



Cyber threat landscape for the manufacturing industry in 2025

UK organisations and businesses continue to be a prime target for cybercriminals. The news continues to report large scale cyberattacks against national and international businesses; this can give a false sense of security for smaller organisations.

When you look closer at the makeup of the UK business population, 99.9% are small and medium enterprises (SMEs). At the start of 2024, the UK government reported that 99.2% of SMEs were small businesses with fewer than 50 employees.

Of the estimated 5.5 million SMEs that operate across the UK, 5% of them are part of the manufacturing sector but, surprisingly, they account for 9% of employment and 14% of turnover. Adding to that, Make UK reported (July 2024):

- The UK is the 12th largest manufacturing nation in the world
- It contributed £217bn to the economy in 2023
- The sector employs over 2.6 million people
- It provides £38.8bn (14%) of total UK business investment

This makes manufacturing a high-risk and a lucrative target. The risk is growing further as manufacturing embraces smart factories, bringing operations online.

In recent times, the focus has been on external cyber threats, including ransomware and phishing. However, this has diverted attention from insider threat, a critical but often overlooked risk.

Recent reports have revealed that more than 70% of data loss is caused by careless or malicious insiders, highlighting the critical need for strong internal security measures.

In this blog post, we will explore the threat landscape across the UK for data loss, delving in to manufacturing specifically, combining internal and external risks and threats.

Why manufacturing is a target

As manufacturing continues to digitise operations, bringing factories and plants online often for the first time, this throws up a number several vulnerabilities. Cybercriminals thrive on exploiting vulnerabilities, making manufacturing a top target. In 2024, manufacturing was 3rd in the sector table of all data incidents reported to the ICO (Information Commissioner's Office), the independent body responsible for data protection and privacy in the UK.

Vulnerabilities

- **Productivity prioritisation:** Historically, maximised productivity is a top priority for the manufacturing sector. This now needs to be balanced with downtime for maintenance and patching of technology to ensure it remains secure. Any delay will leave the infrastructure open to compromise.
- **Legacy and specialist hardware and technology:** From a security perspective, legacy and aged technology and hardware is a challenge for all sectors but as these are moved online it becomes a significant risk for manufacturers. Devices can be out of support, no longer or have never had security patching, and expensive specialist equipment that can be irreplaceable or out of the reach of upgrades due to cost. Working closely with your cyber and IT support provider, they can implement security measures to ensure you have minimised any risk.
- **Employee experience:** Humans are the weakest link when it comes to cyber security, after technical controls. This is heightened if they are not experienced working online in a digital world in the workplace. By providing training and increasing awareness, they can become your greatest line of defence.
- **Organisational structure:** By nature, design and manufacturing facilities are siloed by department and division. This, combined with high email traffic internally and from external partners, creates a hotbed for email-based attacks such as phishing and business email compromise.

- **Complexity:** Manufacturing can be far more complex than other sectors – intricate and multifaceted production processes, along with product design, material sourcing, assembly, and quality control. There is often a requirement for multi-site operations to be identical and centrally managed. With so many moving parts, this can make implementing security measures more complex and increases the risk of missing critical processes, leaving vulnerabilities.

Why your business must protect confidential data

A PwC study found that 85% of clients would stop using a service provider if they perceived a lack of data security. Criminals exploit this, knowing organisations will go to great lengths to safeguard their reputation and client trust to avoid losing business and future opportunities.

Clients place a huge amount of trust in you to protect their data, assets and, in some cases, cash. It is, therefore, critical that your organisation has appropriate IT and cyber security measures and controls in place. Failure to do so could be catastrophic.

Not all businesses are created equal when it comes to the data that they collect, hold and process, so it is important that you take time to assess the risk should data be lost, stolen, or destroyed.

You must also consider your ability to continue to operate should the worst happen. Both your ability to generate revenue and your reputation could become unrecoverable.

What is a data loss event?

A data loss event refers to any incident where sensitive, confidential, or valuable data is lost, stolen or exposed, whether accidentally or through malicious intent.

Proofpoint recently reported that 85% of organisations worldwide experienced at least one data loss event in the past year, with the UK figure standing at 73%.

Alarming, 10% of affected organisations reported more than 30 incidents each.

The root cause of these breaches is surprising, with 70% of organisations that suffered a data loss event claiming it was due to human error or negligence.

In the UK, the Information Commissioner's Office (ICO), the independent body responsible for data protection and privacy, reported that, in 2024, 66% of all data incidents were non-cyber-related, further emphasising the role of human factors in data loss.

Ultimately, data loss is, at its core, a human problem. This risk is magnified when considering that many cyberattacks, such as phishing, rely on human interaction to succeed.

What is a careless user?

A careless user isn't necessarily acting with malicious intent. Often, their actions are simply mistakes. However, it doesn't matter whether a cybercriminal kicks down your front door or an employee accidentally leaves it wide open, the consequences are still equally devastating.

Common careless user actions include:

- Misdirected emails
- Engaging with a phishing attack

- Sharing data to the wrong person/organisation
- Installing unauthorised software

In 2024, Proofpoint reported that just 1% of users were responsible for a staggering 88% of data loss events.

After careless users, technical failures are the next leading cause of data loss. These can typically be traced back to two root issues: compromised systems and misconfigured systems, both of which often stem from human oversight, with around 50% of technical failures attributed to user mistakes.

Even simple errors are widespread. A third of employees admit to having sent an email to the wrong recipient at least once or twice. However, this figure is likely an underestimate. How many times have you mistakenly sent an email to the wrong person in the past year?

If we take this statistic at face value, an organisation with 500 employees could expect around 340 misdirected emails per year. Alarming, 84% of these emails in the past year contained sensitive attachments.

The impact of misdirected emails can range from mild embarrassment to severe reputational damage, financial penalties from the ICO, and legal consequences.

More than 90% of organisations that experienced an incident reported negative consequences, with over 50% facing business disruption and nearly 40% suffering reputational damage.

What is a malicious user/action?

As mentioned earlier, whether due to human error or malicious intent, the outcome can be the same. However, this risk should not be overlooked.

One of the most common causes of intentional security breaches is disgruntled employees, an issue that can be difficult to detect within an organisation.

Some warning signs are easier to identify, such as employees facing disciplinary action, those who have been passed over for a promotion, or individuals being monitored due to poor performance.

Ensuring that access to data and sensitive information is regularly reviewed, especially for employees in these situations, should be a key part of your security policies and procedures.

However, some risks are harder to spot. Employees experiencing financial hardship, struggling with mental health challenges, or dealing with addiction may be more vulnerable to committing malicious acts for financial gain.

One recent example of a malicious user is Rizwan Manjra, a 44-year-old motor insurance worker, who was sentenced for unlawfully accessing over 32,000 policy records and 160 claims not relevant to his job at Markerstudy Insurance Services Limited.

An investigation by the ICO revealed he accessed data outside work hours and shared personal information via his phone. He received a six-month suspended prison sentence and 150 hours of unpaid work, underscoring the importance of strict data access controls.

Data loss for the UK in 2024

In 2023, 33,383 data loss incidents were reported to the Information Commissioner's Office (ICO). The top 10 sectors made up 88% of incidents. Of these incidents, 66% are attributable to non-cyber events.

- Health (17%) 5,520
- Education and childcare (16%) 5,477
- Retail and manufacturing (12%) 3,871
- Local government (10%) 3,361
- Charitable and voluntary (8%) 2,777
- Finance, insurance and credit (7%) 2,386
- Legal (6%) 2,011
- Social care (5%) 1,515
- Land and property services (4%) 1,428
- Transport and leisure (3%) 949

The manufacturing and retail sector bucks the trend for cyber vs non-cyber incidents. Overall, the trend is around 60% non-cyber to 40% cyber. For your sector, 71% were recorded as cyber events.

The cyber-related incidents were primarily caused by:

- Ransomware (39%)
- Phishing attacks (34%)
- Other – non-categorised (18%)

The remaining 29% of incidents were categorised as non-cyber events, with the most common being:

- Unauthorised access (32%)
- Data emailed to the wrong recipient (16%)
- Other – non-categorised (19%)

Following these reported incidents, the ICO took various actions based on the severity and circumstances of each case:

- Informal action taken (65%)
- Full investigation pursued (1%)
- No further action required (26%)
- Cases remain open (8%)

In 2024, data breaches within the UK affected all sectors and between 45.6 million and 172.8 million individuals (data reported in ranges).

Unauthorised access

On analysis of incident type, one thing that stands out is that unauthorised access is a much bigger problem in manufacturing than other sectors. Across the UK, 13% of non-cyber incidents can be attributed to unauthorised access. Across manufacturing, this is 32%.

Unauthorised access is when an individual gain access to a system or data without permission. This can be non-cyber (employee) or cyber (cybercriminal). Employees can view, steal, delete and change data either by accident or with malicious intent. It is worth noting that viewing sensitive personal data without authorisation is classed a data breach, thus the employee is open to prosecution from the ICO.

Limiting any internal data loss or breach impact begins with access controls. The best practice is to apply least privilege and add timing limits when extensive access is required. This reduces the risk of employees accessing data either accidentally or intentionally.

Taking additional care with administrative and system-level accounts is also advised, ensuring those that require that access to perform their role do not use this as the day-to-day account, only logging in to those accounts when they need to perform an action.

Least privilege also limits the access of a cybercriminal should the employee's account be compromised during an attack. Combining this with multifactor or two-factor authentication, a secondary passcode sent to separate device, and strong password policies, all help to reduce risk.

External cyber attacks

Cyber criminals are constantly adapting, refining their techniques, and using more sophisticated tactics to target businesses. We explore the most common types of cyberattacks below.

Phishing (social engineering)

Phishing and similar attacks fall under the category of social engineering, where attackers manipulate individuals into revealing sensitive information or performing an action that compromises security. These methods allow cybercriminals to bypass technical controls entirely.

Phishing is not a new threat. Typically, attackers send mass emails impersonating legitimate organisations, attempting to steal sensitive information such as passwords or bank details – or to deploy malware, such as ransomware.

Gone are the days of easily spotted scam emails riddled with spelling mistakes and poor grammar. Today's cybercriminals are more sophisticated, even using AI-driven language models to craft convincing messages.

Phishing isn't limited to email. Attackers are also using texts and WhatsApp messages referred to as smishing, and vishing, the use of voice calls to solicit the same information.

Spear phishing: a more targeted approach

Unlike mass phishing, which casts a wide net in the hope of tricking as many people as possible, spear phishing is highly targeted. Attackers focus on specific individuals, gathering information from public sources such as social media or company websites to make their attacks more convincing.

Spear phishing messages are often designed to appear as if they are from a trusted colleague or senior figure within an organisation. Attackers may include personal details, such as the target's job role or recent projects, to increase credibility. By creating a sense of urgency, they pressure the victim into acting quickly without thinking critically about the request.

Whaling: CEO fraud & executive phishing

A newer and more sophisticated attack method that gained traction in 2024 is whaling, also known as CEO fraud or executive

phishing. These attacks target high-profile individuals, such as CEOs or CFOs, with the goal of stealing financial data or authorising fraudulent transactions.

Cybercriminals conduct extensive research on their targets, carefully crafting their messages to make them as believable as possible. These attacks are designed to fit the specific responsibilities of the executive being targeted. For example, an email directed at a CEO might focus on approving a financial transfer, whereas one aimed at a CFO could request access to sensitive financial reports. Attackers also add urgency and personalisation, making the request appear both genuine and time sensitive.

Phishing attacks are becoming more targeted because they are proving to be highly effective. Traditional phishing has an 18% success rate, while spear phishing is significantly more successful, with 53% of attempts leading to a breach. Although data on whaling is still emerging, it is expected to have at least a 53% success rate, if not higher.

A solicitor was found guilty of failing to prevent a 'Friday afternoon' cyber scam, which resulted in £290,000 being transferred to cybercriminals. The solicitor, deceived by a spoofed email address, sent the funds without taking additional verification steps. As a result, they were fined £10,000 and ordered to pay £16,000 in costs. This case highlights the devastating impact of phishing attacks and the importance of verifying financial transactions before processing them.

What your business should do if targeted by a phishing attack

If you receive a suspicious email, text or phone call, the most important step is to stop and think before taking action. Even if the request appears to come from a senior executive, always take the time to verify it through an alternative communication method. For example, if you receive an email requesting an urgent bank transfer, pick up the phone and call the person directly to confirm the request.

If you suspect you have fallen victim to a phishing attack, report it immediately. If a payment has been made, contact your bank as soon as possible to attempt to recover the funds. For all other incidents, notify your IT department so they can investigate and mitigate any potential damage. The faster an incident is reported, the better the chances of preventing further harm.

What steps can you take to reduce risk within your organisation?

One effective measure is to implement a "Report Phishing" button within your email system. The easier it is for employees to report phishing attempts, the more likely they are to do so. This helps IT teams detect and block phishing campaigns before they cause significant damage.

Providing continuous employee training is also essential. Regular phishing simulations can help staff learn how to identify and respond to suspicious emails, reducing the risk of human error leading to a security breach. Employees should be trained to look for warning signs such as unexpected requests for sensitive information, urgent language, or slight misspellings in email addresses.

It is crucial to foster a zero-blame culture within the organisation. If employees fear punishment for falling victim to a phishing attack, they may avoid reporting incidents, increasing the risk of further damage. Encouraging a culture of openness and support ensures that employees feel comfortable reporting security concerns without hesitation.

Ransomware

Ransomware attacks are a well-known cyber threat, well documented in the news and depicted in many films and TV shows. In these attacks, cybercriminals encrypt an organisation's data and systems, demanding a ransom for their release. Many attackers also threaten to publish stolen data online, using blackmail tactics to extort further payments.

The National Cyber Security Centre (NCSC) and UK law enforcement strongly advise against paying ransoms. According to the 2023 State of the Phish report, UK organisations reported:

- 63% had paid a ransom
- Only 34% fully recovered their data after payment
- 46% were forced to pay multiple ransoms
- 17% paid but received nothing in return

The NCSC and ICO encourage organisations to be transparent about ransomware incidents and seek their support. This can help your business recover, support investigations, and contribute to efforts in preventing future attacks.

How can you defend against ransomware attacks

As a manufacturer, you should implement these key measures to protect your business:

- **Regular backups:** Ensure data is backed up and stored separately from your operational systems to prevent attackers from accessing it.
- **Backup testing:** Regularly test your backups to confirm you can successfully restore data in case of an attack.
- **Follow best practices:** Strengthen security by implementing:
 - Two-factor authentication (2FA) for added protection
 - Patch Management to keep systems updated and secure

AI

Cybercriminals' use of AI technology isn't as new as you might think. Back in 2019, a UK CEO fell victim to an AI-powered voice spoofing scam. Believing he was speaking with his boss, the chief executive of the parent company, he was deceived by a cybercriminal who manipulated him into transferring \$243,000.

Today, AI is more advanced and widely available than ever. Many people have used ChatGPT or similar tools, and cyber security professionals are leveraging AI to combat threats.

Unfortunately, criminals also have access to their own AI-powered tools. On the dark web, WormGPT, a black-hat alternative to ChatGPT, has been developed with no ethical safeguards. This provides individuals with little or no technical expertise with the right tools and scripts to execute sophisticated cyberattacks.

When AI tools first emerged, the fear was that robots would replace human jobs. However, the real threat is not a robot – it's a human using AI to steal data, money, and identities.

The fight between security professionals and cyber criminals mirrors the classic good vs evil, cat-and-mouse struggle we see in films, with each side adapting to new technologies.

Hackers fall into three main categories:

- **White hat hackers:** Ethical hackers who simulate attacks (with permission) to identify vulnerabilities and help organisations strengthen security.
- **Black hat hackers:** Malicious actors who exploit systems for personal or financial gain.
- **Grey hat hackers:** A mix of both. They hack systems without permission but don't always act with malicious intent. Some inform organisations of vulnerabilities, often seeking payment to fix them.

Regardless of intent, all these groups are now integrating AI into their toolkits, making cyber threats more sophisticated and harder to detect.

How Net-Defence can help

Cyber security isn't just about investing in more tools; it's about having the right expertise by your side. Just as manufacturing employees require training and certifications, cyber security requires specialist knowledge.

Trying to manage security alone can leave gaps that cybercriminals are ready to exploit. Instead, manufacturers should work with trusted partners, like ourselves, to prevent, defend against, and recover from cyber threats.

Achieving industry-leading certifications, such as Cyber Essentials, keeping software and systems updated with the latest patches and accessing a Security Operation Centre (SOC) for 24/7 monitoring and threat mitigation are all critical steps in protecting your business.

At Net-Defence, we provide tailored cyber security solutions designed to meet the specific needs of your business.

We understand the unique challenges the manufacturing sector faces when it comes to IT security, compliance, and data loss prevention, ensuring your business remains protected.

By taking a proactive approach today, you can prevent costly breaches, safeguard your data, and protect your organisation's reputation for the long term.

Get in touch to learn more about how we can help.