SOPHOS
Cybersecurity delivered.

Cybersecurity in manufacturing

A Sophos Whitepaper. August 2022

The changing face of manufacturing

The story of manufacturing is one of constant technological change and evolution. It is also a story with a sweeping geopolitical arc from the industrial revolution in 19th century Britain to modern day China accounting for nearly 30% of the world's manufacturing[1]. The march of the machines is relentless and for large portions of society, alarming. Today's technology is even imbued with the ability to learn – Blake Lemoine, a software engineer at Google, believes a chatbot his firm has created is capable of conscious thought[2].

The past ten years have seen dramatic technological steps forward in manufacturing, not least in the development of AI and big data. Machines are not quite sentient, but the potential for this to happen has moved from the realm of science fiction into a possible and uncanny reality. These developments, in combination with greater levels of automation, lightning-fast ubiquitous global communications networks, and developments in 3D printing, are creating the era of the smart factory[3].

The future of manufacturing is smart and exciting, but it is just as uncertain today as it was centuries ago. With an absolute reliance on technology though, it is a very appealing target for cyber-criminals.

The changing face of technology in manufacturing

There are far fewer people and a great many more machines in manufacturing. Furthermore, in markets where labour is comparatively more expensive, there has been a steady drop in the economic influence of manufacturing. For instance, in the UK, manufacturing's share of economic output in GDP has been in steady decline from 27% in 1970 to 10% in 2018[4].

This is massive oversimplification, of course, manufacturing is a broad church. There are plenty of examples of successful UK manufacturers. It should also be noted that the level and type of technology, automation, and connectivity, varies from sector to sector whether it is foods, pharmaceuticals, automotives or aerospace. Production line automation also varies according to where in the world an organisation is based[5] – an issue that is complicated further by the fact that many large enterprises have a global footprint. But wherever it makes economic sense to replace a human with a robot, it will happen.

These automated systems represent an obvious target for cyber criminals. They don't need to take down an entire production line, in fact they're unlikely to even try. All they need to do is throw a digital spanner in the works. Cyber criminals are much more likely to tweak a small part of a process. This could be something in the production line that doesn't bring manufacturing to a complete halt, but does result in reduced efficiencies or faulty end-products. They might even let the breach continue to run unchecked for a prolonged period of time before informing the manufacturer that they've been producing faulty goods.

The impact of this will vary from industry to industry, and product to product. For instance, in automotives with vehicles becoming ever more connected and automated themselves, if a cyber-criminal can affect a car's internal electronics, that could ultimately cost lives.

1 These are the top 10 manufacturing countries in the world
2 The big idea: should we worry about sentient AI?
3 Information Technology Gartner Glossary – Smart Factory
4 United Nations Conference on Trade and Development (UNCTAD) data, accessed November 2017
5 10 most automated countries worldwide

Other areas of weakness that manufacturing has in common with other sectors are confidential internal data, customer data and intellectual property (IP). With far fewer humans involved, employee data is perhaps not the number one target, and given manufacturers are operating in a B2B world, there is a lot less customer data to consider. But corporate espionage including the targeting of critical IP is not unprecedented.

Finally, as with other sectors, a manufacturer's supply chain also represents a major point of weakness. The advent of 'just in time' delivery where everything is automated, tracked and traced, and even raw materials are barcoded, offers up plenty of weak links prone to cyber-attack. If a supply chain system fails in some way, it can cause chaos and would take a manufacturer a long time to recover.

The increasing cost of cybercrime to manufacturers

According to Sophos data, 55% of manufacturers were targeted by cybercriminals in 2021[6]. While this is lower than a cross-sector average of 66%, Sophos also found the average ransom pay-out, at $2 million, was higher for manufacturers than any other sector, far above the overall average pay-out of $812,360. So, while manufacturers are comparatively slightly less likely to be attacked, it will cost them far more when it happens. And we're not even talking about the loss of earnings or reputational damage they might incur.

In June 2022, the UK's largest ready-meal provider, Wiltshire Farm Foods, was crippled by a cyber-attack[7]. The ramifications of the attack extended beyond financial loss and into the community because it caused issues for the delivery of a service that brings food to the elderly and vulnerable, Meals on Wheels. Attacks like this and those on healthcare providers demonstrate cyber-criminals are not especially compassionate.

Cyber-criminals are not always motivated purely by financial gain. This motivation could arguably cause an organisation much greater harm since there is no option to even pay a ransom. For instance, one hacktivist group, calling itself Predatory Sparrow, has been targeting a variety of organisations in Iran claiming companies were continuing to operate despite international sanctions. Predatory Sparrow attacked Khouzestan Steel Company (KSC), one of Iran's largest steel manufacturers, this June[8]. Manufacture was brought to a complete standstill. The impact of this extends far beyond Iran's borders. The firm exports to 13 countries, 50% to the Middle East and North Africa, 40% to the Far East and around 10% to the Americas[9]. Those customers in turn are producing parts and goods destined for secondary markets in Europe and North America.

Supply chains are truly global, in the case of KSC as steel production drops, prices for their customers globally will inevitably rise. The importance of supply chain security came to the fore recently in the automotive sector. In March 2022 Denso - a global supplier of automotive components – was targeted by ransomware attackers[10]. Denso has major customers around the globe including the likes of Ford, GM, Honda and Toyota. It only takes one missing part to bring production to a halt.

There are countless examples of how manufacturers around the globe are finding themselves under attack from cybercriminals, which emphasises the need for them to prioritise strengthening their defences against ransomware. Investing in modern infrastructure, together with cybersecurity technology and skills, will considerably reduce both the overall cost and impact of ransomware.

6 The State of Ransomware 2022
7 Meals on Wheels Disrupted by Suspected Ransomware Attack
8 IOTW: Iran's steel industry targeted by hacktivists
9 Iran's Largest Steel Exporter Sets Record
10 Automotive giant Denso confirms hack, Pandora ransomware group takes credit

Cybercrime is a multi-layered threat

The threat posed by ransomware attacks is extremely damaging for manufacturers. In terms of security awareness and protection, the sector has a diverse outlook. Some ultra-modern production lines are well protected, but others take the approach that if it's not broken it doesn't need to be fixed – these organisations find themselves running outdated and fragmented IT infrastructures supported by overstretched IT teams. As a result, in the wake of an attack they are often forced to totally rebuild from the ground up, incurring major financial cost. When balancing usability against cost and protection, it is far wiser to bake security in at the beginning of a process rather than retrofitting it to patch up a vulnerability. However, the speed of deployment often means security can be an afterthought.

In today's world, it is no longer enough to simply deploy antivirus software across networks and expect to be protected. Malware and hacking used to be two different threat landscapes; however, they have merged over the last five years.

Attackers are stealthy – if IT teams don't play an active part in looking for signs of a breach, then cybercriminals can use (often legitimate) tools to enter and move around a network undetected, simply waiting for the right opportunity to strike.

'Hands-on attacks', where the adversary goes interactive within an IT estate, are becoming increasingly common and can unfold at lightning speed, quickly overwhelming systems and staff. If this happens, it's crucial that a manufacturer has the expertise to respond rapidly at any time of day or night and bring in incident response services to assist.

Social engineering, for example phishing, is an often-overlooked area of weakness, yet it has been identified as being a precursor of up to 98% of all cyber-attacks[11]. Some organisations will invest resources into software that looks good on paper and makes people feel secure, but they don't do anything about the human element, which has been identified time and again as the weakest link in a security chain.

Barriers to transformative security

The manufacturing sector is not only open to technologies that provide an edge over rivals, it is driven by this competitive force. However, taking a production line offline to update security is a major cost. If a production line is working, a manufacturer will be loath to take it offline to install the latest security patch, partly driven by the fear that it might not work properly again. It is not unprecedented for manufacturers to find that their solutions are completely out of date due to this inertia.

Another barrier comes with digital transformation. The manufacturing sector, as with most other verticals, is undergoing huge digital transformation. This will ultimately result in more data being shared across networks and greater commonality of systems. Which in turn will result in more points of weakness and more cybersecurity risk as changes take place.

Leadership teams are faced with three key, immediate challenges with digital transformation. First is the complexity of the existing or legacy platforms and software across a fragmented landscape. Second is the requirement to address security and compliance - the immediacy of this requirement can lead to quick fix solutions, which does not help with long term challenges. The third challenge is a lack of skills with new technologies such as cloud, AI and cybersecurity.

Coping with these challenges is a major headache for manufacturers. Mergers and/or acquisitions are not uncommon in the sector as organisations strive for growth. This can add even more pressure on staff at a time when many firms are streamlining and centralising IT teams. Network managers working a broadening landscape find themselves under increasing pressure.

Manufacturers are therefore increasingly looking to managed service providers to help with these challenges. As the strategic importance of technology increases in line with its complexity, the role of the IT professional is moving up the value chain, from implementation expert responsible for building, deploying and maintaining solutions, to technology orchestrator responsible for long-term goals and strategy.

11 Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2022

Taking a long-term approach

Security, like insurance, is something you hope you never need, but absolutely must have in place from a compliance perspective and to manage risk. In fact, manufacturers would be well placed to work on the assumption that an attack will happen and ensure they have a tried and tested incident response plan that can be implemented immediately to reduce the impact of the attack. Complicating matters, threats are constantly evolving as criminals try new avenues of attack against the latest security.

The National Cyber Security Centre (NCSC) has made it clear that supply-chain security weaknesses make organisations highly vulnerable to attack. Manufacturers should mitigate this risk by reviewing their existing suppliers' cybersecurity measures immediately and for future contracts, build in security requirements from the start.

Too many cyber breaches are caused by the inadvertent actions of users. Therefore, it is important that users are educated about the cyber risks they face and the safeguards in place to protect them. They should also understand their individual cyber security responsibilities, be aware of the consequences of negligent or malicious actions, and work with other stakeholders to identify ways to work in a safe and secure manner.

Avoiding breaches – the cybersecurity solutions

Taking a proactive approach to cybersecurity is vital. Manufacturers are faced with the choice to either manage IT themselves or outsource. Most do not have the budget, tools, people, and processes in-house to effectively manage their security programme around-the-clock while proactively defending against new and emerging threats. Furthermore, manufacturers who do invest in cyber security solutions often fail to deploy them fully or use them to their full potential – significantly reducing their effectiveness and increasing the likelihood of a successful, but preventable breach.

For an organisation to mount an effective defence against cybercriminals, IT teams often use Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) tools that monitor and scour the network for suspicious behaviour. However, it takes time and expertise to use these tools effectively and investigate the numerous alerts that require triaging, burdening already overstretched IT staff.

In these circumstances, a Managed Detection and Response (MDR) service is an ideal solution. At Sophos, a human-led threat hunting team works together with AI technology to hunt, detect and respond to suspicious activity 24/7/365, while maintaining an ongoing dialogue with IT staff. More than just a notification service, the team's level of involvement is entirely within an organisation's control – from validating threats and removing all the 'noise' of false positives to carrying out targeted actions on an IT team's behalf. Sophos threat hunters are so familiar with malicious behaviour, that once detected, the issue is often resolved within the hour.

Conclusion

With a continually changing threat landscape and limited budgets, securing manufacturers against cyber-attacks requires a collaborative team effort. By working together with your organisation, Sophos can provide the best opportunity to minimise security incidents and keep data safe as digitalisation continues apace.

Having a specialist MDR team in your corner at all times – whether they're needed in the middle of the night, at a weekend or during holidays – ultimately provides you with peace of mind, knowing you're doing all you can to keep your organisation safe, and up and running.

Sophos MDR offers different levels of support, giving your business options around the control you wish to retain or hand over to our team. Plus, there's a wide variety of trusted Sophos security products that work side-by-side with MDR, all managed from within the Sophos Central platform for total visibility of your estate. Choose from Standard or Advanced Sophos MDR[12] – whatever you decide – you'll be safe in the knowledge that our dedicated security personnel will identify and eliminate threats before they can even become an issue.

As in many other sectors, manufacturers must adapt to the acceleration of cyber-risks - but without panicking. Being a target is now a fact of life, but becoming a victim is not.

12 https://www.sophos.com/en-us/products/managed-threat-response/how-to-buy

Learn more about ransomware and how Sophos can help you defend your organization.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2022-08-23 (WP-NP)

SOPHOS