Keep data safe with robust cybersecurity and IS0 27001 certification

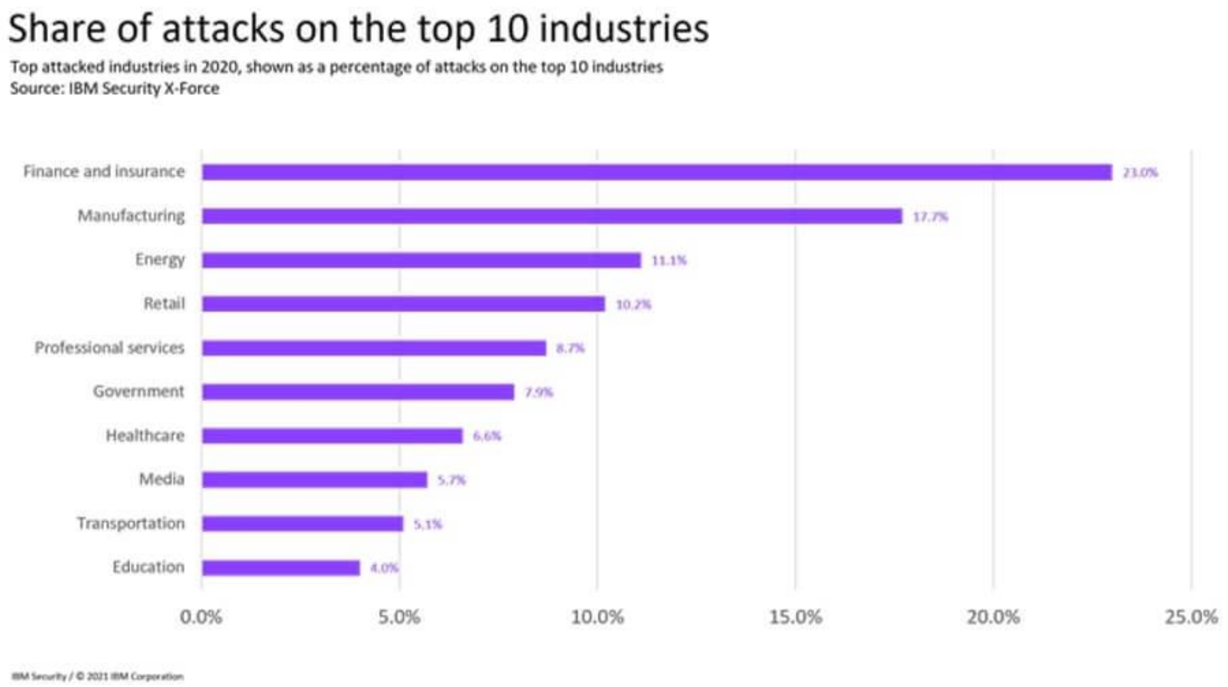
Companies that fall victim to cyberattacks must stop operations, lock down their systems, and often pay ransoms. And this is the best-case scenario. At worst, cybercriminals can steal intellectual property (IP), pilfer patents, and swipe sensitive financial information.

Not taking this seriously is akin to leaving your house open while you go away on holiday. Savvy OEMs (original equipment manufacturers) know this already and take security measures with their own systems. But what about when you outsource part of your operation? You want to ensure that your EMS (electronics manufacturing services) partner is as careful with your information as you are. You need to know they have the most robust information security management system (ISMS) possible.

Frightening stats about cyberattacks in manufacturing

- **969** – weekly attacks on businesses in the manufacturing industry during Q2 of 2022
- **33%** – the year-on-year increase (2021–2022) in weekly cyber attacks on companies in the manufacturing industry
- **350,000** – new types of malware registered by the AV-test institute every day

- **1143.46 million** – different types of malware identified by the AV-test institute that are currently in operation
- **17.7%** – the manufacturing industry was the second most attacked industry, with 17.7% of the total in 2020
- **21%** – of all ransomware attacks happen against companies in the manufacturing industry
- **x4** – four times as many BEC attacks were made on manufacturing companies than any other industry
- **42%** – nearly half of all British manufacturers were hit by a cyber attack in 2022



Share of attacks on the top 10 industries

Top attacked industries in 2020, shown as a percentage of attacks on the top 10 industries
Source: IBM Security X-Force

IBM Security / © 2021 IBM Corporation

Source: IBM X-Force Threat Intelligence Index

Why should the manufacturing industry prioritise cybersecurity?

It could be a Distributed Denial of Service attack, phishing attack, social engineering attack, BEC attack, ransomware attack, or remote access trojan attack. Whatever the attack, it will cost a business more than just money—lost IP and a damaged reputation are much worse.

Both OEMs and their EMS partners are prime targets as they store valuable information on their IT systems. Unfortunately, many companies have insufficient security in place to combat attacks.
EMS providers store sensitive client information, client lists, employee information, supplier information, and financial data—and criminals know this. By attacking EMS companies, cybercriminals can target secondary and even tertiary victims as part of the same network. One attack can lead to other attacks up and down the supply chain.

For example, in early March, Nvidia, a producer of chips and graphics cards, was attacked by the Lapsus$ group. One TB of data was captured, and the criminal organisation published the user credentials of Nvidia employees online, leading to a secondary wave of phishing, spear phishing, and brute-force attacks.

What basic measures should we take to prevent cyberattacks?

We can all adhere to several best practices in the manufacturing industry to reduce the risk of cyberattacks and protect systems and data.

- Implement strong security measures: This includes using strong passwords, regularly updating software and hardware, and implementing multi-factor authentication.
- Train employees on cybersecurity: Educate employees on how to identify and prevent potential cyber threats, such as phishing attacks.
- Conduct regular security audits: Regularly check and assess the security of your systems to identify and address vulnerabilities.
- Use secure communication methods: Use encrypted communication channels like VPNs to protect sensitive data.
- Regularly back up data: Regularly create backups of important data in case they are lost or compromised in a cyberattack.
- Use secure networks: Use secure networks, such as those with firewall protection, to reduce the risk of cyberattacks.
- Implement access controls: Use access controls to limit who has access to sensitive data and systems.

What robust measures increase cybersecurity?

There are also several additional measures EMS providers should be taking to ensure their—and their customer's—data are protected.

Understand your vulnerabilities and where you are at risk

Understanding how criminals attack cyber systems is the first step to preventing attacks by implementing counteractive measures. There are four critical areas where EMS providers are vulnerable.

- Cybercriminals can target Industrial Internet of Things devices. If a device is compromised and shipped to a customer, both businesses could be at risk.
- A compromised security update could infect an EMS provider with malicious code.
- Criminals could demand a ransom payment by impersonating a supplier using their credentials.
- If a supplier is infected with dormant ransomware, it can go undetected until it reaches the desired target.

Prepare for a cyber breach

Proactively preparing for an event rather than sitting back and hoping it won't happen is a sound approach. A dedicated cybersecurity team should audit what parts of the system can and should be strengthened.

EMS providers with cybersecurity insurance can also benefit from the insurer's expertise, which will help improve cybersecurity risk management tools and procedures.

Establishing a process plan to deal with a breach in the event of an attack is also a good idea, as robust procedures will ensure damage limitation.

What is ISO 27001, and how does it help protect sensitive data and information?

ISO 27001 is an international standard that outlines best practices and requirements for establishing, maintaining, and continually improving an organisation's information security management system (ISMS). It provides a framework for EMS providers to follow to effectively manage and protect sensitive information, including their customer’s personal data, intellectual property, and other types of confidential information.

One of the fundamental principles of ISO 27001 is protecting sensitive data and information by using appropriate controls. These controls can include technical measures such as encryption, access controls, firewalls, and organisational measures such as policies, procedures, and training.

By implementing the guidelines and requirements in ISO 27001, organisations can ensure that they have a robust and effective ISMS to protect sensitive data and information from unauthorised access, use, disclosure, disruption, modification, or destruction. This can help reduce the risk of data breaches, cyber-attacks, and other types of information security incidents and help companies maintain the trust and confidence of their customers, employees, and other stakeholders.

Why should OEMs require their EMS partners to have ISO 27001?

As OEMs entrust their EMS partner with important data, it is understandable that they may require ISO 27001 certification for several reasons:

Compliance: Many OEMs must ensure that their suppliers and partners comply with relevant standards and regulations. As ISO 27001 is a widely recognised information security management standard, having an EMS provider certified to this standard can help OEMs meet their own compliance requirements.

Data protection: OEMs entrust their partner with sensitive and confidential information, such as IP and customer data, that needs to be protected. An EMS provider that has implemented the controls and processes outlined in ISO

27001 can help to ensure that this information is handled securely and confidentially.

Risk management: OEMs are understandably concerned about the risk of data breaches, cyber-attacks, and other information security incidents that could negatively impact their business. By working with an EMS provider with ISO 27001 certification, OEMs can have confidence that their information is being managed and protected to minimise these risks.

Reputation: OEMs may also be concerned about their company's reputation and want to ensure that their EMS provider is seen as a trustworthy and reliable partner. An EMS provider certified to ISO 27001 can help demonstrate to customers, regulators, and other stakeholders that the OEM takes information security seriously.

Conclusion

Unlike security on the factory floor, ensuring robust cybersecurity is challenging as it requires addressing invisible risks. However, not being able to see these risks is no excuse for inaction. EMS providers have a duty to their customers to ensure they carry out basic and advanced cybersecurity measures and are ISO 27001 certified. After all, their customer's IP and data are at stake.