ActZero

Manufacturing, Cybersecurity

AND THE NEW NORMAL

How Global Changes Affect the Midsize Manufacturer's Cybersecurity Program

ActZero

Topics Covered:

- INTEGRATION CHALLENGES
- REGULATORY REQUIREMENTS
- AUDITS
- MORE SUPPLIERS, GREATER RISKS
- POTENTIAL FOR LOSS
- STATS FOR MANUFACTURERS
- ASSESS YOUR RISK
- TAKE ACTION
- HOW MDR CAN HELP

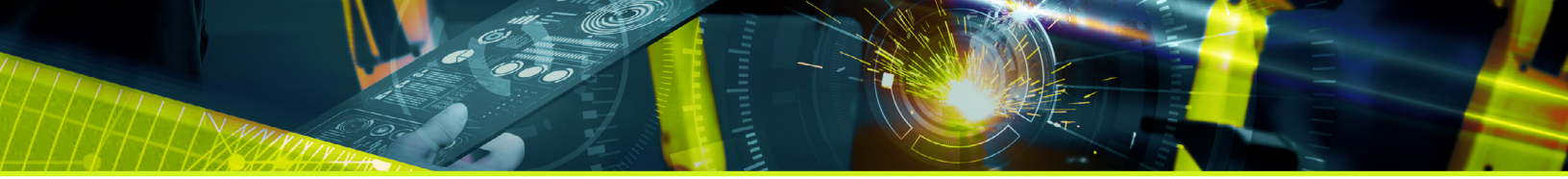
Introduction

Keeping the supply chain secure has always been important, but the added pressures of COVID-19, its impact on consumer behavior, processing time at the border, and changes to what is being produced have served to underscore just how much manufacturers depend on their supply chains. Not to mention the critical steps required to keep the flow of goods and information moving.

The network of partner companies that make up the supply chain has become an increasingly popular means for attackers to gain internal or remote access to data from enterprise-scale companies with poor security practices. With vendors often having access to partner companies' sensitive data or integrations with their systems, supplier-based attacks can prove to be the soft underbelly of otherwise well-defended companies.

If you need to secure your own supply chain, read on for steps you can take. Similarly, if you want to be a trusted supplier, then it is incumbent on you to ensure you are taking cybersecurity just as seriously as larger players, or those who service government customers directly.

To that end, in this whitepaper, we will look at: how the supply chain has evolved, and why; the regulations that have resulted from this evolution like the Cybersecurity maturity Model Certification (CMMC); what these developments mean for manufacturers and small to mid-sized businesses (SMBs) that supply them; what steps they can take to mitigate the risks of the supply chain; and, how a Managed Detection and Response provider like ActZero can help.



New Suppliers, New Roles

Recent years have seen massive growth in both the size and scope of supply chains, which now encompass so much more than the raw materials your organization needs. Data processors that supply or augment information, offer support services such as hosting and remote applications are often outsourced. As a result, not only are there more links in the chain – most organizations likely have more suppliers than they can easily count – but goods and information travels from farther away than ever before. Companies are increasingly responsible for their suppliers' security, given new regulations such as GDPR and CMMC standards. Similarly, breaches have impact across the chain in terms of both notification requirements and financial penalties.

Greater Integration Makes Security Challenging

For manufacturers, special operational technology (OT) running legacy operating systems can be a painful part of vulnerability management programs. Combined with new tools connecting to the internal network such as Internet of Things (IoT) devices, the attack surface is getting larger, and further outside the control of IT. This has also led to much deeper diligence and cooperation between the links of the supply chain. Your suppliers, and their suppliers, are inside your network, and on your systems. They are integrated with your SaaS through APIs, and they are linked to your data center through your website, procurement, and invoicing processes.

This has also led to much deeper diligence and cooperation between the links of the supply chain. Your suppliers, and their suppliers, are inside your network, and on your systems

Why is this a problem? When you have more suppliers, your potential attack surface is expanded, and there are more vulnerabilities to consider. Every integration your providers share brings with it the possibility of exploitation by bad actors. Moreover, the threats aren't limited to your own suppliers: they extend even further, reaching every link along every subsidiary supply chain as well. To top it all off, it's not a two-way street: while your defenses are only as strong as the weakest link in your extended supply chain, your security systems (and thus, your ability to protect that supply chain) reside solely within your own environment. They don't extend to your providers! While audits can offer some control over how third parties secure their systems, audits are also expensive and time consuming to perform.

ActZero

Increased Regulatory Requirements

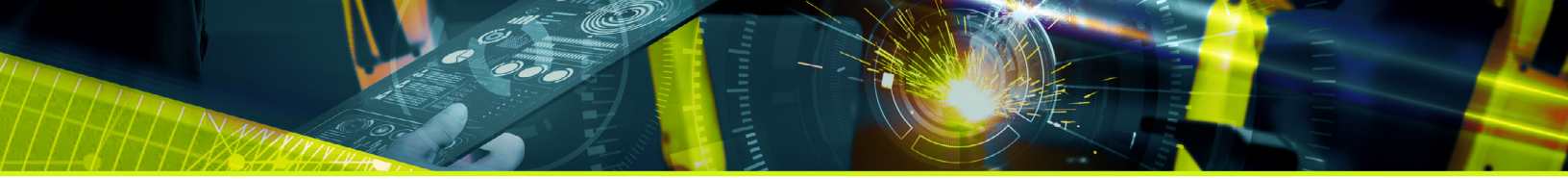
The need to regulate third-party interactions in the manufacturing supply chain has meant the growth of the number and kind of new regulatory regimes. One of the most expansive is the Cybersecurity Maturity Model Certification (CMMC), a new compliance standard spearheaded by the US Department of Defence (DoD).

At its core, CMMC is a unified cybersecurity standard for future DoD acquisitions. It measures five processes across five levels as well as 171 practices across these levels to ensure process maturity and measure the technical capabilities of suppliers.

CMMC is aimed at securing the defence industrial base (DIB)—the network of 300,000+ businesses, organizations, and universities that research, design, supply, and operate military weapons systems. Most of these DIB members are small to midsize businesses, which are the most vulnerable to cyber-attacks. With recent studies suggesting business losses to cybercrime could exceed $5 trillion dollars by 2024, the need to protect the DIB was urgent. One widespread vulnerability within the DIB—leading to potentially devastating losses of intellectual property and controlled unclassified information—was made possible through the multiple interactions and integrations these businesses have with their various suppliers and manufacturers in the supply chain.

Most of these DIB members are small to midsize businesses, which are the most vulnerable to cyber-attacks.

Because the CMMC framework draws on maturity processes and cybersecurity best practices from multiple previous standards, such as the NIST 800-171 framework, it shares many of their requirements. Like NIST 800-171, the CMMC standard mandates that your business could be required to be compliant with the standard even at a three-degrees removed from business with a government agency. Are you doing business with a business that has a Department of Defense (DoD) contract? Then you need to be CMMC compliant if you want to maintain that relationship with the company who has a relationship with the DoD.



Audits – a way for businesses to control their fate?

In a world where breaches and hacks have become commonplace, many businesses are looking beyond the regulations and toward their own audit processes to keep their supply chains secure. In addition to confirming that their internal systems and data are protected, these audits will assess third-party risk (do your diligence!). This should include a regular review of all third-party contracts to ensure not only that all suppliers, vendors, and providers have controls in place, but that all of their suppliers do as well. Organizations will also benefit from recognizing that audits can be especially difficult when your suppliers are operating in different countries, don't have the means to comply with regulations, or simply don't care whether they comply. In such situations, having a plan in place to ensure compliance, or, as a last resort, sever a supplier relationship, will be essential.

In such situations, having a plan in place to ensure compliance, or, as a last resort, sever a supplier relationship, will be essential.

In-house audits offer SMBs several key advantages: they can be conducted on a regular basis, and they can be as stringent as a business feels they need to be. As our security awareness grows on a cultural level, businesses that don't conduct these audits will likely find themselves left behind, even if they aren't hit by a data breach or a regulatory fine.

On the supplier side, perhaps the most cited (or overplayed, depending on your perspective) retailer breach was the 2013 Target hack, in which hackers used stolen vendor credentials to gain access to Target's internal servers and made off with more than 40 million customer credit card numbers.

Tying this back to our discussion of CMMC for manufacturers, we can cite the Boeing "breach" of 2017, in which the aerospace manufacturer lost control of the personal information for 36,000 of its employees when a worker emailed a spreadsheet to his spouse seeking formatting help. While no actual damage was done, in today's regulatory environment Boeing could have faced fines depending on how (and whether) they disclosed the breach.

More Suppliers, Greater Risk

In recent years, of course, supply chains have grown to staggering sizes. Major brands may have tens of thousands of suppliers: Proctor and Gamble lists over 75,000, for example, and Walmart over 100,000. SMBs also find it challenging to maintain knowledge of and control over all their own suppliers, let alone all the suppliers that those companies deal with in turn: a 2018 Ponemon study, showed that only one third of companies could compile a complete list of every third party with whom they shared sensitive data.

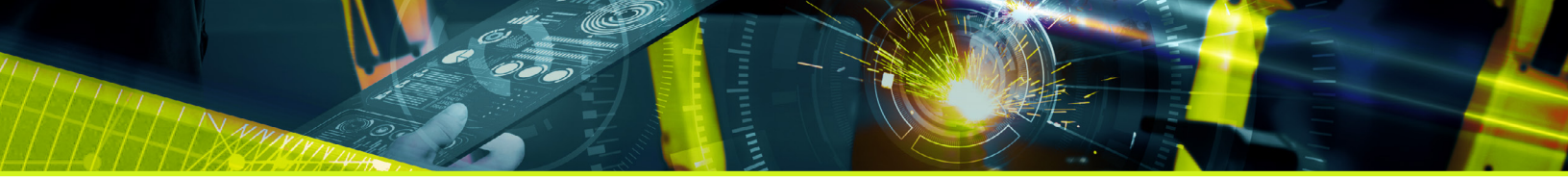
The more suppliers a business has, the more vulnerabilities it faces. Every additional supplier in a chain expands the potential attack surface, and every supplier they work with in turn raises the chance that your business will be exploited by bad actors. And the risks are growing: the Ponemon study also showed that the average numbers of third parties with access to sensitive information rose from 378 to 471. Perhaps we shouldn't be surprised, then, that 56% of organizations had experienced a breach caused by a supplier or vendor.

Here are some notable examples of third-party data breaches in Manufacturing:

- Aerospace company Airbus, which has military contracts around the world, has seen four major coordinated attacks on its vendors since 2018. These include attacks on companies that manufacture engines and technological components for Airbus. At least one of these attacks resulted in unauthorized access to data, and a state-level actor is suspected.

- Also in 2018, computer manufacturer Asus suffered a breach due to a supply chain attack that compromised the Asus Live Update Tool. The malware was accompanied by real Asus security certificates, and nearly 1 million customers had malware pushed to their devices.

- In 2015, tactical goods manufacturer LC Industries experienced a data breach resulting in the loss of more than 3700 customer records due to malicious code embedded in a retail branch of the company.



Greater Risk, Increased Potential for Loss

As the attack surface grows the potential costs of a breach grow as well. A 2019 study by IBM Security and Ponemon Institute found that the worldwide average cost of a data breach was $3.92 million, and that lost business accounted for one third of those costs. The study also showed that third-party breaches increased the average cost of a breach by more than $370,000.

While eye-popping figures like these skew upwards due to breaches suffered by larger enterprises, that doesn't mean small to mid-sized manufacturers are free from risk. These costs reflect the total overall impact on an organization. How much downtime or lost productivity can your business tolerate? To weigh the true costs, you will need to consider the sum of potential impact across areas like these:

Financial

Beyond the immediate costs of responding to a breach and implementing more robust security measures, firms may have to compensate customers if their data is exposed. Staggering fines can be imposed when consumer data is exposed (GDPR allows for fines of up to 4% of a firm's global profits or 20 million Euros, whichever is greater), and breaches can also hit a company's bottom line through falling share prices and valuation.

Reputational damage

Significant data breaches are a leading news story, and while share prices may rebound quickly after the initial shock, the financial impact of lowered reputation and loss of customer loyalty can be harder to quantify. But there will be a cost: a survey of the impact of data breaches on customer loyalty found that nearly two-thirds of customers would end their relationship with an organization if their personal information was exposed.

Operational downtime

If an organization needs to shut down following a breach, the costs can mount quickly. Research by Gartner showed that the average cost of network downtime is $5,600 each minute.

Loss of sensitive data

Beyond the cost of lost customer data, and the potential for class action lawsuits, organizations must grapple with the devastating impact that lost financial data could have. Organizations may also face theft of their own proprietary data, or they may need to pay a ransom to recover or regain access to files or systems.

Cybersecurity Statistics for Manufacturers

Here are some statistics highlighting the problem for manufacturers:

922 incidents, 381 breaches

Greatest vector for attacks – crimeware (e.g., malware such as found in an email claiming a link to a missing package)

Threat actors: 75% external, 25% internal, 1% partner

Actor motives: 73% financial, 27% espionage

Data compromised: 55% credentials, 49% personal, 25% other, 20% payment

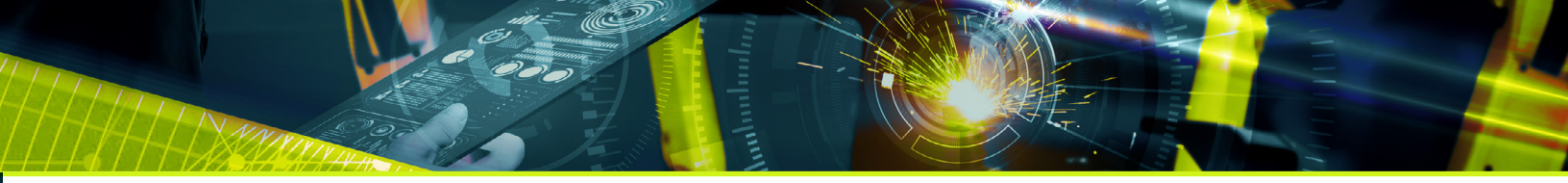
*Verizon 2020 Data Breach Investigations Report

A recent study featuring research by IDC showed that nearly half (49%) of all enterprises have experienced a data breach, and that in the past year, 47% have either been breached or have failed a compliance audit. In addition, the growing importance of Big Data has led businesses of all sizes to embrace the cloud, where half of all corporate data is now stored. Shockingly, the study also reveals that 100% of organizations say that at least some of the data they have stored in the cloud isn't protected by encryption, and that just 57% of sensitive data stored in the cloud is encrypted. Consider the implications here for manufacturers in terms of where their proprietary information is stored.

Given that estimates suggest that approximately 80% of cyberattacks hit supply chains, how much of your sensitive data is at risk from a third-party breach?

As a SMB, you might not feel that this applies to you, but you would be wrong: every business gathers and manages data that can attract malicious attention, not to mention vulnerabilities that are identified automatically by scanners that don't discriminate on business size. The growing interconnectivity of global supply chains has caused an exponential increase in levels of risk.

What is the solution? Businesses must make the protection of their systems a higher priority for the good both of their own operations and those of their partners who make up the supply chain. To do that, you first need to assess the risks. Then, you need to mitigate them.



Assess the Risks to Your Business

Above all, assessing risk means identifying every touchpoint between your organization and your suppliers: every point of interaction, every privileged user, and every integration. This extends to the cases where you are part of the supply chain - every avenue your clients (and even their clients) have into your system must be mapped out.

This is a good chance to conduct an audit of your supply chain and look for vulnerabilities. Even if no obvious issues show up, this is the point at which you need to start making plans. Assume that every touchpoint is vulnerable and put a plan in place with the steps you will need to take to lock down and protect your systems if one of your suppliers suffers a breach. In any disaster, a quick response is essential, so it's also important to make this information available to key personnel.

Finally, even if your own security program protects you from the direct effects of a cyberattack against one of your suppliers, that doesn't mean your business won't be affected. What happens to your manufacturing processes if a key part isn't delivered on time because your supplier's systems have been shut down to deal with a breach? Or if you use a third-party email provider to communicate with your clients, and a breach of their systems exposes sensitive information and leaves your business vulnerable to regulatory penalties or fines?

Even if no obvious issues show up, this is the point at which you need to start making plans.

All these steps involve external risks. But what about internal risks? There are a few types to consider, stemming from your processes, management, or personnel. Business risks that result from disruption of internal processes could include failure to secure an internal network, or an inefficient maintenance schedule that leads to network downtime. There are also potential shortcomings in assessment and planning, risks due to an organizational unwillingness to share or act upon negative data. Finally, there are business risks that result from personnel changes, hand-off processes, or even risks resulting from the actions of specific employees, whether overtly malicious or simply careless.

Mitigate the Risks: Take Action!

Once you have assessed your supply chain risks, the first step in mitigating them is to remove any integrations that are either high risk or low value. While sharing systems can boost your business, in circumstances like these the risks outweigh the benefits, so you will want to shut these down at once.

Your supply chain risk assessment will have identified integrations that are necessary and high value, but this doesn't mean that they don't also pose a threat. Take a critical look at these interactions. Are there levels of access that are no longer needed? Have your current processes evolved in a way that makes some existing integrations redundant? You will also want to examine the security protocols these suppliers have in place, to ensure that you're not exposing yourself to a knock-on risk from a third-party attack.

Finally, consider ways to improve your ability to respond to supply chain risks. You are the expert in your business, but how confident are you at dealing with cyber threats? Does your IT talent pool include a cybersecurity expert? This is where a third-party managed security option can provide a much-needed additional layer of protection. A good security provider will have a dedicated and focused approach to detecting suspicious behavior and will be able to offer a real-time response to threats.

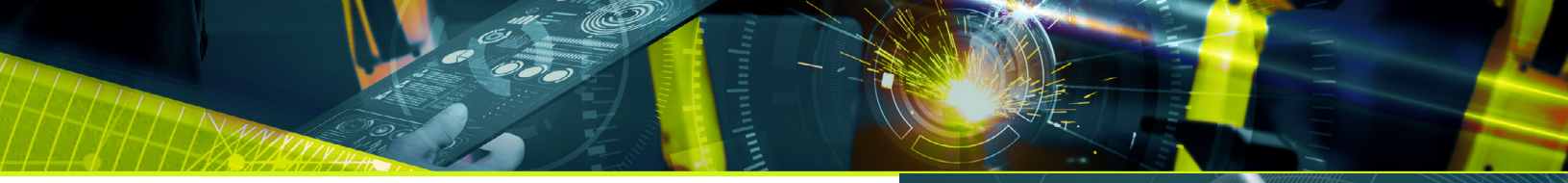
Prioritize and rate your suppliers and vendors
How important are they to your supply chain, and how much integration exists between their systems and your own? Especially for your most essential suppliers, assess the security of their supply chains as well.

Establish clear cybersecurity protocols
According to risk for each level of supplier.

Schedule
Set up an ongoing audit schedule to monitor evolving risks and exposures.

Create a culture of cybersecurity awareness
Not just within your own organization, but within your supply chain as well.

Install an extra level of cybersecurity protection
Work with a third-party managed security provider.



How ActZero's Managed Detection and Response Service Can Help

Our Managed Detection and Response (MDR) service has been specifically designed as a comprehensive cybersecurity solution with organizations like yours in mind. MDR can help your business increase cyber literacy, improve security posture, and adhere to best practices. We do this without requiring you to have in-house expertise, and can do so more quickly and more cost effectively than if you were to develop such capabilities internally.

Ultimately, ActZero's MDR service is about preventing breaches in the first place. Our dedicated Threat Hunters and proprietary AI technology can detect suspicious behaviour and other indicators of compromise as they happen and respond to them in real-time. And if you have been the victim of an attack, we can help determine whether you've lost data or suffered other losses that would necessitate you reporting a breach in accordance with the compliance regulations above.

You can also take advantage of our Virtual CISO (vCISO), to help address specific policy and compliance challenges. Your vCISO will be an experienced security leader that can advise you on the technology and tactics you need to harden your systems, remediate vulnerabilities, and mitigate compliance risks.

ActZero

To find out more about how ActZero's MDR solution can help your manufacturing business overcome threats to your supply chain, and comply with regulatory requirements in the manufacturing sector, contact us.

ActZero | ActZeroAI | ActZero.ai

www.ActZero.ai/contact

TORONTO
207 Queens Quay, Suite 820
Toronto, Ontario M5J 1A7

MENLO PARK
2882 Sand Hill Road, Suite 115
Menlo Park, California 94025

SEATTLE
925 4th Ave., 20th Floor
Seattle, Washington 98104