MAKE uk
The Manufacturers' Organisation

CYBER SECURITY IN MANUFACTURING

Foreword

The cyber risk in manufacturing is akin to an iceberg. Industry can plan and mitigate the risks they see, but in reality the biggest threats can cause the most damage. It's the vulnerabilities below the surface, in the systems, machinery and supply chains, that can catch businesses out.

And that's because manufacturing is distinctly at risk as digital systems are directly connected to physical production. Meaning that the risk doesn't stay in the digital world for too long. What starts as an IT issue very quickly becomes a production problem, a customer problem and a financial problem very quickly.

This report highlights the scale of the challenge facing manufacturers today, but it also shows that businesses are not powerless. Cyber risk cannot be eliminated altogether. What matters is understanding where the vulnerabilities lie, taking sensible steps to reduce them, and ensuring that when incidents do happen, they do not become business threatening events.

Manufacturers have always been good at managing risk. Cyber resilience should now be viewed in the same way: as a core part of running a successful, competitive and productive business.

Stephen Phipson, CBE

Executive summary: key statistics, messages and recommendations

The central message from this report is simple: cyber resilience is no longer just about protecting data, it is about keeping factories running, supply chains moving and customers confident. As factories, supply chains and customer systems become more connected, cyber incidents can quickly become production, delivery and commercial problems. The findings show that many manufacturers are strengthening their defences, but a significant minority remain exposed to disruption, particularly through operational technology, supplier dependencies and gaps in governance.

Key findings

- Most manufacturers are becoming more resilient: seven in ten (70%) avoided cyber incidents that affected operations, but nearly one in three (30%) still faced a serious incident directly or through their supply chain.
- Cyber resilience is now a commercial issue, 46% experienced increase of operational cost and production downtime. Customers increasingly want proof that manufacturers can protect data, keep production moving and avoid disruption.
- A cyber incident at one supplier can quickly affect many others, causing delays, experienced by 31% affected manufacturers, reduced capacity (31%) and shortages of components or materials (23%).
- Preparedness is improving, but it is still uneven. Many firms have basic protections in place, but gaps remain in patching, 51% has incident response plans, 45% has senior ownership and recovery testing.
- The current standards landscape can feel too complex, especially for SMEs. Manufacturers need a simpler, proportionate route to cyber resilience.
- Cyber resilience should help manufacturers adopt digital tools, automation and AI with confidence, rather than becoming a barrier to innovation.

1. CYBER IS OPERATIONAL RISK

Cyber incidents affect production, capacity, delivery performance and customer confidence, not just IT systems.

2. SUPPLY CHAINS CARRY RISK

Supplier incidents can reduce production capacity, delay deliveries and create shortages of components or materials.

3. RESILIENCE NEEDS GOVERNANCE

Controls matter, but resilience also depends on named accountability, tested plans and board-level ownership.

RECOMENDATIONS

FOR MANUFACTURERS:

Treat cyber resilience as a production priority; map critical systems and suppliers; test recovery plans; and ensure senior ownership of cyber risk.

FOR GOVERNMENT AND SUPPORT BODIES:

Make cyber support easier for SMEs to navigate, simplify cyber resilience standards so businesses have a clear and proportionate route to compliance, and embed cyber resilience into digital adoption programmes such as Made Smarter.

1. The current manufacturing cyber story: **connected factories, connected risk**

Manufacturing has a distinct cyber risk profile because digital systems are directly connected to physical production. Businesses rely on enterprise IT, operational technology, robotics, connected machinery, suppliers, logistics providers and customer systems. Which means for manufacturers, cyber incidents are not simply an information security issue. They can disrupt production, delay orders, affect customer relationships and create significant commercial costs.

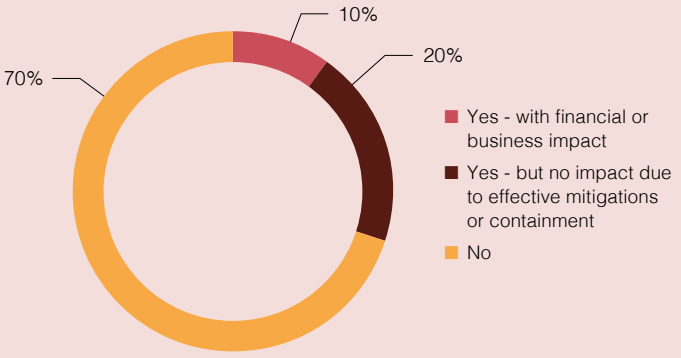
This is especially important in operational technology (OT) environments, where a cyber event or configuration change can affect machinery behaviour, safety controls and visibility on the factory floor. Could a cyber event or unauthorised change create a hazardous situation? If the answer is yes, the issue must be managed as both a cyber risk and a machinery safety risk.

Manufacturers depend on digital systems more than ever before. If those systems fail, production can stop, deliveries can be delayed and customers can be affected. The knock on effects can spread quickly through the business and its supply chain.

The risk environment has changed because IT and OT are increasingly connected. Machinery that was once isolated is now linked to business systems, cloud platforms, suppliers and remote monitoring tools. This brings real productivity benefits, but it also means equipment designed for reliability and long life can be exposed to modern cyber threats.

Seven in ten (70%) manufacturers report successfully avoiding any cyber incidents that would have affected operations over the past year. This may reflect increasing investment in cyber security and resilience across the sector. However, the fact that nearly one in three (30%) manufacturers have experienced an incident severe enough to affect operations demonstrates that cyber threats remain a significant business risk, with the potential to disrupt production, impact revenue and undermine customer confidence. Of those affected, 20% were able to mitigate the impact, while 10% faced financial costs and more severe consequences.

Chart 1: Cyber attacks and security incidents affecting manufacturing operations



Source: Make UK, Cyber Resilience 2026

The practical implication is simple: manufacturers should assume cyber risk is already present somewhere in their operating environment. The question is not whether every firm will be targeted, but whether they can spot weaknesses early, contain disruption quickly, and keep production moving when something goes wrong.

2. Manufacturing interconnected: **how the factory is targeted**

For manufacturers, the most serious threats are those that disrupt production, compromise supply chains or put valuable intellectual property at risk. Ransomware can lock production management systems such as ERP or MES platforms. Supply chain compromise can give attackers a route into larger customers through smaller, less well-resourced firms. Intellectual property theft can expose designs, processes and commercial advantage.

Cyber incidents through supply chain

Many manufacturers have strengthened their own cyber security in recent years. However, their exposure does not end there. Disruption elsewhere in the supply chain can still affect production, deliveries and customer commitments, even where a business' own systems remain secure.

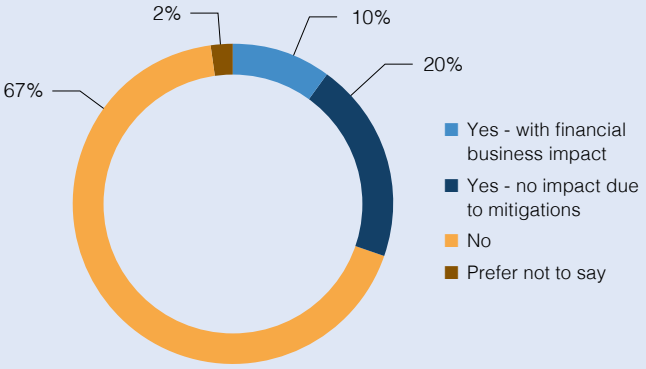
Supplier cyber incidents can create a similar operational impact to direct attacks. While two-thirds (67%) of manufacturers report no financial impact from cyber incidents in the past 12 months, one in ten (10%) experienced an incident with a direct financial impact and a further 20% reported successfully mitigating attacks before they caused business disruption. This suggests many firms are improving their resilience, but a significant minority still face risks that require active management and investment.

The ripple effects of supplier cyber attacks

The findings show the interconnected nature of modern manufacturing supply chains and the growing impact of third-party cyber risk. Among manufacturers affected by a cyber attack on a supplier, the most common consequences were delays to customer deliveries (31%) and reduced production capacity (31%). Nearly a quarter reported delivery delays from suppliers (23%) or shortages of components and materials (23%).

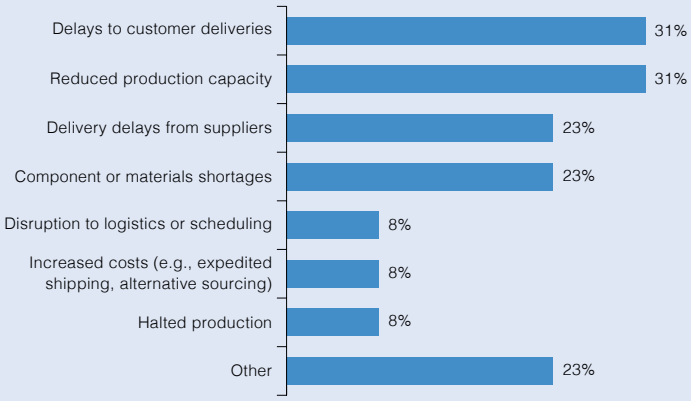
These results demonstrate that a cyber incident affecting a single supplier can quickly ripple through the wider manufacturing ecosystem, disrupting production, delaying orders and increasing operational pressures across multiple businesses.

Chart 2: Exposure to supply chain cyber incidents



Source: Make UK, Cyber Resilience 2026

Chart 3: How supplier cyber attacks affected businesses



Source: Make UK, Cyber Resilience 2026

Customer demand for cyber security compliance

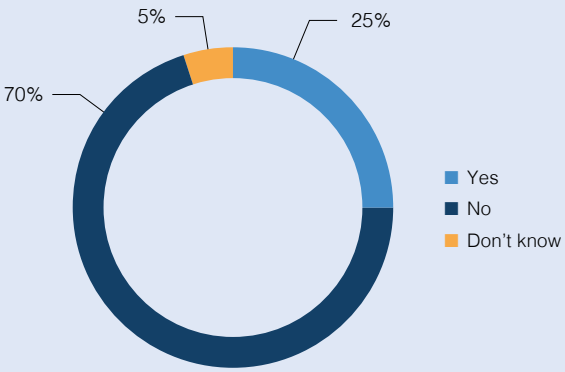
Good cyber security is becoming a commercial necessity. Customers want confidence that their suppliers can protect data, keep production running and avoid disruption. For some businesses, demonstrating those standards is now a requirement for winning and retaining work.

The reverse - supplier

The previous findings showed that customers are increasingly asking manufacturers to demonstrate cyber security compliance. However, cyber assurance is not a one way process. As manufacturers become more dependent on digitally connected suppliers, many are also seeking assurance that their own supply chains meet appropriate cyber security standards. This reflects growing recognition that cyber risk can originate anywhere within a connected supply network.

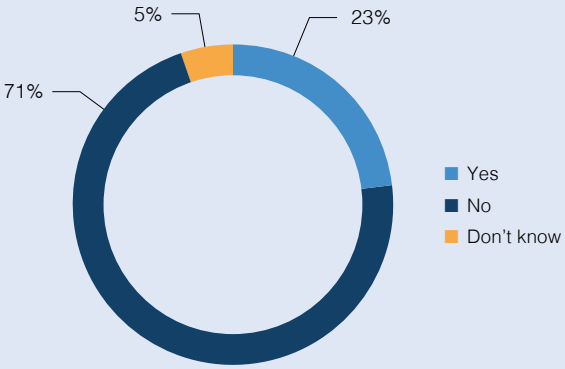
Cyber security assurance is increasingly flowing in both directions across manufacturing supply chains. Nearly one in four manufacturers (23%) report that they have asked suppliers to demonstrate cyber security compliance, closely mirroring the 25% that have been asked to provide similar assurance to their own customers. This demonstrates a growing awareness of third-party cyber risk and highlights how responsibility for cyber resilience is becoming embedded across supply chains. While most manufacturers have not yet introduced such requirements (71%), the findings suggest that cyber security is increasingly being treated as a shared responsibility rather than an issue confined within individual organisations.

Chart 4: Cyber security compliance requests from customers



Source: Make UK, Cyber Resilience 2026

Chart 5: Manufacturers requesting cyber security assurance from suppliers



Source: Make UK, Cyber Resilience 2026

3. Impact of cyber attack, disruption and cost

The cost of a cyber attack can vary significantly depending on the evidence source, the size and type of business, and the nature of the incident. Some estimates reflect direct financial losses, while others include wider operational impacts such as downtime, disruption to production, supply chain delays, recovery costs and reputational damage.

The figures below should therefore be read as indicative benchmarks rather than directly comparable costs.

Source	Focus	Key cost figure
UK Government (DSIT)	Significant cyber incidents in UK manufacturing	**£330,406** per attack[1]
ESET UK study	Operational disruption among UK manufacturers	**More than £250,000** for 52% of affected firms[2]
IBM Security / Ponemon	UK enterprise data breaches across sectors	**£3.29 million** per breach[3]
UK Government	Estimated annual cost of cybercrime to the UK economy	**£14.7 billion** (0.5% of GDP)[4]

However, the true cost of cyber incidents often extends far beyond direct financial losses. Understanding the financial impact of cyber attacks is therefore critical for assessing the business case for investing in cyber resilience.

Among manufacturers that experienced a financial impact from a cyber incident, costs were spread across a wide range of values. The most common reported impacts were either up to £10,000 or between £25,000 and £50,000, while fewer firms reported losses of £10,001–£25,000 or £50,001–£100,000. This suggests that the financial consequences of cyber incidents can vary significantly, with some manufacturers facing substantial costs from a single event.

Chart 6: Financial cost of cyber attacks

Cost band	Midpoint (£)[5]	% of firms
Up to £10,000	5,000	36%
£10,001-£25,000	17,500	14%
£25,001-£50,000	37,500	36%
£50,001-£100,000	75,000	14%

Source: Make UK, Cyber Resilience 2026

Using the midpoint of each cost range to calculate a weighted average, the estimated direct financial impact of a cyber incident on an affected manufacturer is approximately **£28,000 per incident**. This should be treated as a conservative estimate, as costs within the highest band may exceed £100,000 and significant indirect impacts, such as lost production and reputational damage, are not captured.

Among companies that experienced an impact, the most common consequences were increased operational costs (46%) and production downtime (46%). A further 15% reported supply chain disruption, data loss or breach, and ransom demands, while smaller proportions experienced reduced output, delayed customer orders or other impacts (8% each). These findings show that the cost of cyber attacks is often driven by business interruption and lost productivity, not just immediate IT recovery.

[1] Written questions and answers - Written questions, answers and statements - UK Parliament
[2] ESET reports 78% of UK manufacturers face cyber incidents as disruption becomes widespread - Industrial Cyber
[3] Cost of a Data Breach 2025: IBM Global Report | Northdoor
[4] Economic_modelling_of_sector_specific_costings_of_cyber_attacks.pdf
[5] Estimated average financial impact per affected manufacturer: c.£28,000 per cyber incident. Calculated using the midpoint of each reported cost band and weighted by the proportion of respondents. As the highest band is capped at £100,000 and indirect costs are not captured, the true average impact may be higher.

The most important point is that cyber incidents are not abstract technical events. Where they bite, they show up in the language manufacturers understand best: downtime, higher costs, disrupted schedules and pressure on customer delivery. That is why cyber resilience needs to sit alongside productivity, quality and health and safety as a core operational priority.

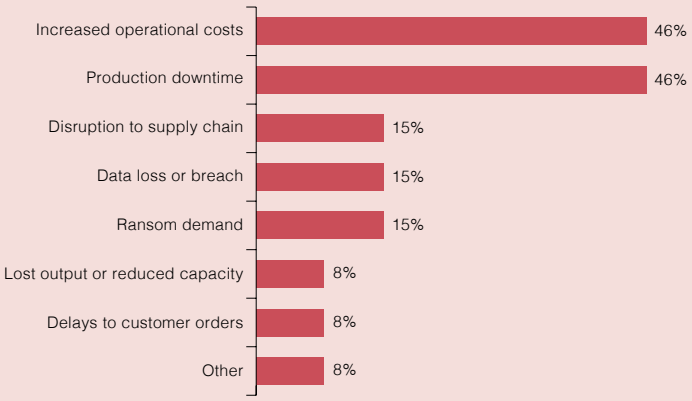
Chart 8: Comparative impact of UK manufacturing and supply chain cyber disruptions

Recent incidents show how cyber disruption can move quickly from a single organisation to wider production, logistics and supply chain impacts.

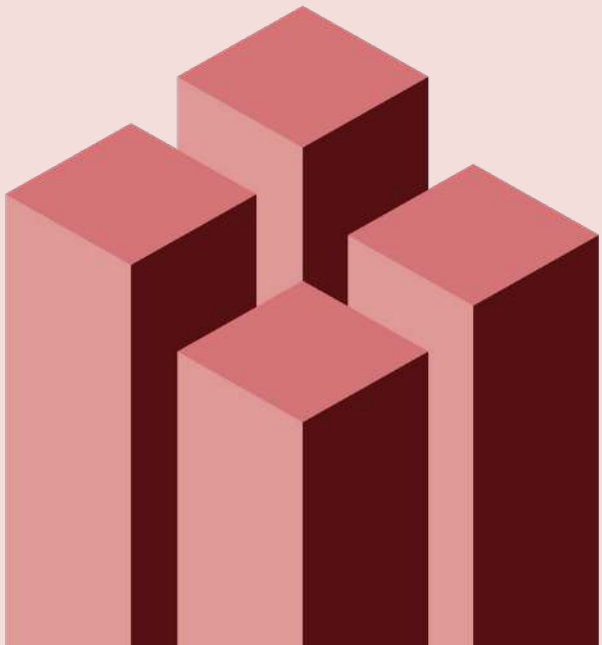
Company / incident	Operational disruption	Financial impact	Supply chain and wider impact
Marks & Spencer, 2025	Online orders and parts of retail operations were disrupted for several weeks, including a 46-day suspension of online clothing and home orders.	Reported cyber-related costs of around £131 million and an earlier estimated profit impact of around £300 million.	Disruption affected online fulfilment, store availability, logistics and customer service, showing how digital disruption can quickly affect physical retail and supply networks.
Stryker Medical, 2026	Global network disruption affected business operations, shipping and distribution, and halted production.	Financial cost was not confirmed in NHS England's public update.	The incident disrupted supply of medical equipment and consumables, with NHS England, DHSC and NHS Supply Chain working with the company to manage UK supply risk.
UK sector evidence	Incidents vary widely, but even short disruptions can create production delays and recovery costs.	DSIT-commissioned research indicates sectors including manufacturing can face average costs above £300,000 for significant cyber-attacks.	Wider impacts can include component shortages, missed delivery commitments, customer assurance pressure and higher costs across the supply chain.

What this shows: the longer production or logistics systems are unavailable, the more quickly the impact spreads beyond the breached organisation. Cyber resilience is therefore a supply chain, continuity and economic security issue, not simply an IT control issue.

Chart 7: Wider business impacts of cyber incidents



Source: Make UK, Cyber Resilience 2026



[6] Cost of a Cyber Attack 2026: UK Breach Costs | Ingenio
[7] Supply Issues Stryker Cyber Attack » NHS Supply Chain
[8] Summary of research on the economic impact of cyber attacks - GOV.UK

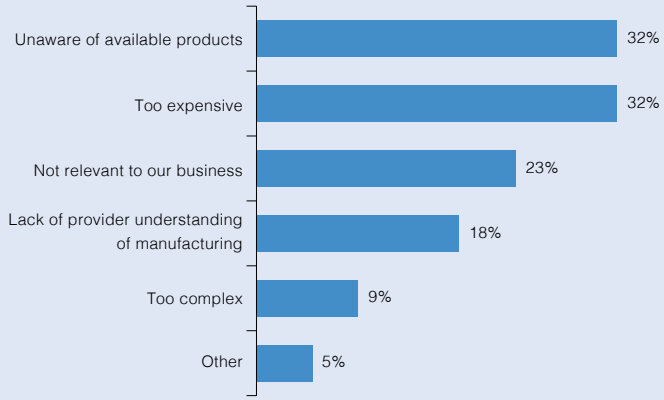
4. Barriers to cyber resilience

While manufacturers increasingly recognise the importance of cyber security, many still face practical barriers to improving their cyber resilience. These barriers can limit the adoption of cyber security products, services, standards and insurance, leaving businesses more exposed to cyber threats. Understanding these challenges is essential if manufacturers are to strengthen resilience while continuing to invest in digital technologies and innovation.

The survey highlights a combination of awareness, cost and relevance challenges. The most commonly cited barriers are a lack of awareness of available products and services (31.8%) and affordability (31.8%). More than one in five manufacturers (22.7%) believe available solutions are not relevant to their business, while 18.2% report that providers lack a sufficient understanding of manufacturing operations.

These findings suggest that the challenge is not simply one of cost. Many manufacturers struggle to identify solutions that align with the realities of industrial environments, including operational technology, production processes and business continuity requirements. A smaller proportion cite complexity as a barrier (9.1%), indicating that some organisations continue to face challenges navigating an increasingly crowded cyber security market.

Chart 9: Barriers to improving cyber resilience



Source: Make UK, Cyber Resilience 2026

- Cost and competing business priorities
- Lack of in house cyber skills
- Complexity of standards and guidance
- Limited awareness of government backed support

Cyber security and digital adoption

The findings reflect a wider challenge confronting the manufacturing sector. Across Make UK's technology and innovation work, cyber security is frequently identified as both an enabler of digital transformation and a barrier to adoption. Manufacturers are increasingly investing in digital technologies, automation, AI and connected systems to improve productivity and competitiveness. However, greater connectivity also increases exposure to cyber risks.

This creates a connected cycle. Businesses need digital technologies to become more productive and resilient, but concerns around cyber risk, cost, skills and security can slow investment and adoption. Equally, organisations that delay digital transformation may find it harder to implement modern security controls and build cyber resilience. The challenge therefore is not choosing between digitalisation and security but ensuring that cyber resilience is built into digital adoption programmes from the outset.

Our research suggests that improving cyber resilience requires more than simply increasing awareness of cyber threats. Manufacturers need affordable, accessible and relevant support that reflects the operational realities of industrial businesses. Greater engagement between providers and manufacturers, alongside stronger awareness of available products, services and frameworks, could help reduce barriers to adoption. As manufacturing becomes increasingly digital, cyber resilience must be viewed not as a separate challenge, but as a fundamental component of successful digital transformation.

5. Preparedness: confidence, controls and governance

As cyber threats continue to evolve, resilience depends not only on preventing attacks but also on having the people, processes and governance structures in place to respond effectively when incidents occur.

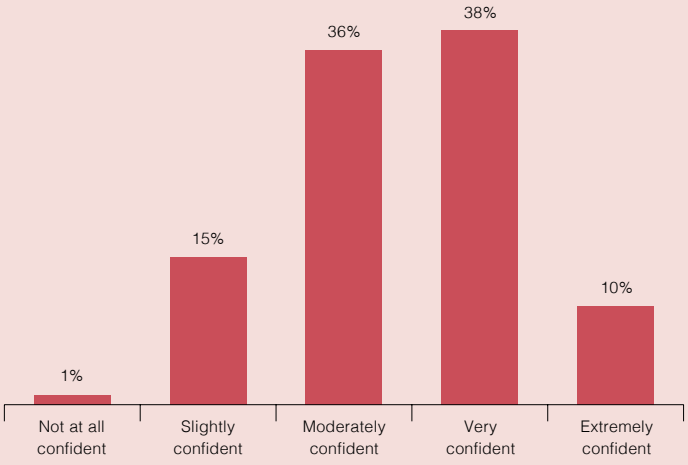
Understanding how confident manufacturers feel in managing cyber risk, the controls they have implemented and the governance arrangements supporting cyber security provides an important indication of the sector's overall preparedness. Together, these factors help determine how well businesses can withstand disruption, minimise downtime and maintain operational continuity in the face of growing cyber threats.

Confidence gaps

While many leaders express moderate to high confidence in managing cyber risks, a substantial minority report low confidence, especially in understanding which standards apply to them.

The confidence picture should be interpreted carefully. Confidence is useful, but only if it is backed by tested plans, clear accountability and evidence that controls work in practice. A firm may feel prepared because it has antivirus software and firewalls, but resilience also depends on whether leaders know who is responsible, what systems are critical, and how the business would recover if production stopped.

Chart 10: Confidence of manufacturers in cyber preparedness



Source: Make UK, Cyber Resilience 2026

Controls and governance

The findings suggest that most manufacturers have implemented a range of core cyber security controls, indicating a generally good level of cyber maturity across the sector. Firewalls are the most widely adopted measure (92%), followed by malware protection (80%), secure configuration (67%) and access controls (61%). These technologies form the foundation of cyber resilience and can help organisations prevent, detect and respond to common threats.

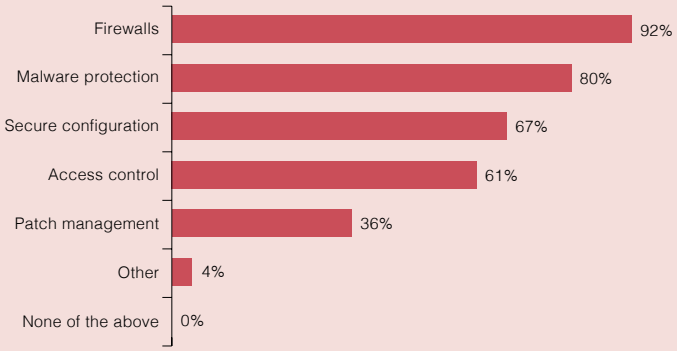
However, patch management is used by only 36% of respondents, representing a potential vulnerability. Keeping software and systems up to date remains one of the most effective ways to protect against cyber-attacks, particularly ransomware and the exploitation of known vulnerabilities. The findings suggest that while many manufacturers have invested in preventive controls, there remains scope to strengthen basic cyber hygiene and improve resilience against evolving threats.

Governance is where many manufacturers can make the biggest improvement. Cyber risk needs a named senior owner, regular discussion at board or risk meetings, and a simple incident response process. Without this, cyber security remains a technical task rather than a business risk that is actively managed.

For OT, governance needs to be joined up across engineering, production, maintenance, IT, health and safety, procurement and senior leadership. OT cyber security cannot sit with one team in isolation because machinery risk cuts across several areas. Clear governance should define how changes are approved, how suppliers access systems, how risks are escalated, and how cyber incidents are assessed for potential safety or production impacts.

Many manufacturers have adopted basic cyber governance measures, with 51% having incident response plans and 45% assigning senior leadership responsibility for cyber security. However, fewer than a quarter (23%) have a dedicated Chief Information Security Officer (CISCO), suggesting there remains room to strengthen cyber leadership, governance and organisational preparedness across the sector.

Chart 11: Cyber security controls in place



Source: Make UK, Cyber Resilience 2026

Chart 12: Cyber security governance and incident preparedness

Source: Make UK, Cyber Resilience 2026

Awareness of existing frameworks and standards

The current state shows both opportunity and confusion. Cyber Essentials, ISO 27001, the NCSC Cyber Assessment Framework and sector-specific guidance can all help firms improve assurance, but the landscape can feel crowded. The report should therefore avoid simply listing standards and instead explain the route: start with the basics, use proportionate assurance, and build maturity over time.

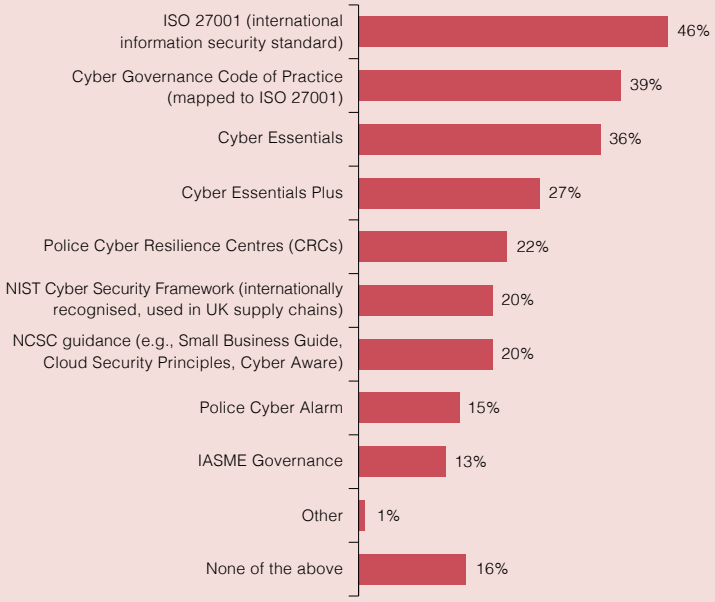
Insurance

Cyber insurance should be framed as part of resilience, not a substitute for it. Insurance can help firms manage the financial consequences of an incident, but it does not keep production running on its own. Businesses still need basic controls, tested backups, clear reporting routes and practical recovery plans.

Cyber insurance has become an increasingly important component of cyber risk management, helping businesses manage the financial consequences of cyber incidents and access specialist support during recovery. The survey shows that two-thirds of manufacturers (67%) have cyber insurance in place, indicating growing recognition of cyber risk as a business continuity issue rather than solely an IT concern.

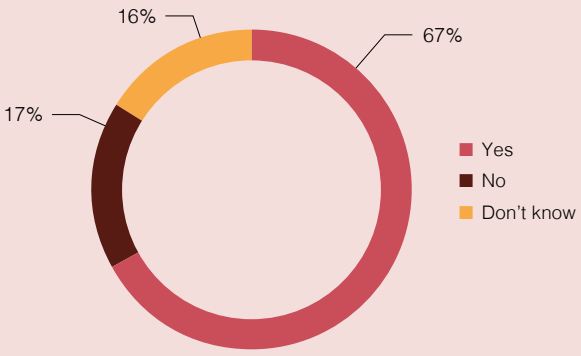
However, a significant minority either do not have cyber insurance (17%) or are unsure whether they are covered (16%). This lack of visibility may itself present a risk, as organisations could discover gaps in coverage only after an incident occurs. The findings suggest that while cyber insurance is becoming more common across the sector, many manufacturers may still need to review their coverage and ensure it aligns with their cyber risk profile. In addition, manufacturers often report that insurers lack a detailed understanding of industrial operations, making it difficult to obtain coverage that fully reflects the operational technology, production processes and business interruption risks unique to manufacturing.

Chart 13: Cyber security certifications, standards and guidance used by manufacturers



Source: Make UK, Cyber Resilience 2026

Chart 14: Cyber insurance coverage across manufacturing businesses

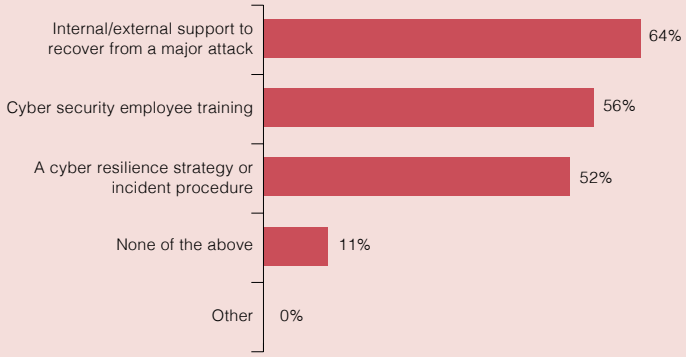


Source: Make UK, Cyber Resilience 2026

Our survey suggest that many manufacturers have taken practical steps to improve their ability to prevent, respond to and recover from cyber incidents. Nearly two-thirds (64%) have access to internal or external support to recover from a major cyber attack, while 56% provide cyber security training for employees. Just over half (52%) have a cyber resilience strategy or formal incident response procedure in place.

However, the findings also show that preparedness is not universal. More than one in ten manufacturers (11%) report having none of these arrangements in place, leaving them potentially more exposed to disruption when cyber incidents occur. While overall levels of preparedness are encouraging, there remains scope for manufacturers to strengthen their resilience by combining technical controls with training, recovery planning and governance.

Chart 15: How manufacturers prepare for cyber incidents



Source: Make UK, Cyber Resilience 2026

6. Strategic roadmap: **building the defensible factory**

The NCSC is actively engaged with the manufacturing sector to provide help in improving cyber security. At the Board level there is a Board Toolkit and the Cyber Security Code of Practice, which sets out the governance actions that board members need to take ownership of. This is backed up with an extensive e-learning suite.

Manufacturers can also sign up to the Early Warning service which provides automatic alerts to the presence of malware and vulnerabilities on their networks. If organisations wish to test their incident response procedures, Exercise in a Box is a collection of ready-made exercises that organisations can download to create their own incident response exercises.

NCSC runs a trust group for manufacturers where members come together and share good practice, common experiences, and hear from external experts on topics of interest, backed up by dedicated SLACK channels.

The group also seeks to do work that will strengthen cyber security in the sector, such as exploring ways to get Cyber Essentials embedded more deeply into the supply chain. The NCSC emphasises that the most significant improvements in cyber resilience come from getting the fundamentals right, which is what Cyber Essentials is designed to support.

Those with an interest in industrial control systems can join the ICS Community of Interest, which runs regular webinars on ICS security topics, and which has a number of expert groups looking at specific ICS cyber security issues.

Key OT message

Cyber security, machinery safety, software integrity and control system reliability are now closely linked. For Operational Technology, manufacturers need to understand not only whether a machine works, but whether it is protected from unauthorised or accidental change.

The practical test: could a cyber event or unauthorised change create a hazardous situation? If yes, it must be managed as both a cyber risk and a machinery safety risk.

7. Recommendations

- **Make cyber resilience a production priority:** treat cyber security as part of operational performance, continuity and competitiveness, not as a narrow IT responsibility.
- **Map the systems and suppliers that keep the factory running:** identify the machinery, platforms, service providers and supply chain dependencies that could stop production if compromised.
- **Test recovery, not just response:** run practical exercises that ask how quickly production schedules, orders, logistics and customer commitments can be restored after an incident.
- **Close the cyber resilience gap for SMEs:** make guidance, assurance requirements and affordable tools easier to navigate so smaller manufacturers are not left carrying risk for the wider supply chain. Enhance Made Smarter Adoption Programme with cyber resilience training.

Conclusion

Manufacturing can no longer treat cyber risk as a distant technical threat. It is now part of the day-to-day operating environment for every connected factory, every digital supply chain and every business investing in automation, AI and advanced manufacturing. The good news is that disruption is not inevitable. Seven in ten manufacturers avoided cyber incidents that would have affected operations over the past year, showing that investment in controls, preparation and resilience is already making a difference. But the warning is just as clear: nearly one in three experienced a serious incident directly or through their supply chain. When cyber incidents break through, they do not stay in the IT department. They stop production, increase costs, reduce capacity, delay orders and put customer confidence at risk.

The challenge now is making sure disruption does not become the new normal. Manufacturers cannot prevent every attack, but they can be better prepared for them. Businesses that understand their risks, strengthen their defences and plan for incidents will be in a much stronger position than those that assume it won't happen to them.

The UK's manufacturing ambitions are built on digitalisation, automation and greater connectivity. Cyber resilience needs to grow alongside them. Without it, the benefits of digital transformation will always be undermined by the risks that come with it.

Make UK is backing manufacturing – helping our sector to engineer a digital, global and green future. From the First Industrial Revolution to the emergence of the Fourth, the manufacturing sector has been the UK's economic engine and the world's workshop. The 20,000 manufacturers we represent have created the new technologies of today and are designing the innovations of tomorrow. By investing in their people, they continue to compete on a global stage, providing the solutions to the world's biggest challenges. Together, manufacturing is changing, adapting and transforming to meet the future needs of the UK economy. A forward-thinking, bold and versatile sector, manufacturers are engineering their own future.

www.makeuk.org
@MakeUKCampaigns
#BackingManufacturing

For more information, please contact:

Nina Gryf
Senior Policy Manager
Make UK
ngryf@makeuk.org

makeuk.org

~~KF.06.05.2025~~