THE NEXT INDUSTRIAL REVOLUTION

Andrea Carcano *and* **Chris Grove** *examine the growing significance of cybersecurity to automated manufacturing*

In Germany it's called Industry 4.0, in Japan it's Society 5.0, while the Chinese Government has recently been talking up an economic plan called Made in China 2025. While not exactly equivalent to one another in every detail, what each of these has at its heart is the central importance of manufacturing for the future of the digital economy.

It sounds paradoxical: aren't future economies supposed to be driven by services and the free-flowing movement of data? In fact, making things, and particularly the way things are made, has never been more important for the future of economies. However, what each of these initiatives stresses is that the future of manufacturing will involve integration between the digital world and the physical world where raw materials are processed into goods, including those on which the service economy depends. It's most explicit in Industry 4.0, which proposes that this integration should form the basis of a fourth industrial revolution based on high levels of automation, smart manufacturing, optimisation of Operational Technology (OT) and logistics, all driven by the expansion of big data analysis, real-time data collection, and machine learning.

As impressive as this sounds, the issue it fails to address is the ways that the extraordinary surge in cyberattacks over the last decade might put these visions at risk. Some of this is simply an extension of the same risks business in all sectors face, namely that cybercrime has turned into a huge and rapidly expanding industry that threatens everyone. But for anyone who embraces the concept of Industry 4.0, or simply sees automation and digitalisation as the next incremental gain, it's clear that a future built on technologies now being targeted by cyberattacks is inviting a huge level of business risk. Even now, the full scale of this added risk is hard to calculate, predict or mitigate. It's as if global companies and their supply chain must invest in expensive new technologies, protecting their business plans with nothing more than crossed fingers.

A future built on technologies open to cyberattacks invites a huge level of business risk

Although cyber incidents affecting manufacturers are rarely publicised, glimpses of what is happening occasionally emerge in third-party reports. One of these, based on customer data analysed by IBM's X-Force threat intelligence platform in 2019, noted a large increase in deliberately destructive malware attacks, 50 percent of which were against manufacturing companies. The malware behind these attacks were all tied to large ransomware campaigns, which have increasingly threatened to damage victims as part of a business model built on extracting large ransoms from the stricken.

Another cybercrime that caught out manufacturing was Business Email Compromise (BEC), where servers, email accounts and telephone systems are compromised to carry out invoice fraud involving foreign supply chains. And all this is before considering traditional cybercrimes that have been evolving over the last 20 years such as the theft of intellectual property, which manufacturers still cite as a constant worry.

While disparate, these attacks underline common themes for anyone tasked with defending the networks on which a manufacturing company depends. The first of these is that they are all highly targeted. Although that's also true for every company in every sector, it is something the manufacturing sector is unusually vulnerable to. All companies protect their networks and data, but in manufacturing this is also about sensitivity to timing, delay and a resource not being available when needed. Attackers understand this means they need only successfully compromise one element of a network – invoicing or email systems for example – to bring whole production lines to a standstill.

PROBING FOR WEAKNESSES

Targeting isn't just about who is targeted but what is targeted too. Ransomware campaigns now employ extensive reconnaissance designed to probe for weaknesses, often penetrating networks via weakly secured software interfaces such as company Virtual Private Networks (VPNs) or remote support or diagnostic ports, often months before a demand for money is made. Defending against this sort of threat requires careful attention to network design, but it's often difficult to know where the weaknesses are until it is too late. The critical issue is visibility, the very thing that turns out to be hard to achieve.

A second issue is that although the distinctive aspect of manufacturing companies is their specialised Industrial Control System (ICS) and production networks, everyday weaknesses in business IT systems can still be their undoing. The infamous examples of this are the WannaCry and the NotPetya attacks of 2017, which targeted Windows computers and brought numerous manufacturing companies, including Nissan, Renault, food manufacturer Mondelez, and pharmaceutical giant Merck, to a partial standstill. It didn't matter that only some of the computers were in production environments when those environments depended on the smooth working of IT to function.

Far from being the separate entities they once would have been, IT and production networks have become increasingly connected to one another. This makes sense from an operational point of view because it allows a single IT team to manage production systems as an integrated resource, but it opens those systems to attack in ways that are difficult to anticipate. An oft-cited early warning of the bleak possibilities came in 2014 when the German Federal Office for Information Security (BSI) revealed that a cyberattack had been able to cause damage to the ICS systems used by a German steel mill using nothing more sophisticated than a phishing campaign. This gave the attackers access to credentials for the mill's ICS systems, accessed remotely after compromising the main network. This resulted in failures that caused major damage to the mill's furnaces.

The attackers were not identified, nor their motivations, but its likely at that time it was simply a dry run to test out the possibilities of causing real-world effects in ICS and production system. These days, attempted attacks of this type are so routine that motivation – to aid ransom demands, as a way of creating a diversion while data and IP is stolen, for economic advantage or simply to further the geo-

THE VERY THING THAT MAKES MANUFACTURING EASIER IS ALSO WHAT MAKES IT VULNERABLE

political aims of a nation state – almost seems like a secondary worry. What matters is it is possible at all.

For years, industrial networking an ICS was based on proprietary OT systems, many of which have proved expensive and prone to serious software vulnerabilities, which were hard to patch – assuming such a thing was even available. Many of these were also specified before cybersecurity became a big concern and depended on remote access via third-party management, which added risks. However, despite inadequate cybersecurity, what is driving migration from these systems to Industrial Internet of Things (IIoT) is the need for greater automation, monitoring, efficiency and lower costs. For companies investing in a new generation of Manufacturing Operations Management (MOM), this is largely competitive and isn't something manufacturing companies can simply choose to opt out of.

Operationally, OT and IIoT covers a wide range of technology, including SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems), sensors and machine-to-machine communication, which are now typically mixed to create complex, inter-dependent networks. But adding IIoT doesn't just add to the security challenge, it changes it in important ways. IIoT technologies have emerged chaotically alongside consumer IoT and are built on common platforms and protocols, which means they offer a similar set of potential security weaknesses as the same technology used in a non-IIoT setting. The very thing that makes it easier to manage and cheaper from a development point of view is what also makes it vulnerable. Realising manufacturing control systems are increasingly built

around common technologies, attackers can now look to deploy simpler exploits that require even less customisation.

As with IoT, the industry behind IIoT underestimated the need for security, which has resulted in many first and second-generation hardware suffering a range of vulnerabilities in their configuration and software design. Once in the field, these are not easy to remediate, particularly where shutting down sensors and devices would cause production problems. For many organisations, the scale of vulnerability in the equipment requires a level of visibility they have no way to achieve.

It has become clear that the longer organisations fail to address the challenges the digitalisation of manufacturing throws up, the more difficult it will be to address. This isn't so much a nuisance for manufacturing in the age of Industry 4.0, but a mortal challenge to it. If organisations invest in IIoT and process automation to gain the benefits, this can't come at the expense of opening themselves to the likelihood of major cyberattacks that hold businesses, or parts of their supply chain, to ransom. Some have proposed cyber-insurance as a form of risk mitigation, but this increasingly imposes limits on payouts and demands in terms of cyber-resilience that can be as expensive to meet.

Longer term, meeting this challenge can't be done piecemeal and requires overlapping defences to work together in a unified way via a single management system. Far from reverting to the past and naively isolating industrial networks, it makes more sense to integrate them in a secure way. Organisations must have an accurate inventory of their systems, be able to monitor their state in real time, and have a means to model maintenance, including patching, in a complex way. Before equipment is even bought, its security design and ability remediate weaknesses should be assessed. Another important integration is threat intelligence from as many sources as possible in order to gain insight on attacks detected in real-world incidents as well as those which are anticipated from wider intelligence. At the same time, connections to IT networks must also be carefully handled so as not to create backdoors attacks might exploit, for example unpatched VPNs used for remote maintenance.

PRESSING AHEAD

While it's certainly a truism that manufacturing is worryingly exposed to the threat of cyberattacks, it might be more accurate to say all sectors are exposed but in different ways. Nevertheless, what's true is that it's only recently that it's dawned on the manufacturing sector that this poses existential risks that can't be dodged. Manufacturing companies that plan to still be in business in a decade have no choice but to press ahead. For the manufacturing sector to emerge from the era of weak insecurity intact, it must turn cybersecurity from the job description of one department into a business calling ●

Chris Grove, CISSP, NSA-IAM, Technology Evangelist at Nozomi Networks, brings more than 25 years of cybersecurity experience with deep knowledge of IT, OT and IoT networks and mission-critical infrastructure.

Andrea Carcano, Founder and Chief Product Officer at Nozomi Networks, is an expert and international leader in industrial network security, artificial intelligence and machine learning.

The automation of freight vehicles remains at risk of being disrupted by ineffectual cybersecurity