

# The ultimate guide to taking cybersecurity seriously in your manufacturing business

The cost of a cyber attack

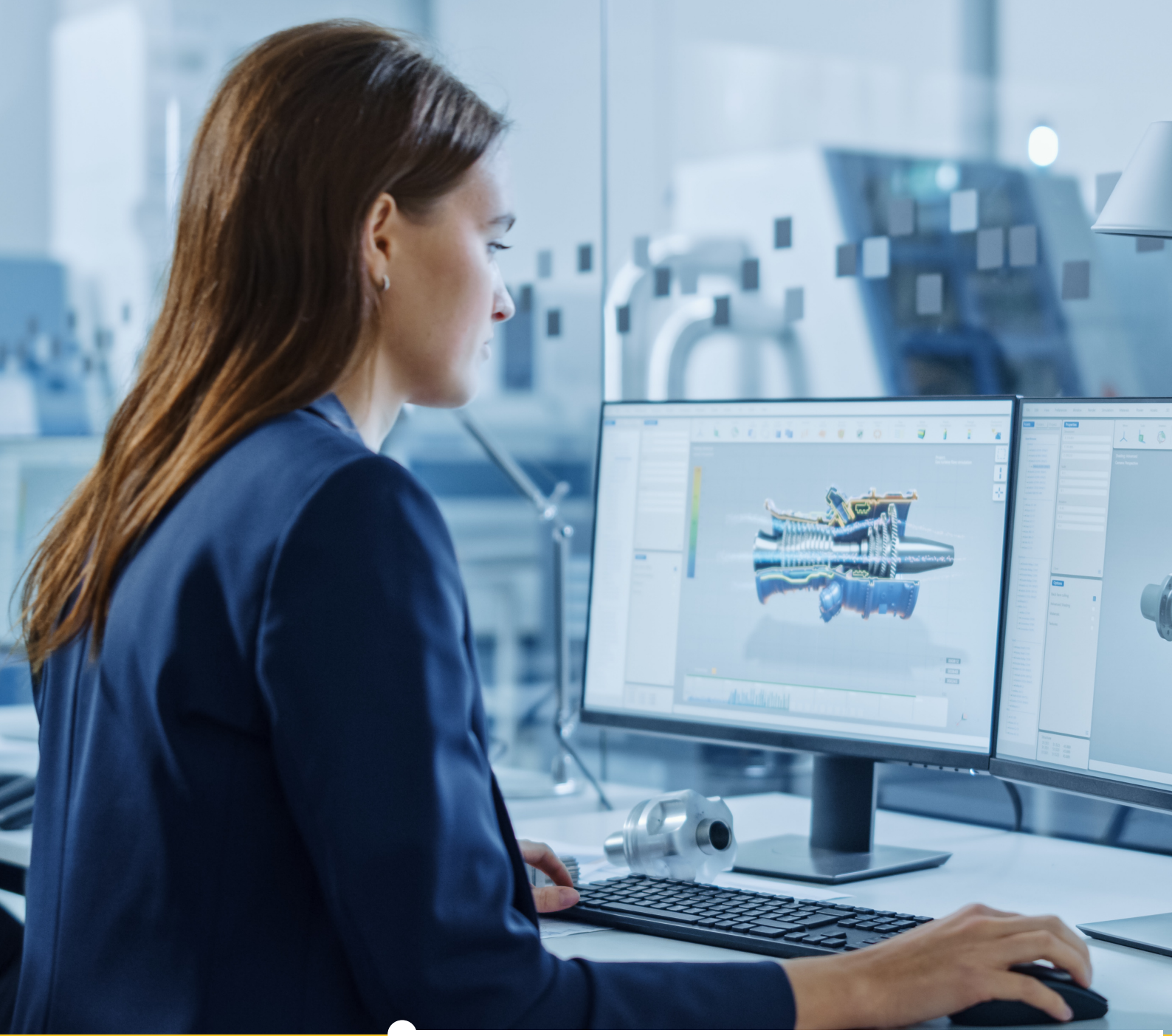
Types of cyber attack

Common cybersecurity weaknesses

5-step cybersecurity process

Key cybersecurity measures

Where to seek specialist technical support



Since the start of the pandemic, there has been a huge increase in cyber attacks. According to internet service provider Beaming, UK businesses faced a **20% rise in threats** compared to 2019 (the equivalent of one attempted attack every 46 seconds). Cybersecurity research firm CrowdStrike also found that **manufacturers saw an 11% increase** in network intrusions.

A rise was anticipated considering the switch to remote working. However, it appears that many are not fully protecting themselves. In this guide, we explain exactly why you can't afford to disregard cybersecurity, and offer some practices you can implement in your business.

# What is the potential cost of a cyber attack?

In monetary terms, **the average cost of a breach is £1,010**, although this figure increases with the size of the business. But there is also a time cost, not just a financial one – large organisations spend an average of 3.4 days managing the impact of an attack. Both costs can damage your capacity to operate your business as usual, as well as cause irreversible harm to your reputation.

Cybersecurity is taken very seriously by suppliers and customers – they increasingly want to see security credentials before signing purchase orders, meaning you could lose business if you don't take the necessary steps. Data protection is required by law through GDPR too, and you could land a hefty fine if you fail to notify a data breach to the regulator within 72 hours.

Given that cybersecurity is so critical for ensuring business continuity and growth, it's far better to prevent a cyberattack than risk one happening. It will cost a lot less in the long term when it comes to your brand's image, resources and bottom line.



# What types of cyber attack are there?

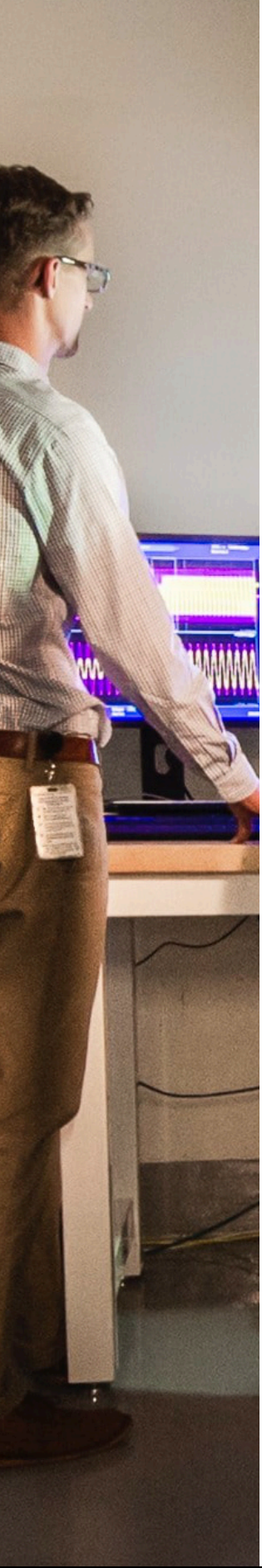
You can reduce the risk of a cyber attack if you know what they are and how to recognise them. Here are some of the most common ones:

- 1. Phishing** – This is one you've most likely heard of, as there are very few people who haven't received a phishing attempt in their inbox. These are often sent via email (but can be via telephone or text), and appear to be a reputable source. The user is encouraged to click a link and provide sensitive information.
- 2. Spear-phishing** – Here, either an organisation or individual is targeted with communications which are specific to their environment, and is often used alongside ransomware. They take small pieces of information over a period of time to complete the knowledge later, and then hold you to ransom.
- 3. DDoS (distributed denial of service) attack** – This is where a denial-of-service message is received; services and networks are bombarded with traffic to drain the resources and bandwidth, leading to the system being unable to fulfil user requests and becoming exposed. At the end of this, or a similar process, the company may potentially be contacted by the criminal organisation, demanding ransom in return for the encryption code, which could have catastrophic ramifications for a business – especially an SME.

## How do cyber attacks occur?

A few things that could leave you open to cyber attacks are actually very basic. We recommend checking if any of the following apply to your business, and taking corrective action if they do:

- Open ports or services
- Default settings
- Vulnerable applications and legacy operating systems
- Vulnerable makes and models of network equipment



If you're guilty of any of these, don't worry – many SMEs are. It's tempting to have fully open systems so that people can access them and be productive. However, it's important not to forget how dangerous this open and uncontrolled access is, and it's important to work on resolving the issues at hand.

## What can I do to boost cybersecurity?

The following five-pillar best practice is a highly recommended framework for cybersecurity:

**Identify** – Review your cybersecurity practices, and see if there are any clear weaknesses in your approach. If you don't do the basics, it's easier for cyber criminals to launch an attack.

**Protect** – Look at how to protect your operational technology network and critical assets. There's unfortunately no silver bullet to this. You'll need to consider security at every stage, and put the maximum layers of defence to make any compromise as difficult as possible. This can include centralised protected data management, passive or active monitoring, and endpoint protection.

**Detect** – Carry out regular network audits and install the likes of anti-malware protection and firewalls so you can detect any suspicious activity. Here, it's helpful to share your experiences and talk to others so you can benefit from their best practices.

**Respond** – Make sure you have the tools and tactics to effectively react by contacting a professional consultancy service and participating in their workshops. This will help you to instil a continuous improvement culture within your business.

**Recover** – Put a disaster recovery plan in place. This will ensure you can maintain continuity in the event you do suffer a cyberattack. You can introduce resilience networking, and draw on knowledge from forums such as the National Cyber Security Centre's **Cyber Security Information Sharing Partnership**. Their website also has a wealth of relevant guidance and documents, along with updates on recently identified cybersecurity threats.

With these steps, it's important to note that you need to constantly ensure you're taking cybersecurity seriously. It's a continuous process framework, and so it's up to your business leaders to guarantee that a cybersecurity culture is present throughout the organisation once it has been applied.

## What preventative measures can I put in place?

There are also some very basic cybersecurity measures you can implement straight away:

- Ensure your systems are always updated to the latest version (especially for remote workers)
- Make firewalls active on all computers
- Only allow authorised and secured access to systems and databases
- Secure, protect and manage remote devices (like tablets and mobile phones)
- Don't ever use public WiFi
- Educate staff on cybersecurity best practices and question anything out of the ordinary
- Introduce a password change regime
- Make sure that no sensitive data is stored on third-party portals
- Migrate your office-based local servers to the cloud or a hybrid platform
- Frequently back up data and test your backups
- Speak to a trusted technology partner or technical consultant



We always recommend the final point here, as this will make it significantly easier to strengthen your cybersecurity overall. Introducing a data management strategy will also put you in control of your data, and allow you to effectively secure it. You should empower your IT department to manage the entire IT infrastructure, too, and grant them access to the latest technology in threat detection.

## Take cybersecurity seriously with **Made Smarter**

If you need help implementing cybersecurity practices, or would like advice on the current systems within your manufacturing organisation, our specialist business and technical advisers are on hand. Not only can we support you in uncovering the tools you may need to protect yourself, but we can also discuss how to fill any skill gaps you might have in your workforce.

What's more, Made Smarter's support is completely impartial, meaning we will always work in your best interests. To get started, **speak to our team today.**