SOCURA

Cyber Security in Manufacturing

“Manufacturing businesses will continue to be a very attractive target to cyber criminal groups due to their soft underbelly. Attackers know the devastating effect of their campaigns and the high likelihood of a quick payday.”

JAMIE BRUMMELL – CTO & FOUNDER

FOREWORD:

A Well-Oiled Machine?

The cyber security challenges facing the manufacturing sector cannot be overstated – in terms of scale, complexity, and urgency. Manufacturers are a highly attractive target for attackers, they have complex IT estates to secure, there are severe consequences when they are breached, and many are woefully mismatched against attackers.

Toyota is a perfect recent example of cyber security complexities and their consequences. In 2022, a data breach impacting a single plastics suppliers put the brakes on Toyota's global production. The recovery was protracted and complicated, because the knock-on effects of a data breach in this scenario are so extreme. There is no room for error with just-in-time production control systems, and this incident delayed the production and sale of tens of thousands of cars, at great financial and operational cost to the company. Most factories have this issue, and an urgent need for digital assets to be protected. There are also challenges around basic cyber security hygiene, Mergers and Acquisitions (M&A) activity, patching, insider threats, espionage and employee training.

This makes a mockery of the notion that the manufacturing sector is a slick, well-oiled machine where tasks are completed like clockwork with man and machine working together. Even the most modern and technologically advanced sites have operational, technical and personnel issues that make operational priorities like cybersecurity a lot more complex, and a lot more chaotic, than outsiders imagine.

Andrew Kays, CEO

AUTHORS

Andrew Kays,
CEO
Andy is the CEO at Socura where he is responsible for delivering and optimising the company's services. He has over 20 years of experience growing and managing cyber security companies and specialises in building high performing teams to deliver outcomes for customers.

Jamie Brummell,
CTO & Founder
Jamie is a cyber security leader with over 20 years of experience working with multinational organisations, security vendors, and systems integrators. Jamie works with senior executives, architects, analysts, and engineers alike; helping them manage cyber risk and improve their cyber defence capability.

Marc Chang,
NED & Founder
Marc is passionate about building teams and organisations that at their heart use technology to bring positive change to society and improve people's lives. He founded Socura to help organisations address the rapid rise of cyber security threats and make the digital world safer.

Contents

A Special Case

When there's a major breach, emerging threat, or new vulnerability, manufacturers are over-represented among the victims. They are also hit hardest in terms of the operational and financial impact of cyber incidents. In manufacturing, any disruption can wreak havoc with just-in-time delivery methods. There's also the risk that hacked systems could lead to catastrophic events that put employee and customer safety at risk.

Indeed, the industry research on cyber security in the manufacturing sector makes for grim reading.

Half of British manufacturers have been the victim of a cyber attack in the last twelve months. During this time, the industry also spent more than any other sector on ransomware payments. It paid 62% of the ransoms transferred to cyber criminals in a single calendar year, according to research by Kivu Consulting, despite manufacturing only representing 18% of cases.

Manufacturing organisations must contend with internal and external threats simultaneously. In a sample of more than 120 manufacturing industry breaches, 28% were found to be motivated by espionage. It's common for external actors to target employees with attacks that trick them into handing over key credentials, data and systems access.

Kaspersky research indicates that nearly a fifth of organisations impacted by the SolarWinds supply chain attack were from the manufacturing sector.

Approximately 50% of manufacturers said that cyber security has become a higher priority since the start of the Covid outbreak, and 61% of companies revealed that they now have a designated board director responsible for cyber protection across the whole of their business.

Over the course of this paper, we'll review 3 of the biggest challenges facing manufacturing business leaders and we'll detail how they can harden their defences, improve security processes, respond to cyber incidents more effectively and limit the damage done.

Basic security hygiene – what's stopping us?

It's hard for manufacturers to get on the front foot against potential attackers and adopt the latest security controls used by other industries such as finance when they are in a state of 'technical debt'.

CISOs will be acutely aware of AI, biometric security, automation tools, and will want to invest more in security. However, their priority for the foreseeable future will be basic security hygiene, rather than cutting edge technology. Their technical priorities are as follows:

- **Patch management** – patching devices that could be an entry point for attackers otherwise
- **Locking down machines** – securing devices that weren't built with security in mind
- **Threat detection/response** – detecting breaches early and mitigating their impact

Patch management

Manufacturing is a data rich sector, and this data is used as an intelligent resource to guide decision-making and optimise operations. It's one of the reasons that modern manufacturing companies have hundreds, if not thousands, of connected devices and industrial controls on site. Unfortunately, each one is a potential entry point for attackers, or a point of failure if they are not kept up to date and secured.

Patch management is therefore essential for security teams, ensuring that known vulnerabilities are identified and fixed continuously. However, old and outdated machines are a major problem. Even manufacturers at the cutting edge of robotics and Internet of Things (IoT) tech will usually have some legacy machines on the floor too. Often these are machines that are too old to be updated with the latest security patches, but too expensive or important to be replaced. Many won't have been designed with cyber and data privacy in mind. In critical infrastructure and manufacturing, sometimes devices cannot be updated and restarted because organisations cannot afford the downtime.

When you work in an environment where you cannot patch, then the primary solution must be segmentation. Rather than "patch, patch, patch", the correct motto should be "segment, segment, segment." The Purdue model for separating layers of technology in fields like Industrial Controls (IC), Supervisory Control and Data Acquisition (SCADA) and IoT has existed for a long time, and has stood the test of time because of its effectiveness.

Locking down machines

ICS/SCADA equipment is behind the curve when it comes to security, and could never be described as “secure by design”. To make matters worse, ICS/SCADA systems rely upon niche protocols which were designed to work effectively in environments with low computational power. Infosec was never a consideration in their design. These niche protocols can present challenges to standard infosec tooling.

Manufacturing also has a device variety and complexity issue that is a very different to the average office workplace. It is not a simple case of securing a laptop, PC or smartphone per employee plus a few other connected devices – which can all invariably run similar platforms and security controls. Factories have myriad connected devices of every size, shape, purpose, and manufacturer. They may be accessed more easily and readily than the CEO’s laptop, they can be damaged on site, and getting data from these devices to see if they are behaving as expected isn’t always straightforward.

Threat detection and response

For manufacturing security teams, the pursuit of future perfection cannot come at the cost of achieving good security processes in the here and now. This can mean ignoring more advanced security tools in the short term and focussing on the basics that align with business priorities – namely ensuring that cyber incidents do not impact a factory’s ability to run on schedule and on budget.

Effective threat detection and response hinges on an organisation’s ability to detect threats and potential cyber incidents in their infancy. It also means having a detailed plan in place to respond to breaches, and what the company will do in the event of a ransomware attack, for example.

It should be noted that the manufacturing industry is estimated to have spent more than any other sector last year on ransomware payments. This suggests that the industry is a primary target, due to its soft underbelly. Few manufacturing companies have a plan for how to combat the threat beyond paying the demand.

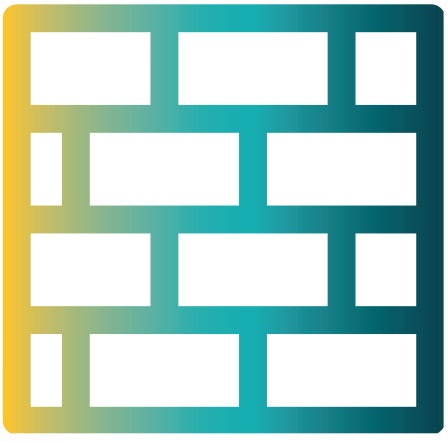
The priorities and issues for security teams in manufacturing

The priorities of manufacturing bosses and security teams broadly align. Both want to eliminate downtime and ensure that sites and teams run as efficiently as possible. However, there are other business priorities and unique business models used in manufacturing that can become major issues for security teams.

M&A increases complexity and attack surface

M&A are extremely common in manufacturing, which inevitably introduces new people, new systems, and new technologies to an organisation's operations. Suddenly, a security team may be responsible for securing a whole other company, site, or even an entire region. Management naturally wants to break down silos as quickly as possible. They want everyone and every department to be using the same tech, processes and systems as each other for the sake of efficiency. However, security teams know that each new department adds to their IT scale and complexity, increasing their potential attack surface even further. Their primary concern is that a potential a breach in one of these previously unconnected departments can have serious ramifications for others. They may also be inheriting the IT and security issues of another company, on top of their own problems.

It's vital that security teams have complete oversight of the entire estate, no matter how big it has grown. They must have the controls put in place to analyse traffic, spot malicious activity and limit traffic 24/7. Often this Security Operations Control is outsourced if a manufacturer does not have the skills or manpower to monitor this activity in house.



Use of Systems Integrators can obstruct security

A common security issue in manufacturing stems from the use of Systems Integrators (SIs). Vendors are generally abstracted from customers by a SI, who often have a rudimentary infosec understanding. Even through vendor knowledge is improving, that is effectively nullified by the SI.

When a production machine is installed by a SI, it will often be delivered in an insecure, yet functionally tested state. The systems integrator may not allow patching irrespective of the Common Vulnerability Scoring System (CVSS) score of a vulnerability present within their software. They are too concerned by the extensive regression testing required.

Whilst the likes of Rockwell and Siemens are making significant strides forward and demonstrating that they understand that whether they like it or not, at the point you cut any code, you have an inherent infosec responsibility for that code, most ICS/SCADA manufacturers have not yet had that realisation.

Remote access is another thing that both management and SIs insist upon (after all they want their production line back up and running ASAP when there are issues), however very few SIs can deliver remote access in a secure manner. A prime example of this is the Adige breach last year. Only one of their customers (with active remote access) was not subsequently breached and that was because they had insisted on using their own brokered remote access solution.

It all begins and ends with one thing... our people

Manufacturing's people problems broadly reflect its connected device problems – namely scale, variety, and complexity. Manufacturing employees are a varied group, including on site, office-based, and roaming employees, as well as third-party contractors and suppliers. Most workforces are not chained to their desk and a single device, and it's likely that they are less IT security savvy than their office counterparts who spend more of their time online. Manufacturing also has a physical security/access issue. People need to move freely on site and between multiple locations and devices, while simultaneously ensuring that devices are only accessed by people with the right permissions. Again, all this creates a large attack surface for cyber criminals.

The sector is plagued by a shortage of skilled ICS/SCADA infosec professionals. All sites need experienced people who understand that the normal rules of "patch, patch, patch" don't always apply. All employees need formal training in how infosec works in an ICS/SCADA environment.

Meanwhile, there is also the insider threat issue. Manufacturers often have extremely valuable IP that may be the result of years of Research and Development (R&D). It's often an organisation's most valuable asset, and its theft is among the most damaging potential consequences of cyber incidents in the manufacturing sector. Indeed, manufacturing executives have cited IP protection as their primary concern.

The theft of IP is a human issue as well as a technical and process challenge. It is such a lucrative target for competitors and cyber criminals alike, that it is common for them to target someone on the inside to give them the access they need.

Manufacturers struggle enough with outside threats to their organisation – such as ransomware gangs. Identifying or preventing insider threats is more difficult in many respects. These are users with easy access to devices, permissions to view and change files, who are known and 'trusted' by security teams and their defensive tools. If they are compromised, if they share confidential details, grant access to attackers, or are impersonated by attackers – they are very difficult to stop.

According to Verizon's Data Breach Investigations Report, 28% of manufacturing industry data breaches were motivated by espionage in 2021.

To combat personnel issues and insider threats, manufacturers should prioritise regular employee training sessions so that staff know how to identify phishing attempts and what to do if they receive any suspicious communication. The ability to monitor all employee devices and detect unusual activity among staff is also vital. Companies need to know if someone is accessing files or machines that they are not permitted to use, or don't usually. Likewise, they need to spot abnormal behaviour that may indicate an insider threat, such as downloading files en masse, or accessing files from another location/out of office hours. These are all activities that warrant closer scrutiny and investigation.

How to combat cyber security risks

The manufacturing sector urgently needs to harden its defences. Cyber incidents are hugely disruptive and costly, the sector cannot remain such a seemingly soft target to attackers, and businesses need a more robust and effective policy than simply paying them off.

When it comes to detecting and responding to advanced threats, we would recommend the following principles:

1

Discover assets

Understand what assets and valuable IP your organisation holds. A regularly updated inventory is essential to accurately catalogue assets. You can't protect what you can't see.

2

Segment what you can't patch

If you can't patch machines, ensure they are segmented. Follow tried and true models such as Purdue to guide you on this journey.

3

Detect immediately

If you're struggling to hire in house security analysts and build an effective Security Operations Centre (SOC), invest in services that can analyse this telemetry and spot anomalous patterns indicating unauthorised activity. These services should be capable of acting upon detections in near real-time and containing confirmed threats.

4

Respond swiftly

Paying a ransom is not a advisable, sustainable or effective approach to dealing with cyber criminal threats. It's important to respond swiftly and decisively in the event of a cyber incident – to mitigate the impact as much as possible

The value of MDR

Socura offers a Threat Detection and Response managed service, often referred to as MDR. It is perfectly suited to the manufacturing sector, due to the skills shortage in the sector and MDR's ability to ingest and analyse huge amounts of data.

Expert analysis outsourced

Socura's MDR service acts as a trusted extension of your in-house capability and is operated by a team of highly experienced security experts. Our analysts work in partnership with you to detect and defend against cyber threats.

We operate a best-in-class service that monitors your environment 24/7 looking for signs of malicious activity and, upon discovery, taking action to contain and eliminate the threat. Critically, we also determine the root cause so that we can stop the same attacker returning or the same intrusion method being used again.

Our people-centric approach is what sets Socura apart. Technology can only take you so far and legacy approaches of building centralised SOC environments can greatly restrict the analyst talent pool available based on their proximity to a specific geographic location. In an industry where experienced SOC analysts are in short supply, compromises are made.

At Socura we've tackled this head-on by building a nationally distributed, fully remote SOC environment in which we can recruit the best talent from any location. This optimises the experience for team members and clients alike and frees us to select, train and mature the best talent in the industry.

Tight integration with enforcement points also enables Socura to respond to threats quickly and apply the knowledge gained through our investigations to detect similar potential attacks in the future.

Unlimited data analysis

Socura's MDR consumes all of your security telemetry, with no limit on volume, and use the latest advancements in security analytics technology combined with a highly skilled and experienced team to analyse your data, identify what's bad, and take action to stop it.

Data volume can be a critical barrier to effective threat detection & response in the manufacturing sector. Growing infrastructure, more applications, and more security tools have resulted in data volumes that are higher today than ever before.

This has meant that significant infrastructure investment has been needed to enable scalable and swift analysis of security-relevant data. Mean Time to Detect (MTTD) threats and Mean Time to Respond (MTTR) to threats – key security metrics – suffer without this capability.

Conversely, security analytics pricing models have traditionally been based on volume, incentivising you to limit the collection and analysis of security-relevant data, therefore reducing your threat visibility.

Socura has broken this traditional pricing model and offers unlimited security analytics + log ingestion. With Socura's MDR service, there are no such compromises. We can ingest all of the security data that your systems generate, resulting in complete visibility across all relevant data sources. This data is retained for 12 months, whilst remaining hot and searchable in milliseconds, meaning we can also instantly and retroactively match newly discovered indicators of compromise against your entire historical telemetry dataset.

If you would like to find out more about how we can help you, please contact the team at hello@socura.co.uk

While we no longer have the distasteful task of clearing dead bugs from giant computers, new, complex challenges emerge every day for manufacturing security teams to contend with.

While great strides have been made in recent years in regards to security controls and resources, we have to admit that most organisations in this sector are not ready for them yet. There is a messy reality to contend with now, but doing so will ensure that cyber incidents do not impede an organisation's ability to deliver goods and services on schedule and on budget.

JAMIE BRUMMELL – CTO & FOUNDER