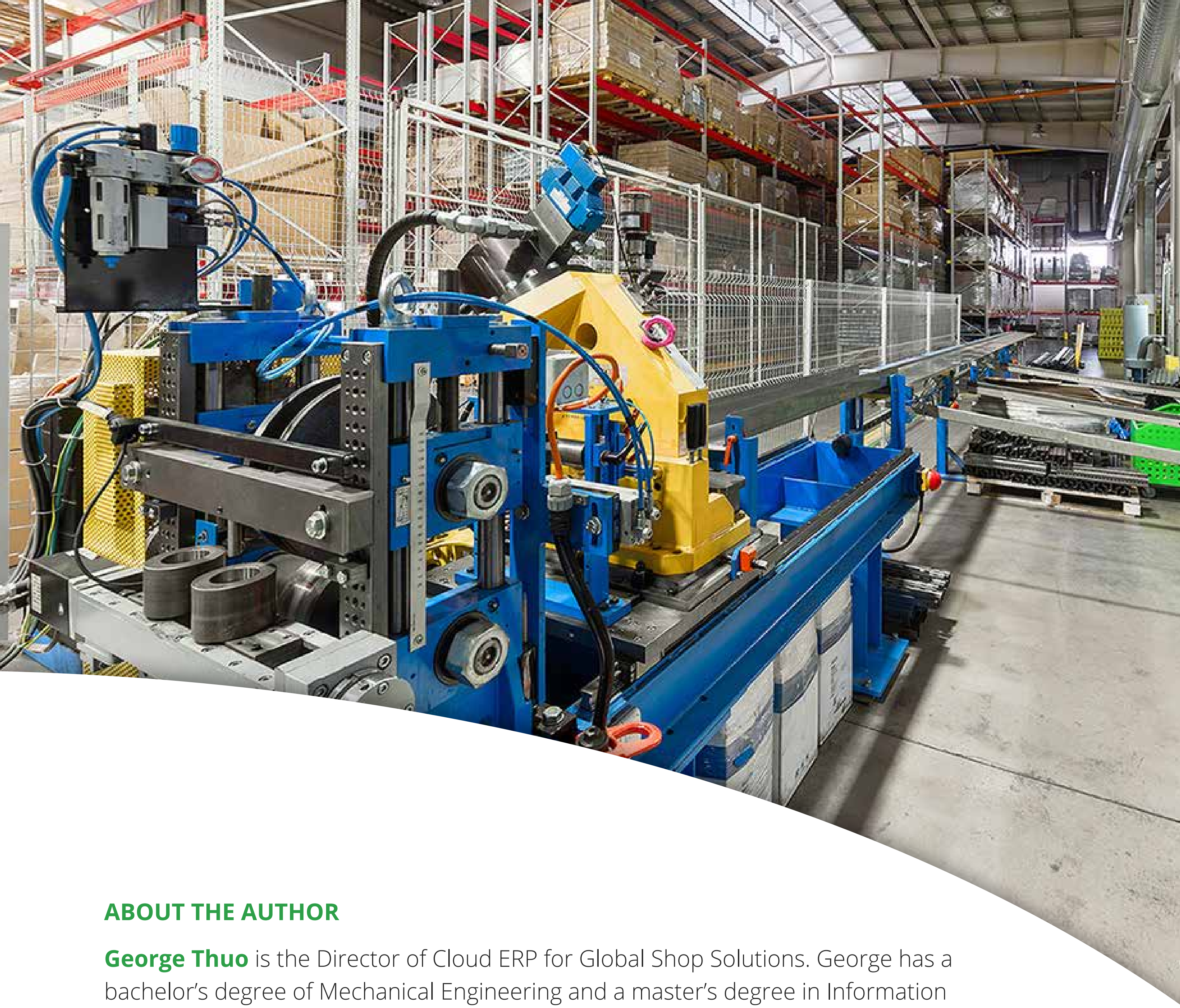
11 Have strict access management.

Allowing employees to install software on business owned devices could compromise your systems. Reduce risk by using managed administrative rights to prevent your staff from installing or even accessing certain data on your network.

12 Use a different password setup for each application.

Never assign the same password setup for different applications. Otherwise, if hackers discover the password, it could provide access to any application you use. Using different password setups and changing them often will sustain high protection levels against external and internal threats. This can be made easier by using a password manager program so the user doesn't have to remember every single password.

Above all, have an experienced IT expert to keep your security infrastructure up to date with new technologies and functioning as it should. At Global Shop Solutions, growing numbers of our manufacturing customers are migrating to cloud ERP for the security of having their software and data securely stored on off-site servers. Click here to learn the advantages of Cloud security for manufacturers.



ABOUT THE AUTHOR

George Thuo is the Director of Cloud ERP for Global Shop Solutions. George has a bachelor's degree of Mechanical Engineering and a master's degree in Information Systems Management from Baylor University along with more than two decades of cloud and technical experience. George is dedicated to helping customers run more efficiently with cloud ERP.

Global Shop SOLUTIONS ERP SOFTWARE

We simplify your manufacturing.™