CyberSmart

PROTECTING THE PRODUCTION LINE

The value of cybersecurity in manufacturing

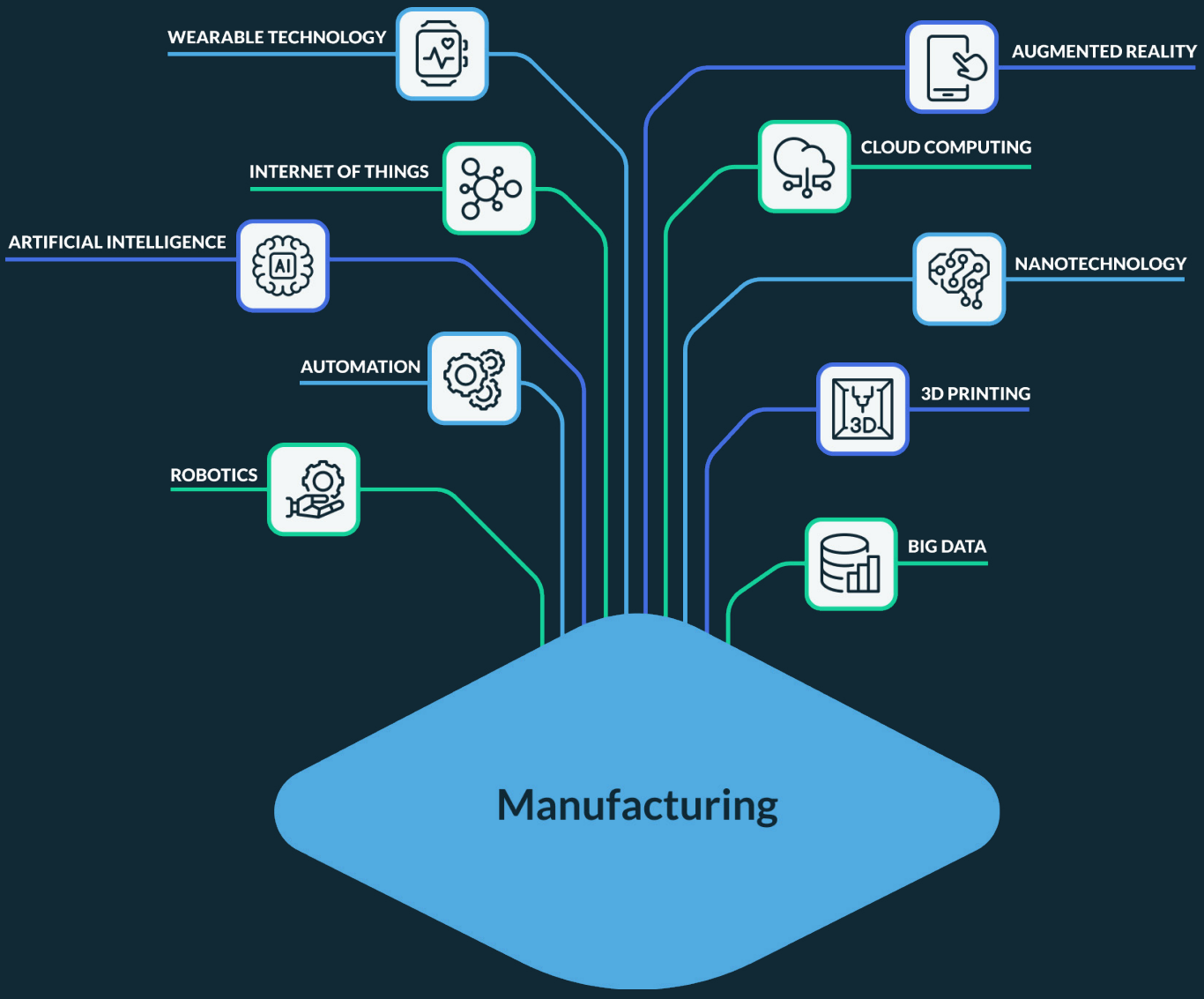
cybersmart.co.uk

Contents

INTRODUCTION

Data-driven manufacturing means higher rewards and risks

Technology innovations have propelled manufacturing forward in the last decade. Automation speeds up production lines, predictive technology and data analytics help to improve processes and resolve issues faster, and cloud computing connects data across multiple locations to increase efficiency, to name just a few.



But, the volume of technological advances alongside growing supply chains and reliance on SaaS for everyday operations means the average manufacturing tech stack is large. When it comes to proper IT management, manufacturers have a lot of responsibility on their hands. What once was easy to manage is now difficult to keep track of.

And, hackers are aware of this potential vulnerability. Manufacturing is now the most targeted industry for cyberattacks. In this guide, we explain common risks and ways to protect your business from threats.

MANUFACTURING BY NUMBERS

The security landscape

Managing cybersecurity and risk effectively is a difficult task, and it's one that the manufacturing industry has yet to master because of its complexity.

Attacks are common, manufacturers don't always have full visibility of their security or vulnerabilities, and growth is restricted as a result.

$4.47M

The average cost of a data breach for manufacturing companies.[1]

Every minute

State-sponsored hackers attack healthcare manufacturing companies like Johnson & Johnson every minute of every day. [3]

24.8%

of all cyber-attacks target manufacturers.[2]

42%

of UK manufacturers were the victim of a cyber-attack in 2022.[4]

49%

of CEOs say cyber risks are the biggest threat to growth.[5]

30%

of extortion attacks target manufacturers.[6]

41%

of UK manufacturers say they don't have the data to assess their cyber risk.[7]

90%

of manufacturers can detect cyber events, but few extend those capabilities to operational technology.[8]

70%

of manufacturers planned to increase their cybersecurity budgets in 2022.[9]

56%

of manufacturers say that they don't have enough people to handle the increasing volume of security events.[10]

COMMON THREATS

Understand common threats

Know which attacks are most common in your industry, how they occur, what they look like, and what you can do to prevent them. Get a good understanding of your vulnerabilities so you can prioritise how to remedy them to make your business less accessible to threat actors.

The 5 biggest cybersecurity threats to manufacturers

Ransomware

65% of ransomware attacks target manufacturers.[11]

Phishing

91% of all cyberattacks begin with a phishing email.[12]

Industrial IoT Attacks

69% of industry leaders expect IoT attacks to increase in the coming years.[9]

Intellectual property theft

34% of manufacturers say IP theft is their biggest cyber threat.[14]

Supply chain attacks

89% of businesses have experienced a supplier risk event in the past five years.[13]

Production grinds to a halt at Toyota

A supply chain attack reduced production to a third of its global output. 28 production lines were forced to stop for at least a day when a top tier supplier directly connected to Toyota's production control system, suffered a breach.[15]

Industry-specific risks

Many processes in manufacturing are dependent on one another, and there's often a complex web of systems and equipment linking everything together. From raw materials or parts to equipment for production and distribution, the number of processes and logistics to keep things on schedule can be overwhelming. And a single compromised component can bring operations to a grinding halt.

Hackers know this, which makes manufacturers a great target. One successful attack could cost millions in lost revenue and give a threat actor the notoriety they're looking for. This is a particularly big risk because supply chains are vast – some manufacturers have tens of thousands of suppliers – which gives hackers even more opportunities to compromise your systems and processes.

Using smart machinery, though fantastic for speed and production levels, also creates more opportunities for attackers. And, as more back-office staff work remotely, unsecured networks could cause problems, too. There's a lot to be aware of and keep up to date as processes and the way we work change.

PROLIFIC ATTACKS

Damages caused by cyber criminals

You probably don't need any convincing that investing in your cybersecurity is a wise decision, but these examples are a sobering reminder of why it's important to take precautions and stay on top of developing threats. Don't let these scare you – they're simply a way to arm yourself with information and act as a reminder that even the biggest companies with the biggest budgets can fall victim to cybercrime.

1. WannaCry ransomware attack

Year: 2017
Attack type: Ransomware
Scale: Global

Summary: 2017's WannaCry ransomware attack exploited vulnerabilities in unpatched versions of Microsoft's Windows operating system to compromise over 230,000 computers across the globe. Among the victims was global car manufacturer, Renault-Nissan.

2. LockerGoga

Year: 2019
Attack type: Ransomware
Scale: Company

Summary: Global aluminium producer Norsk Hydro had to temporarily suspend production after falling victim to a LockerGoga ransomware attack. The attack affected 160 plants across 40 countries and cost the manufacturer an estimated $35m-$41m in just one week.

3. Operation CuckooBees

Year: 2019-2021
Attack type: IP theft
Scale: Global

Summary: The Operation CuckooBees campaign used zero-day software exploits to steal intellectual property and trade secrets from technology companies across East Asia, Western Europe, and North America. Investigators attributed the campaign to Winnti, a state-sponsored Chinese threat group. Due to its complexity and scale, investigators say it's impossible to measure the campaign's financial impact.

4. Colonial Pipeline attack

Year: 2021
Attack type: Ransomware
Scale: National

Summary: The 2021 Colonial Pipeline ransomware attack made global headlines when it brought operations to a halt at a major US oil pipeline. The attack, which caused President Biden to declare a state of emergency, affected consumers across the east coast and triggered a four-cent increase in fuel prices. It remains the largest publicly disclosed cyber-attack against critical infrastructure in the US.

5. Nvidia LAPSUS$ ransomware attack

Year: 2022
Attack type: Supply chain
Scale: Company

Summary: Nvidia, the US' largest microchip manufacturer, suffered severe outages in its internal network for two days in February 2022 following a targeted supply chain attack. As well as disrupting production, hackers belonging to the LAPSUS$ ransomware group successfully stole 1TB of technical data.

6. Visser Precision

Year: 2019
Attack type: Ransomware
Scale: Company

Summary: Visser Precision, a space and defence manufacturer, suffered an attack where sensitive documents were stolen and published online. The hackers asked for $2.3 million in ransom, which the company refused to pay. Amongst the sensitive documents stolen were non-disclosure agreements with Tesla, SpaceX, and General Dynamics as well as a schematic for a missile antenna.

7. JBS

Year: 2021
Attack type: Ransomware
Scale: Global

Summary: Global food company, JBS, experienced a ransomware attack on its servers by REvil. The attack caused meat production to grind to a halt for more than five days, compromising food supply and prices for consumers, and cost $11 million in ransom.

STAYING SAFE

Securing your business

Every business is a target for hackers, so it's important to maintain your security. Here are some top tips for securing your business so it's less susceptible to attacks and better at responding to them if they do occur.

Protect yourself first

Build a solid foundation based on cybersecurity best practices to keep your processes, systems, data, and employees secure.

Update software regularly

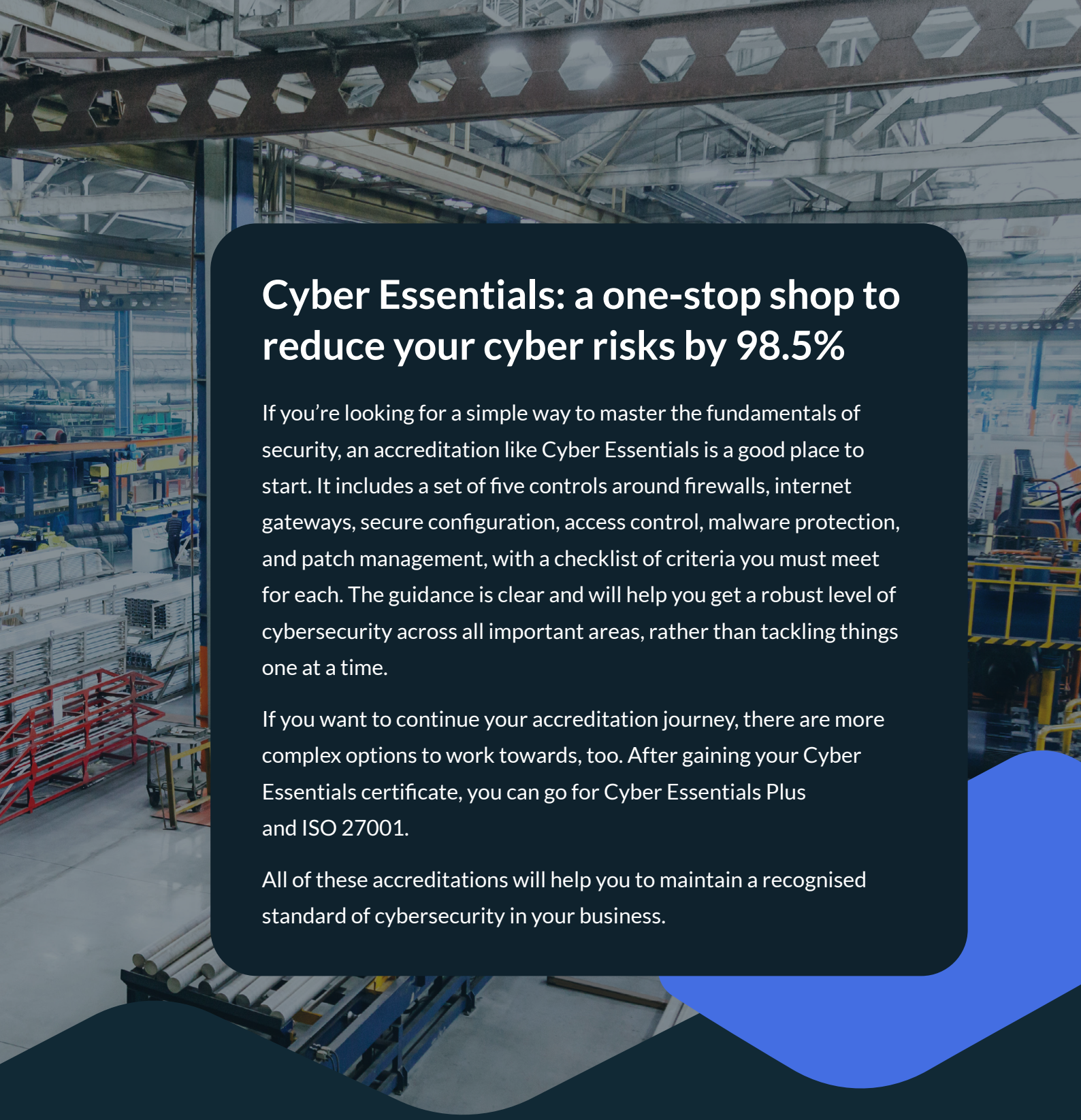
Install patches as soon as they're released to ensure your applications and software are up to date.

Control access

Limit exposure to sensitive data by ensuring employees can only access the data they need. Set up different access levels to make this easier and give employees user profiles based on their permissions.

Strengthen your password policy

Have an organisation-wide password policy that stipulates what criteria users must meet to set appropriate passwords and how often to change them. Set up multi-factor authentication using tools such as Google Authenticator to add an extra level of security.



Cyber Essentials: a one-stop shop to reduce your cyber risks by 98.5%

If you're looking for a simple way to master the fundamentals of security, an accreditation like Cyber Essentials is a good place to start. It includes a set of five controls around firewalls, internet gateways, secure configuration, access control, malware protection, and patch management, with a checklist of criteria you must meet for each. The guidance is clear and will help you get a robust level of cybersecurity across all important areas, rather than tackling things one at a time.

If you want to continue your accreditation journey, there are more complex options to work towards, too. After gaining your Cyber Essentials certificate, you can go for Cyber Essentials Plus and ISO 27001.

All of these accreditations will help you to maintain a recognised standard of cybersecurity in your business.

Encrypt data

Encrypt sensitive data so that, in the event it's stolen, it's unreadable without the encryption key.

Train your employees

Empower your employees with the knowledge to confidently keep hardware, software, data, and systems safe. Have regular refresher sessions to keep security front of mind, and deliver information in digestible chunks.

Respond to incidents effectively

Prevention is better than cure, but it helps to be prepared for every eventuality. One way to respond to incidents is through a security operations centre (SoC). But just 17% of manufacturers have SoCs that operate 24/7, which could waste several precious hours if an attack occurs outside of its operation. For complete peace of mind, it's worth looking at 24/7 SoC options. Third parties can provide this for you to take pressure off your IT team.

Secure your supply chain

Because supply chain attacks are so popular with hackers, you need to secure yours. This is a growing trend, with 95% of organisations increasing their focus on third-party risk assessment.

Talk to your suppliers

Understand where your suppliers and partners are with their cybersecurity and share your experiences. Keep an open dialogue so you're front of mind if they suffer an attack.

Risk assess

Find a controlled, detailed way to assess supplier risks. Talking to them is a good start, but having structured risk assessments to measure their approach against your needs is going to speed the process up, especially for manufacturers with thousands of suppliers.

Make good cybersecurity practices contractual

Establish what you expect from your suppliers around cybersecurity and apply those principles to contracts. An agreed level of acceptable cyber hygiene sets expectations and keeps suppliers accountable.

For some businesses, requiring that anyone you work with completes Cyber Essentials certification will be enough. For others, something more comprehensive like ISO 27001 certification might be better.

Follow the NCSC's guidance

If you ever want to find out more about supply chain best practices, the National Cyber Security Centre (NCSC) has some useful guidance and information.

THE BENEFITS OF ROBUST CYBERSECURITY

There’s more to cybersecurity than peace of mind

For objectively little effort and investment compared to that needed if you face an attack, you’ll get a lot back from prioritising security.

1. Preventing disruption

Implementing strong cybersecurity tools and processes, such as regularly backing up data, will help you minimise the impact of cyber-attacks on your operations. Any time you prevent a disruption you’re enabling business continuity, which means more uptime, more profit, and better results for your business.

2. Building trust with partners and customers

As a manufacturer, you’re reliant on your supply chain but you’re also part of a supply chain. That means other companies are counting on you to stay secure. Doing so will build trust and strengthen your partner relationships.

Having comprehensive security practices will also resonate with customers and protect your brand reputation, which is only too easy to damage.

3. Saving money

Far from a cost centre, research shows that investing in cybersecurity pays off in the long run. It costs significantly more to recover from cyber-attacks than it does to protect against them. The average IoT attack costs manufacturers $330,000, on average[6] – a drop in the ocean compared to annual cybersecurity costs.

4. Qualifying for government contracts

Government contracts are a vital revenue source for many UK manufacturers. But with cybersecurity under greater scrutiny than ever, public sector organisations only allow manufacturers with an active Cyber Essentials certificate to bid for government tenders. Getting accredited will help you expand your portfolio of customers and build lasting partnerships.

5. Increasing productivity

Building a good base level of cybersecurity frees up time to focus on operations, improving productivity. You'll need to stay on top of security, but it'll be much easier to maintain when you have a strong foundation.

6. Earlier threat detection

Investing in 24/7 security monitoring gives you the comfort that no matter what time disaster strikes, someone will be on hand to alert you and help stop it, minimising the extent of the damage caused.

YOUR CYBERSECURITY JOURNEY

Shape up your manufacturing cybersecurity

It's not easy being one of the most targeted industries for cybercrime. But, don't let the threat scare you. Instead, let defending yourself against ill-intentioned criminals put fire in your belly to make their job as difficult as possible.

Take sensible, steady steps to improve your security, save money, and improve productivity. The benefits will outweigh the time and money needed to set up your defencess and far outweigh the cost of a breach, so you're guaranteed a good ROI.

Remember, if you're looking for a straightforward way to cover the fundamentals of security in one go, you can work towards an accreditation like Cyber Essentials. And, if you don't want to leave threat detection to your already stretched IT team, you can outsource to a dedicated third party. With the fundamentals covered, you can then focus on what to do next to continue your cybersecurity journey.

For support with accreditations, 24/7 threat detection, cyber insurance, and more, get in touch – we're happy to help.

Talk to us

Logoipsum

CyberSmart

cybersmart.co.uk

SOURCES

1. Cost of a Data Breach Report 2022 (IBM)
2. Distribution of cyber attacks across worldwide industries in 2022 (Statista)
3. Johnson & Johnson CISO: Healthcare orgs are seeing nation-state attacks every single minute of every single day (ZDNET)
4. Research Reveals UK Manufacturing Sector Under Threat as Almost Half Suffer Cyberattack in the Last 12 Months (BlackBerry)
5. Reimagining the outcomes that matter (PwC)
6. IBM Security X-Force Threat Intelligence Index 2023 (IBM)
7. Cyber Security for Manufacturing (Make UK)
8. Cybersecurity for smart factories: Tools for managing cyber threats to manufacturing (Deloitte)
9. Manufacturers ramp up cyber defenses as supply-chain bottlenecks—and vulnerabilities—deepen (PwC)
10. State of security report (Splunk)
11. What to Expect in the 2022 Dragos ICS/OT Cybersecurity Year in Review (Dragos)
12. 12 91% of all cyber attacks begin with a phishing email to an unexpected victim (Deloitte)
13. Supply Chain Risk Management: Increase supply chain risk readiness to combat market disruption (Gartner)
14. Cyber risk in advanced manufacturing (Deloitte)
15. Toyota's Supply Chain Cyber Attack Stopped Production, Cutting Down a Third of Its Global Output (CPO Magazine)