

Cybersecurity

What is it?

Cybersecurity is the practice of protecting computer systems, networks, devices and sensitive information from digital attacks, unauthorised physical access and damage.

Cyber attacks come in many forms, including: malware such as ransomware, viruses and spyware; phishing emails designed to steal sensitive information; social engineering techniques that manipulate people into bypassing security procedures; and physical threats such as device theft or intrusion into premises, equipment and networks.

Cybersecurity combines technology, processes and human awareness to help keep information secure, accurate and accessible.

It's also a mindset and a set of procedures that help protect operations, supply chains, safety, customer trust and business continuity from both external and internal threats.

Why it matters

As manufacturers pursue digital transformation through automation, industrial IoT, cloud platforms and data-driven technologies, greater connectivity also introduces new risks, making effective cybersecurity essential.

Manufacturing is the most frequently targeted sector for cyber attacks because operational disruption can have immediate financial consequences.

Cyber incidents can halt production, delay deliveries, compromise sensitive information



and damage customer confidence, while valuable assets such as intellectual property (IP), engineering expertise, product specifications and customer data are attractive targets for cyber criminals.

The impact can extend beyond individual businesses, causing disruption across global supply chains.

Manufacturing environments present additional challenges, including:

- Legacy equipment not designed with cybersecurity in mind
- Connected operational technology (OT)
- Industrial IoT devices
- Complex networks developed over many years.

The rise of AI-powered tools is also enabling attackers to create more convincing phishing campaigns and target organisations at greater scale.

What it enables

Effective cybersecurity not only reduces risk, it enables manufacturers to embrace digital transformation while protecting the systems, information and operations that underpin long-term success.



Continuity - Protects production, operations and revenue from disruption.



Resilience - Enables faster recovery when incidents occur.



Trust - Strengthens confidence among customers, suppliers and partners.



Innovation - Empowers manufacturers to adopt new technologies and innovate.



Competitiveness - Helps meet growing customer and supply chain expectations.



IP - Safeguards designs, specifications, know-how and commercially sensitive information.



Integrity - Ensures critical information is accurate, available and trustworthy.

Where it works

Practical applications to help you see where cybersecurity could add value in your business:

Connected machines, sensors and monitoring systems

Protects equipment from unauthorised access and disruption to maintain operational continuity.

OT and control systems

Manages risks associated with connected production equipment and the convergence of IT and OT, particularly in vulnerable legacy systems.

Business and production data

Protects customer orders and the information used to support planning, scheduling, quality management and decision making. Maintaining accuracy and availability helps reduce the risk of disruption, errors and safety issues.

Intellectual property and technical knowledge

Safeguards CAD files, drawings, product designs, process specifications and commercially sensitive information.

Supply chains and customers

Demonstrates cyber resilience to customers and helps minimise disruption across the supply chain.

Cloud platforms and business systems

Secures ERP systems, planning software, supplier portals and collaboration tools that support operations.

Remote and hybrid working

Protects laptops, mobile devices, online meetings and remote access technologies, helping staff work securely from anywhere.



How it works in practice

- ↓ Identify the systems, devices, data and processes that are critical to your business.
- ↓ Implement practical controls such as strong passwords, multi-factor authentication, access controls and software updates.
- ↓ Monitor systems and networks for unusual activity, vulnerabilities and potential threats through threat alerts, security monitoring, anti-malware tools and firewalls.
- ↓ Develop plans and responsibilities for responding quickly and effectively to incidents.
- ↓ Back up critical information, establish recovery plans, review risks regularly and learn from incidents to strengthen cyber resilience over time.

Cybersecurity is not a one-off project, it is a continuous process. Many manufacturers start by embedding good practices in a single system, process or area of the business before extending them more widely.

Case study snapshots



"An incident involving one of our customers showed how cybercrime impacts the wider supply chain. Although our own systems weren't compromised, it highlighted the importance of continually reviewing cybersecurity."

GW Shelter Solutions, a manufacturer of modular bus shelters, is working towards Cyber Essentials accreditation with support from Made Smarter to strengthen its knowledge, processes and security.

"AML wholeheartedly endorses Made Smarter for its support and funding to expand our digital capability."

AML, an advanced manufacturing solutions provider, upgraded cybersecurity, unlocking access to new defence and nuclear contracts, and supporting a forecast surge in turnover, from 1% to 25% within the next three years.

Key considerations

- **Cybersecurity is a business issue** - Resilience requires leadership, ownership and accountability.
- **People matter as much as technology** - Most successful attacks involve human error. Awareness and training are critical.
- **Start with the basics** - Many successful attacks exploit simple weaknesses. Strong passwords, multi-factor authentication, software updates and backups remain highly effective.
- **Understand what matters most** - Identify the systems, devices, data and processes that matter most.
- **Think beyond IT** - Cybersecurity must consider IT, OT, networks, devices and physical access to premises.
- **Protect your value** - Product designs, technical knowledge, engineering expertise and other IP are a key source of competitive advantage.
- **Look across the supply chain** - Suppliers, partners, service providers and internal users can all introduce cyber risks.
- **Prepare for disruption** - Response and recovery plans can significantly reduce the impact of an incident.
- **Build capability over time** - Cybersecurity is a continuous process of improvement.

Common pitfalls to avoid

- Assuming cyber criminals only target large organisations.
- Treating cybersecurity as an IT-only issue.
- Neglecting basic controls such as strong passwords, multi-factor authentication and physical and digital access management.
- Ignoring legacy systems and OT risks.
- Failing to prepare for incidents through backups, recovery planning and regular testing.
- Treating cybersecurity as a one-off project rather than a continuous process.

6 steps to success and how Made Smarter can help

1

Understand your risks - Identify the systems, devices, data and processes that matter most to your business, and assess where vulnerabilities may exist.

MADE SMARTER SUPPORT:
Digital Transformation Workshop

2

Get the foundations right - Introduce practical controls such as strong passwords, multi-factor authentication, access controls, software updates and backups.

MADE SMARTER SUPPORT:
Digital roadmap development

3

Build awareness and skills - Create a culture where staff understand cyber risks and their role in protecting the business.

MADE SMARTER SUPPORT:
Leadership and Digital Champions programmes

4

Secure your technology and data - Protect connected machines, systems, OT, IP and business-critical information.

MADE SMARTER SUPPORT:
Roadmap, expert support, Grant funding application, Digital Internship

5

Prepare for disruption - Develop incident response plans, backup procedures and recovery processes to minimise the impact of cyber incidents.

MADE SMARTER SUPPORT:
Expert support, signposting to the National Cyber Security Centre (NCSC) and Cyber Essentials.

6

Review, improve and strengthen - Regularly assess risks, review incidents, update controls and strengthen resilience as your business evolves.

MADE SMARTER SUPPORT:
Expert support, Grant funding application, Digital Internship

MADE SMARTER

www.madesmarter.uk



Take the next step

Start your digital journey today. Register for support and speak to a Made Smarter advisor to explore how cybersecurity could support your business.