ARCTIC WOLF

Security Operations for **Manufacturing Organizations**

END CYBER RISK

MANUFACTURING CYBERSECURITY GUIDE

TABLE OF CONTENTS

SECURITY OPERATIONS FOR **MANUFACTURING ORGANIZATIONS**

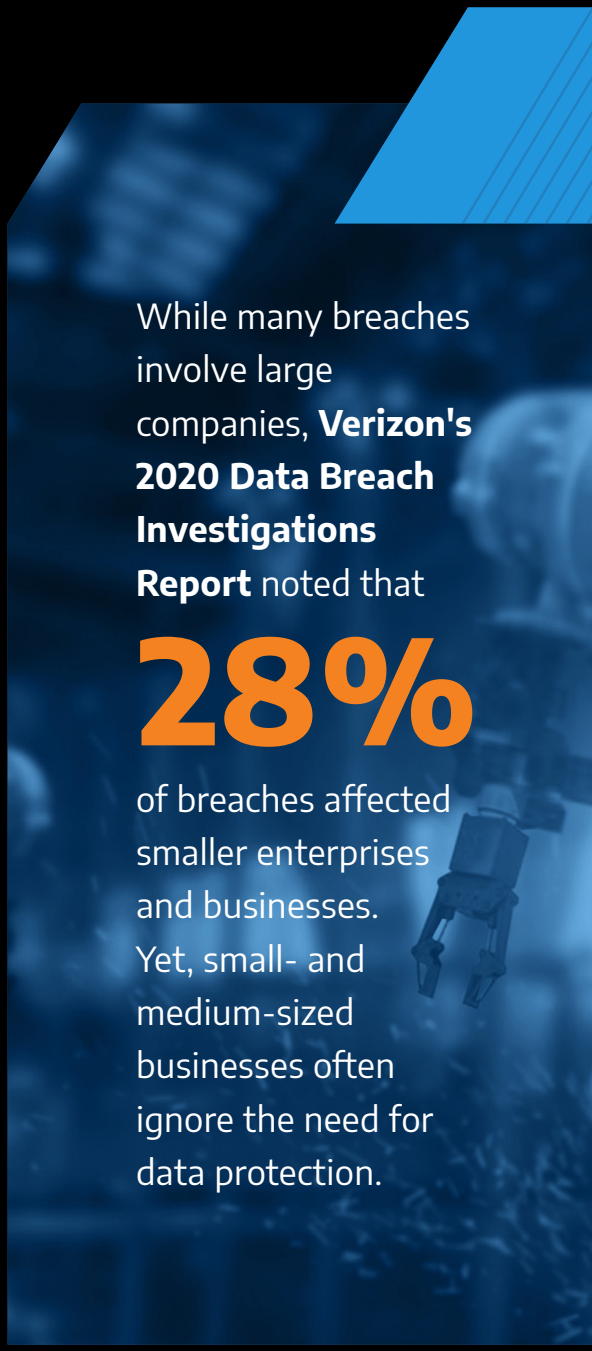
As the manufacturing sector rushes to embed the latest technologies, the risk of cyberthreats continues to grow at an unprecedented rate. Unfortunately,with each new device a manufacturer adopts, the pathways cybercriminals can exploit grow exponentially.

When criminals launch an attack, the resulting downtime can have a crippling effect on every aspect of production. A single attack can take down an entire production line and impact delivery schedules for weeks, and sometimes months.

Given the ramifications of a successful attack, manufacturers must prioritize building a security posture that is strong enough to prevent attacks and keep production flowing. They must eliminate security risks so they can satisfy partners and customers who depend on a consistent production schedule. In some cases, such as when customers rely on a manufacturer for their supply of medicine, honoring that commitment is critically important.

When a manufacturer fails to live up to its commitments, it calls into question its ability to deliver in the future. That's why an attack can cause irreparable damage to your relationship with partners and customers.

Investing in a robust cybersecurity program helps manufacturers protect critical infrastructure, blueprints, critical data, trade secrets, and more. It also allows manufacturers to deliver on their customer commitments.



While many breaches involve large companies, **Verizon's 2020 Data Breach Investigations Report** noted that

28%

of breaches affected smaller enterprises and businesses. Yet, small- and medium-sized businesses often ignore the need for data protection.

THE RISE OF CYBERATTACKS ON MANUFACTURING

Recent attacks against manufacturers underscore the severity of the threats facing the industry.

A 2019 attack on Norsk Hydro, involving the LockerGoga ransomware, impacted the company's IT systems in Norway, Qatar, and Brazil, and cost the company approximately **$75 million**. And in 2018, attackers used the WannaCry virus to target the Taiwan Semiconductor Manufacturing Company, crippling the company's production line for three days and wiping out **$170 million in revenue**.

For many, the **NotPetya ransomware attack**, which originated in the Ukraine and spread infections around the globe in 2017, provides the most compelling evidence of what can happen when cybercriminals attack. According to an estimate by the White House, the virus produced losses of **$10 billion**, including a loss of $870 million for Merck, a global pharmaceutical company, and $188 million for Mondelez, a leading food company.

As recently as July 2020, Japanese car manufacturer Honda announced that a ransomware attack involving its **IT environment took** several factories offline, along with its customer and financial service centers.

$75M

LockerGoga ransomware's impact on Norsk Hydro in 2019.

$170M

WannaCry virus' impact on the Taiwan Semiconductor Manufacturing Co. in 2018.

$10B

NotPetya ransomware's impact on companies around the globe in 2017.

COMMON CYBERATTACKS ON MANUFACTURING

While ransomware attacks happen with alarming regularity, they are not the only threats facing the industry.

For example, **Datto's Global State of the Channel Ransomware Report** identified phishing emails as the primary cause of successful attacks.

To increase their chances of success, the perpetrators of phishing and ransomware attacks use highly targeted approaches, which include leveraging the pandemic with messages related to COVID-19.

Cybercriminals also continue to use perennial favorites to deliver infections—such as emails supposedly from DocuSign that ask for the recipient's signature while also downloading malware.

Phishing campaigns conducted via Snapchat have also proven effective, with **55,000 individuals** sharing their login credentials in a 2018 attack. Web attacks, which exploit vulnerabilities in web applications and often rely on SQL injection as well as cross-site scripting, continue to present a significant problem.

Lastly, manufacturers cannot overlook the threat of an account takeover. Given the widespread use of corporate credentials on third-party sites and the common practice of password recycling, a seemingly unrelated breach can pave the way for cybercriminals to get past a manufacturer's defenses.

According to our analysis, since March 2020, the number of account takeover schemes involving corporate credentials and plain text passwords shared via the dark web has grown by a staggering **429 percent**.

YOU CAN'T PROTECT WHAT YOU CAN'T SEE

Given the severity of the threats facing the manufacturing sector, how can you determine your company's risk factors and how can you ensure they're secure?

Discovery & Visibility

The first step involves asset discovery and visibility. You can only begin to shore up your defenses once you know what areas cybercriminals could potentially exploit.

Incident Response

Next, it's important to determine how your company detects a threat that penetrates your security layers. What is your current plan to respond to incidents once they occur? Due diligence in this area may uncover a lack of visibility across the supply chain.

Risk Management

Along those lines, strategic customers may require your company to complete a vendor risk management questionnaire, which can include information gathering about security monitoring and external vulnerability assessments. The ability to uncover malware beaconing on endpoints, involving communication with a malicious command and control server, is also an important capability.

Questionable Account Activity

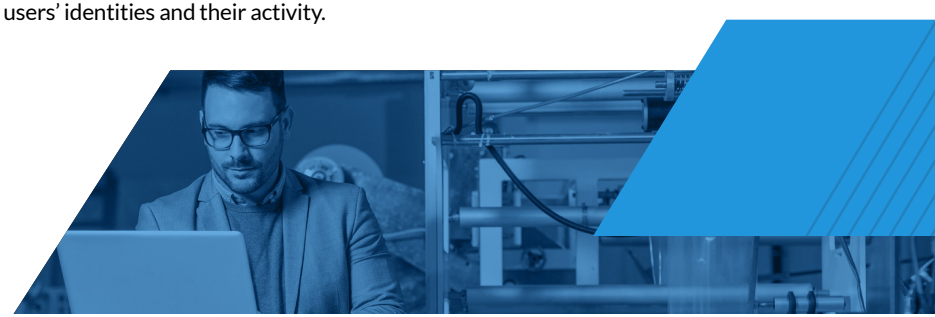
What's more, unearthing questionable administrative account activity must also be within your company's capabilities. Quickly identifying causes behind account lockouts to facilitate the unlock processes should be a priority, especially when it could impact the company's manufacturing capabilities.

Access Management Hygiene

Identity and access management hygiene also plays a role in an effective security program. It ensures that each digital entity grants the appropriate level of access and that mechanisms exist to validate the users' identities and their activity.

Cloud Configuration

When it comes to the cloud, your organization should make certain every cloud environment is properly configured. Cloud security posture management (CSPM), which is a continuous process of cloud configuration monitoring and adaptation to minimize the potential for an attack, can help your organization make significant strides towards securing its data in the cloud. By adopting this approach, organizations can also minimize the potential for cloud configuration "drift," where cloud security is affected because of one or more undocumented changes creates weakness in the environment.



DEVELOPING A PLAN

Despite severe cyberthreats infiltrating the tech landscape, many organizations lack a comprehensive approach for holistically monitoring infrastructure, or for gathering security insights from log data generated by various IT systems.

In addition, the unfortunate reality is that many manufacturers don't perform annual cyber risk assessments. That inability to test their environment leaves vulnerabilities unaddressed and makes an attack nearly inevitable in many cases.

Considering the changes brought about by the pandemic, manufacturers must also adjust patching programs to account for the remote workforce. And without an effective password management program, the threat of account takeover remains.

An effective security defense requires a solution operating 24x7.

One that includes people you can depend and rely on—cybersecurity experts who can act as a natural extension of your team. This is particularly important when you consider that 35 percent of threats appear after-hours, as our analysis shows.

Therefore, it's vital to have a dedicated, scalable support team that functions a force multiplier to generate outcomes, instead of relying on the latest security products that too often produce an overwhelming number of false positive alerts.

HOW PREPARED ARE YOU?

Is your organization investing in the right measures? It's not about the tools, it's about finding the right team to have your back.

- Has your team built an effective framework to handle a potential attack?
- Has your team effectively protected against third-party risks?
- What IoT devices are used in your organization?
- How are your patching programs performing? What adjustments need to be made?
- Does your risk-based vulnerability management program need an upgrade?

SUMMARY

Cybercriminals often follow the path of least resistance, meaning they seek out weaknesses in a manufacturer's defenses they can exploit.

An effective security program requires identifying the assets your company needs to protect, and then implementing a plan to do so. It also requires the ability to detect threats and the means to develop and execute an effective response plan when needed.

Ultimately, the goal is to prevent an attack, but when that's not possible the goal becomes to return your company to normal operating conditions as quickly and efficiently as possible. It's critical that manufacturers keep the production lines running, which means cybersecurity must always be a top priority.

ABOUT ARCTIC WOLF

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture.

For more information about Arctic Wolf, visit **arcticwolf.com**.

END CYBER RISK