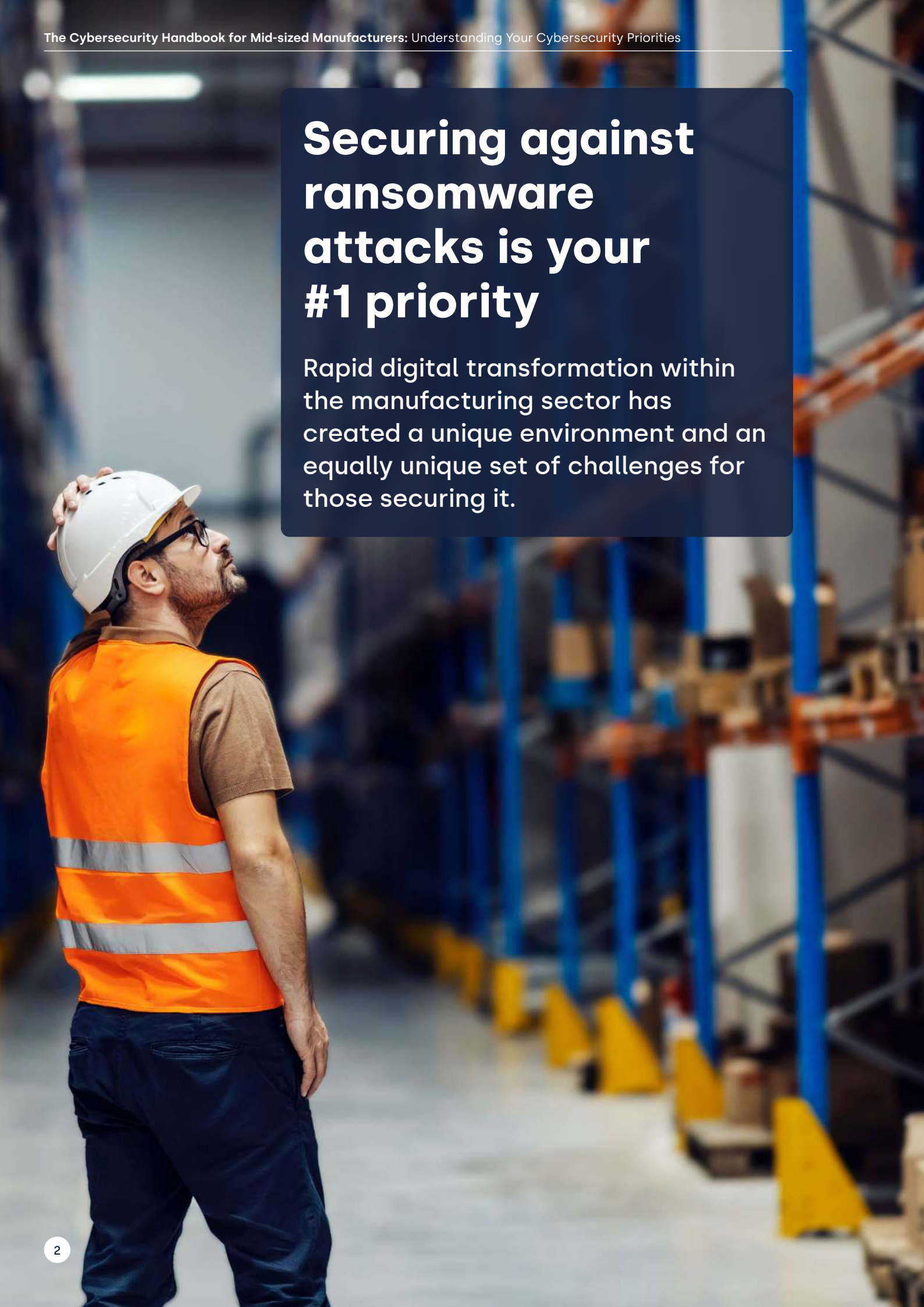
eye.

Visit eye.security

The Cybersecurity Handbook for Mid-sized Manufacturers

Understanding Your Cybersecurity Priorities



Securing against ransomware attacks is your #1 priority

Rapid digital transformation within the manufacturing sector has created a unique environment and an equally unique set of challenges for those securing it.

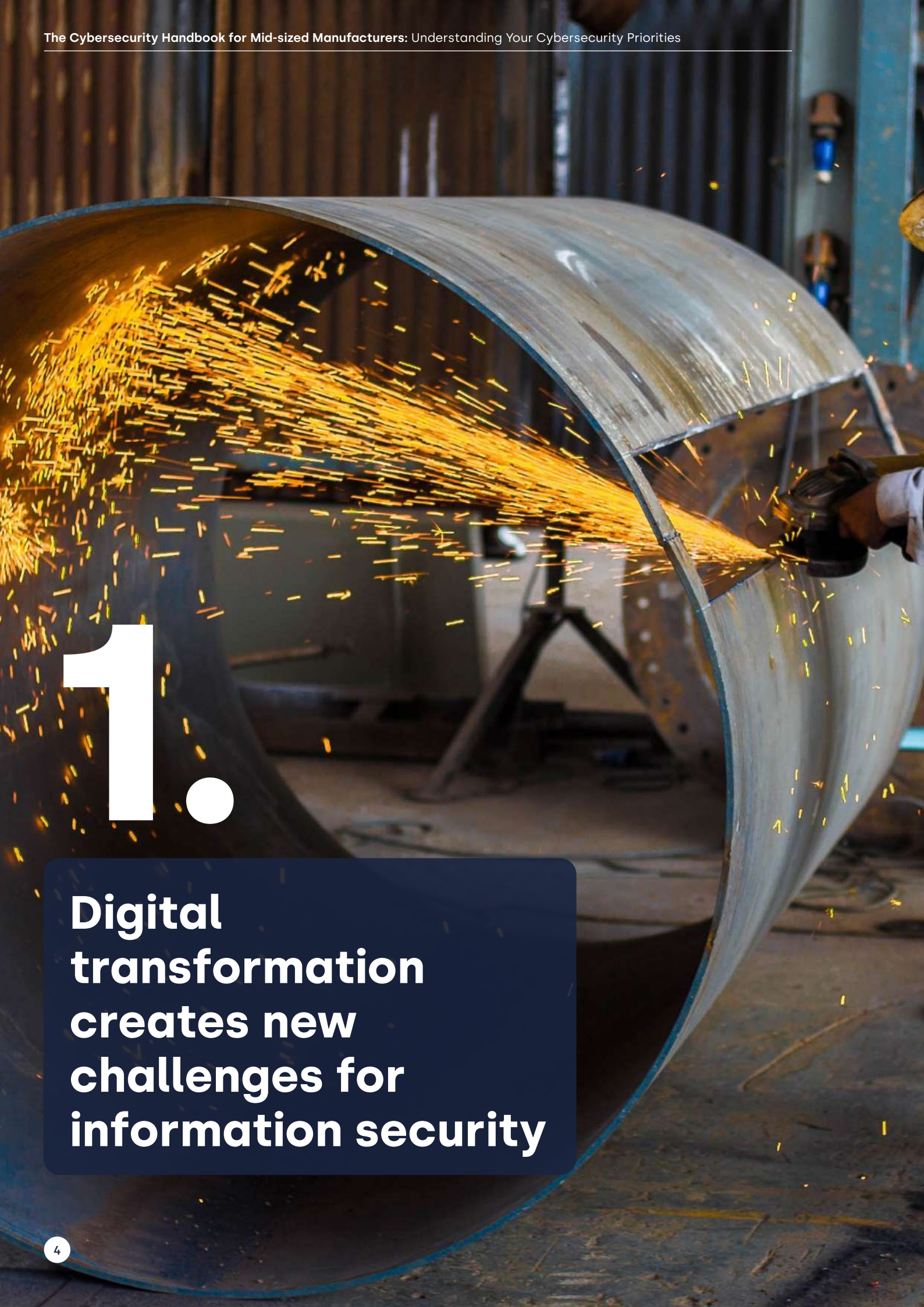
The most prevalent cyber attack facing manufacturing is not dissimilar from other industries – ransomware.

26%

of all cyber attacks in the past three years targeted manufacturers

71%

of all cyber attacks targeting manufacturers were ransomware



1.

Digital transformation creates new challenges for information security

Organisations in the manufacturing sector have embraced digital transformation to drive innovation, growth, efficiency and profitability. The rate and scale of this change has created a unique environment consisting of converging information and operational technologies (IT and OT), complex supply chains, employees with diverse skillsets, and numerous regulatory challenges. Combine this with a rich array of high-value information and the potentially disastrous impact of business downtime, and you have a highly sought-after target for cyber criminals and other threat actors.

In response, several cybersecurity companies offer a portfolio of products that are designed specifically to protect manufacturing businesses, primarily focusing on operational technologies (OT). However, the reality is that, while there have been attacks designed to sabotage OT, the main threat facing manufacturers is not dissimilar from many other businesses. A World Economic Forum report published in May 2024 stated that, in the previous three years, the manufacturing sector was the most targeted by cyber attacks and **71% of them were ransomware.**

Manufacturing businesses are highly sought after targets for cyber criminals. Protecting the information they are attempting to steal, encrypt, and hold for ransom must be your number 1 priority. In what follows, we highlight the top 9 security measures you should consider. To put these in context, it is first worth considering why are manufacturing organisations so highly targeted? Here is a breakdown:

2.

A unique technology environment

Manufacturing environments have always been unique, consisting of IT and OT, but digital transformation has resulted in further complexity and opportunities for cyber criminals.

Rapidly expanding attack surface

The attack surface is the sum of everything that a threat actor can exploit to achieve their goals, including software, hardware, people, and processes. In manufacturing organisations, this is expanding due to the introduction of new technologies, the proliferation of IoT, the introduction of remote work, and the increase in BYOD (bring-your-own-device) practices.

Increased interconnectivity

Previously air-gaped industrial control systems (ICS) are now often connected to the IT network and the internet, and IoT has resulted in large networks of connected, often heterogeneous devices. While well-designed, segmented and secured networks should prevent attackers jumping between OT and IT networks, no security measures are 100% effective.

Vulnerable, legacy OT

Many OT systems have been in use for years and were not designed to modern security standards. They were never deemed to be a target, and they often use embedded operating systems and software that are no longer supported by the publisher. They exist because they are doing one job well. Replacing them would be costly and result in business disruption. While they are unlikely to be a target, any exploitable vulnerability can result in them being used by an attacker to move laterally through your network to reach their goal.

3.

A unique commercial environment

Combining these technology challenges with typical manufacturing business processes and structures has created an environment that cyber criminals are exploiting.

Complex supply chains

Supply chain attacks abuse trusted business relationships to gain entry to an organisation's systems and network. These can be as simple as compromising an email account of a business partner and using it to send an email with a request to click a link that downloads malware. As it was sent from a trusted business partner, the recipient will often fall for the scam. Or they can be more complex, such as compromising a software supplier and embedding backdoors into applications that allow the attacker to access your network.

The manufacturing sector consists of complex supply chains and a high degree of business interconnectedness. Many manufacturers are a producer and consumer and there are likely many sole suppliers in this network. Any one being unable to deliver due to an attack can have far-reaching consequences across the whole supply chain.

Regardless of the maturity of your security programme, you are only as secure as your business partners and customers. Many smaller businesses underestimate their cyber risk. You can only go so far when auditing your suppliers — how do you guarantee the security maturity levels of their other business partners?

According to the World Economic Forum, ransomware was the top risk for manufacturing, followed by social engineering and supply chain attacks, both of which form the initial incursion stages of an attack which could end in ransomware.

54%

lack visibility of vulnerabilities in their supply chain

41%

blamed a breach on a 3rd party

Organisation structure and culture

When compared to industries like banking and financial services, manufacturing businesses often have immature security programmes that have not evolved to keep pace with their digital transformation, and they lack a culture of security awareness.

Manufacturing organisations consist of many different departments employing diverse groups of people with very different experiences, skillsets and priorities. There is likely a lack of knowledge and resources spanning IT, OT, cybersecurity, information security and governance, risk and compliance (GRC). The outcome can be fragmented transformation strategy and decision making that leads to gaps in security measures.

Regulatory landscape

The regulatory landscape is changing to reflect changing business practices and digital transformation in general, and many regulations contain specific clauses that impact manufacturing. For example, the EU Network and Information Systems Directive (NIS2) regulates manufacturers supplying the critical infrastructure industries. The Cyber Resilience Act emphasises security-by-design principles to mitigate the risks of cyber attacks in manufacturing environments. Equally, manufacturing-specific regulations are evolving. For example, the Machinery Regulation (2023/1230), when last updated, introduced clauses to specifically accommodate new risks from cyber threats.

Given the prevalence of ransomware threats, the regulation of most importance is one that applies to all businesses, the EU General Data Protection Regulation (GDPR). Ransomware groups often use double extortion, where data is not only encrypted but stolen with the threat of exposure, which could leave the victim facing hefty penalties under GDPR.

EU Agency for Cybersecurity (ENISA) Threat Landscape for 2024

72% of threats targeting manufacturing were ransomware

Ransomware is the biggest threat facing manufacturing.

Manufacturing is the 2nd highest targeted industry for ransomware.

Manufacturing is considered the most frequent, high-impact victim of ransomware.

Many threat actor groups focus on specific industries, but manufacturing is targeted by most of them.

4.

Why is the manufacturing sector so highly targeted?

Why are manufacturers more targeted than any other sector? Much of the answer lies in the challenges described above – a large attack surface, vulnerable systems and high levels of technology and business connectivity. When you combine this with immature security programmes compared to other sectors such as financial services and banking, manufacturing becomes a low-hanging fruit for ransomware threat groups.

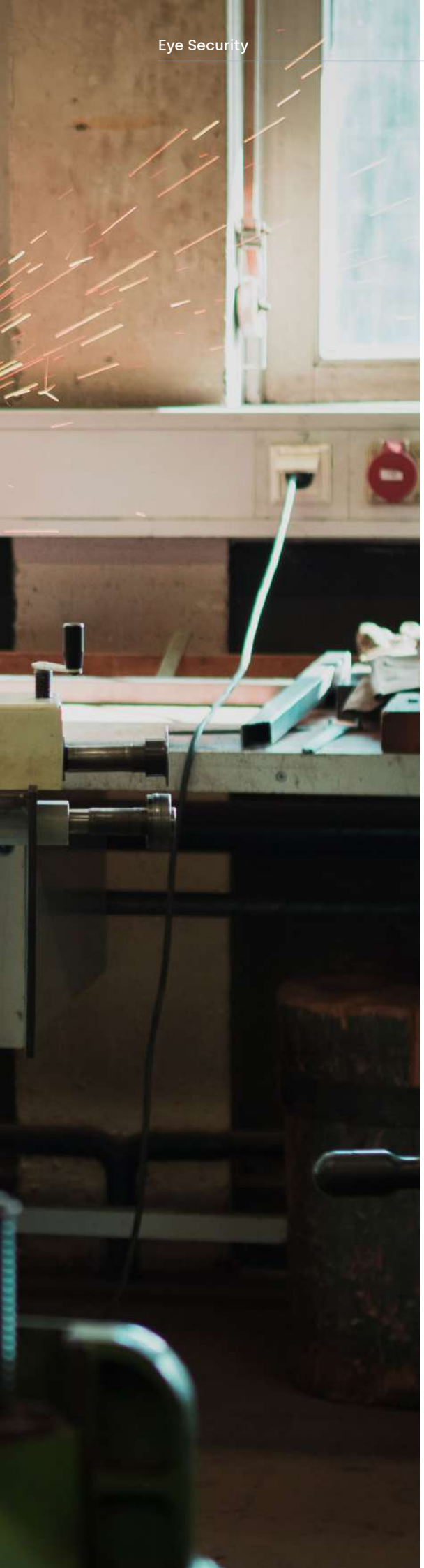
Why ransomware?

1. In manufacturing, ongoing business disruption from an attack can have a far more serious impact than for other industries, resulting in manufacturers being more likely to pay a ransom. Manufacturers are heavily reliant on continuous operations and the impact of missing fixed delivery dates could be disastrous across the supply chain.

2. Along with sensitive personal and business information, manufacturers have considerable amounts of valuable data, including trade secrets and intellectual property that might be sold to the highest bidder on the dark web.

5.

Protect your manufacturing business with 9 critical security measures



1. Follow best practices

There are many cyber and information security frameworks, produced by government organisations, such as the US National Institute of Standards and Technology (NIST), Germany's Bundesamt für Sicherheit in der Informationstechnik (BSI) and the Netherlands National Cybersecurity Centre (NCSC). Pick one that is appropriate for your organisation's cybersecurity maturity level and size and consider any constraints around budget and resources.

2. Understand your security posture

It is difficult to secure your business if you don't know what you are protecting. You should identify your critical assets and information, assess your infrastructure, recognise where your high-priority vulnerabilities are and how to mitigate them.

3. Create immutable off-site backups

If the worst happens and a ransomware attack is successful, even paying the ransom might not result in you recovering encrypted data. Having a reliable, untampered backup of your critical information is essential.

4. Deploy preventative security measures

These are the essential foundation of your security. Technologies that are designed to block attacks, such as endpoint protection platforms (EPP), firewalls, email and web security. Segment your IT, OT, BYOD and guest networks, and consider a micro-segmentation strategy for different security zones.

5. Create a culture of cyber awareness

Build a security awareness training (SAT) programme. Many organisations consider this a "tick box" exercise to comply with regulations or qualify for cyber insurance. Phishing simulations go some way to training users to identify email threats. However, to drive employee behavioural change and create a culture of security awareness, choose a SAT provider that offers engaging computer-based training created by education experts in collaboration with ethical hackers and cybersecurity experts.

6. Secure identities

The Verizon Data Breach Investigations Report 2024 stated that 25% of breaches in manufacturing resulted from the use of stolen credentials, and 55% of system intrusions used phishing. To reduce this risk, create strong password policies and use multi-factor authentication.

Deploy cloud detection and response (CDR) to continuously monitor user activity in your cloud applications. This will detect suspicious behaviours such as impossible travel, where a user logs in from multiple locations where they could not possibly be at the same time. If you license Microsoft applications, assess your existing entitlements as you may already be licensed for Microsoft Sentinel, which provides Entra ID protection.

7. Assume breach

Preventative measures will fail to block every attack. Prepare for the eventuality where an attacker has successfully infiltrated your network or applications.

Regardless of whether their initial access was via an identity, laptop or ICS, a ransomware threat actor will move laterally across your network, searching for high-value information to steal and encrypt. To do so, they must compromise a server or a user's computer. To detect these threat actors as they progress their attack, you should deploy endpoint detection and response (EDR).

If you have chosen one of the leading EPPs, such as Crowdstrike or Microsoft Defender, you already have these capabilities built in. If your EPP doesn't include EDR, you should upgrade to one that does.

8. Oursource to an MDR provider with a 24/7 SOC

As described above, many organisations already have detection and response technologies. However, to obtain full value and realise a return in your investment, you need skilled security operations (SecOps) staff with the time and tools to respond to attacks. The global cyber skills shortage is well documented and to overcome this, financial and time constraints, many organisations outsource this responsibility to a managed detection and response provider (MDR).

An MDR provider will monitor your CDR and EDR and respond to contain any attacks. Some go further and will offer an incident response service, and many provide a full end-to-end partnership across your security programme, helping out with many of the earlier measures highlighted above.

9. Purchase cyber insurance

This is your final and extremely important security measure. If you have accepted that breaches do occur, you need detection and response technologies, SecOps and incident response professionals to reduce the risk of a successful attack. And you must still plan for the worst outcome.

Insurance should cover direct and indirect costs, including any potential liabilities across your complex supply chain. Many MDR providers have deep relationships with broker networks and combining insurance with their services will often result in significant premium discounts and simplified application processes.

This guide has focused on ransomware and protecting your business from it should be your highest priority, but do consider there are other threats you face, such as corporate espionage and sabotage.

Once you have the basics in place, the next stage is to protect yourself from these less prevalent threats. To do so, you might consider building your own security operations centre with appropriate tooling and employing specialist SecOps staff.

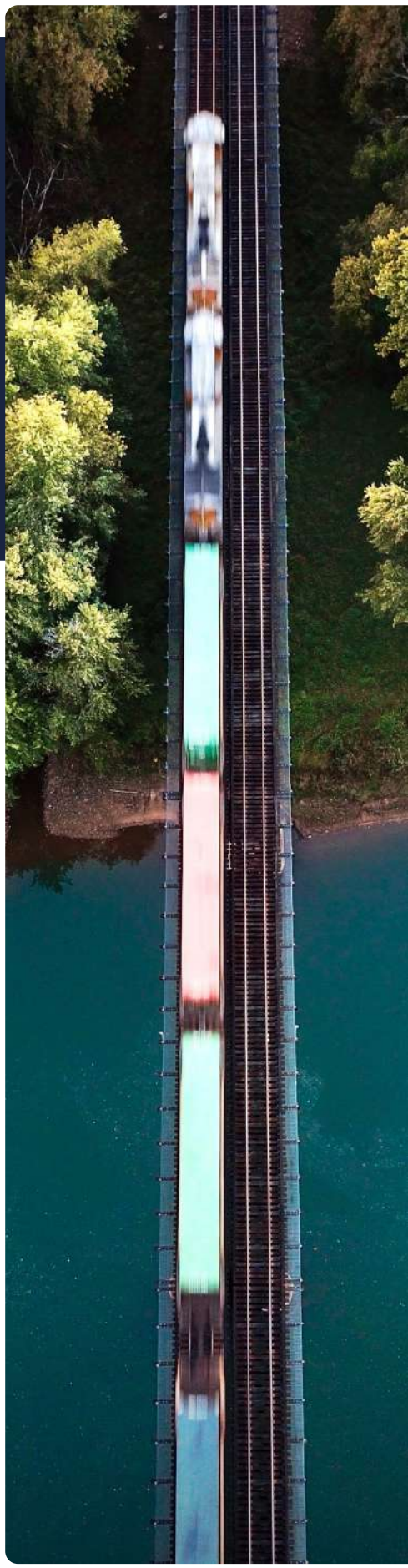
Once in place, you should look to further securing your OT environment with specialist asset and vulnerability management. Network detection and response (NDR) tools will provide deep visibility into all network traffic but will require experts to deploy and monitor. For more information, read EDR vs NDR: Why Endpoint Security Has a Clear Advantage.

6. Conclusions and next steps

You have likely already deployed or plan to add many of the recommended security measures. To determine your priorities for additional security, do consider ransomware protection is your number one priority, and most attacks will involve credential and/or endpoint compromise and data exfiltration.

You should therefore focus your efforts on detecting, responding to and containing such attacks.

This guide has helped you to understand why you are being targeted, the measures you should take to reduce the risk of a successful attack, and how to mitigate the impact of the worst-case scenario.



Further resources for manufacturing businesses

Case study: KeyTec Netherlands

As reports of ransomware in their industry soared, manufacturing company KeyTec Netherlands decided to take action. Find out how Eye Security helped them proactively bolster their defences and create a cyber-savvy work culture.

Case study: Signature Foods

As cyber crime becomes increasingly sophisticated, companies racing to keep up are turning to external suppliers. Find out how Eye Security helped Signature Foods get blanket cyber protection in just a few weeks.

Eye Security helps manufacturers stay safe with 24/7 threat monitoring, rapid incident response, and integrated cyber insurance. We make cybersecurity straightforward and effective so you can focus on maintaining operations and meeting production deadlines with confidence.

Visit www.eye.security