In association with:

BlackBerry | Cybersecurity

MAKE uk
The Manufacturers' Organisation

CYBER SECURITY
IN UK MANUFACTURING

blackberry.com/us/en

makeuk.org

EXECUTIVE SUMMARY

Nearly half of the UK's manufacturers (42%) have been a victim of cyber-crime over the last 12 months, but the majority (74%) said that the cyber protection processes they had in place prevented any business impact whatsoever. However, the remaining 26% revealed they had sustained substantial financial loss, and of those answering the survey question, those losses ranged from £50,000 to £250,000.

LOSSES DUE TO CYBER ATTACK RANGED FROM £50K TO £250K

An added risk for companies has been the need to speed up the adoption of digital processes to boost production in today's challenging economic climate. This increase in the implementation of technology solutions at the heart of production operations has led to an increased emphasis on cyber security within businesses, with 95% of companies reporting that cyber security is a necessary function of their operations. However, the known additional cyber risk for a little over a third of companies (37%) has stopped them investing in technological advances through interconnectivity which is hampering potential productivity gains.

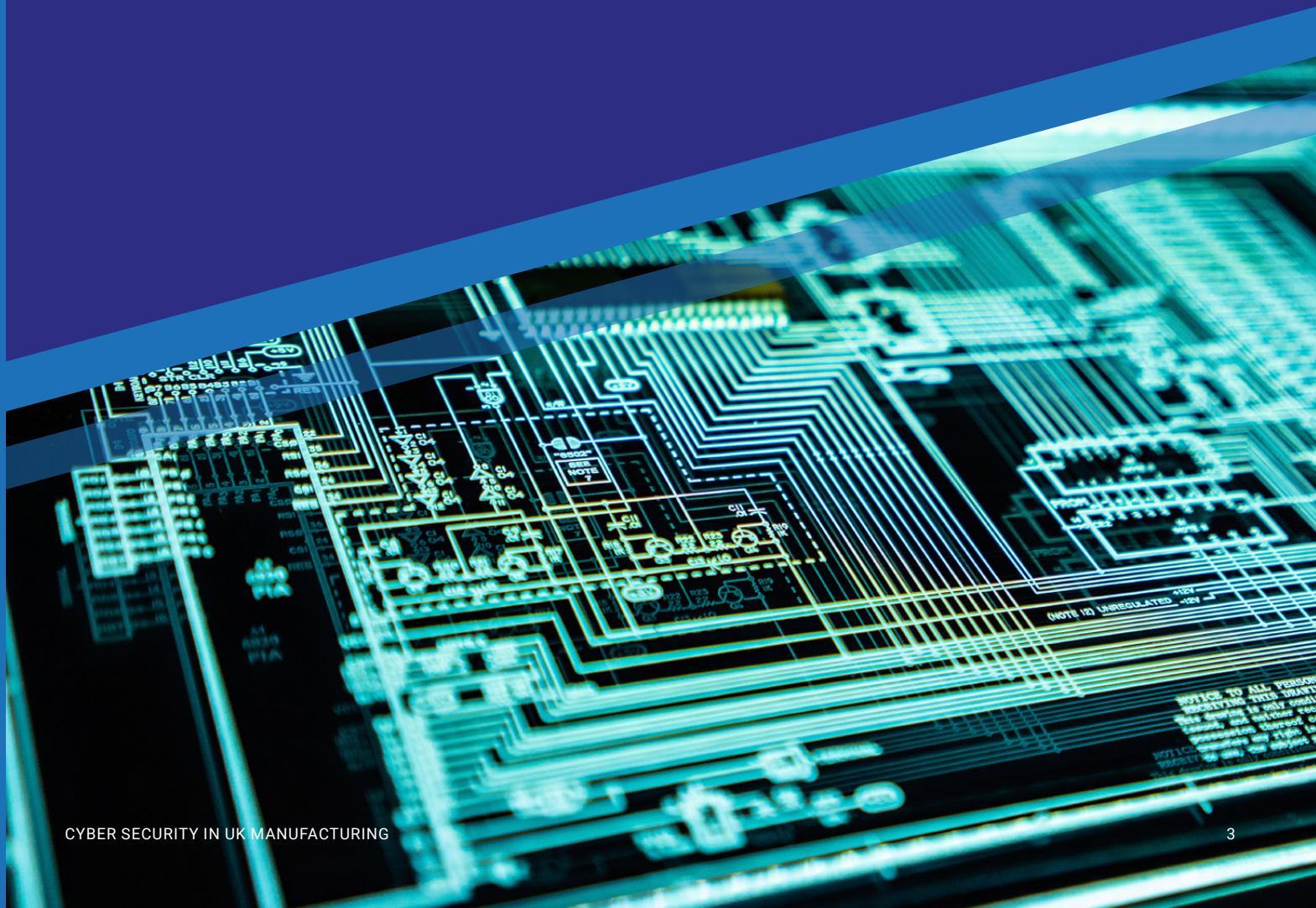
This new report reveals that targeted attacks are the most common, with operational disruption the most frequent result of a cyber incident. Reputational loss is the second most significant issue for companies, with customers looking for evidence of cyber protection. Legacy IT within a business was found to be the most common risk to manufacturers (45%) followed by a lack of cyber skills. The necessity of providing access to third parties for monitoring and maintenance is the third most frequent reason for a cyber incident amongst manufacturers.

Despite knowing the risks, the majority of companies (54%) have not taken further cyber security action even after adopting new technologies. Only those who have introduced systems from the Internet of Things – which encompasses functions such as sensors driving production line efficiencies – appear to have invested heavily in cyber protection. These IoT technologies often lie at the centre of the manufacturing process and are seen as business critical, driving companies to spend more to protect them.

Employee error remains the most common reason for a cyber-attack. 62% of companies now offer cyber security training to their staff to cut this risk. Smaller companies are still doing less, with just 50% of companies with staff levels of 0-9 employees offering any training at all. Some 62% of manufacturers now have a formal cyber security procedure in place in the event of an incident, up 11% on last year's figures. And encouragingly 62% of the industry now say that there is a senior manager involved in a cyber security committee within the business while 58% told us that a main board director is responsible for driving cyber protection for the firm.

The composition of cyber defence is wide – with 89% of companies investing heavily in antivirus software and firewalls to secure internet connections. Very few companies, under one per cent, report not having any technical mitigation at all in place to protect against unwanted intrusion. Russia and China hold equal spot with 75% of manufacturers perceiving a cyber threat originating from these regions, followed by the EU (25%) and the USA (23%).

The main barriers to companies increasing their level of cyber security remains the initial cost of cyber protection products, with just over four in ten manufacturers saying that is the main block. The second most cited barrier is the cost of maintaining these security systems, with 35% of the industry suggesting this is a key barrier.



CYBER SECURITY AND ITS IMPORTANCE TO UK MANUFACTURING

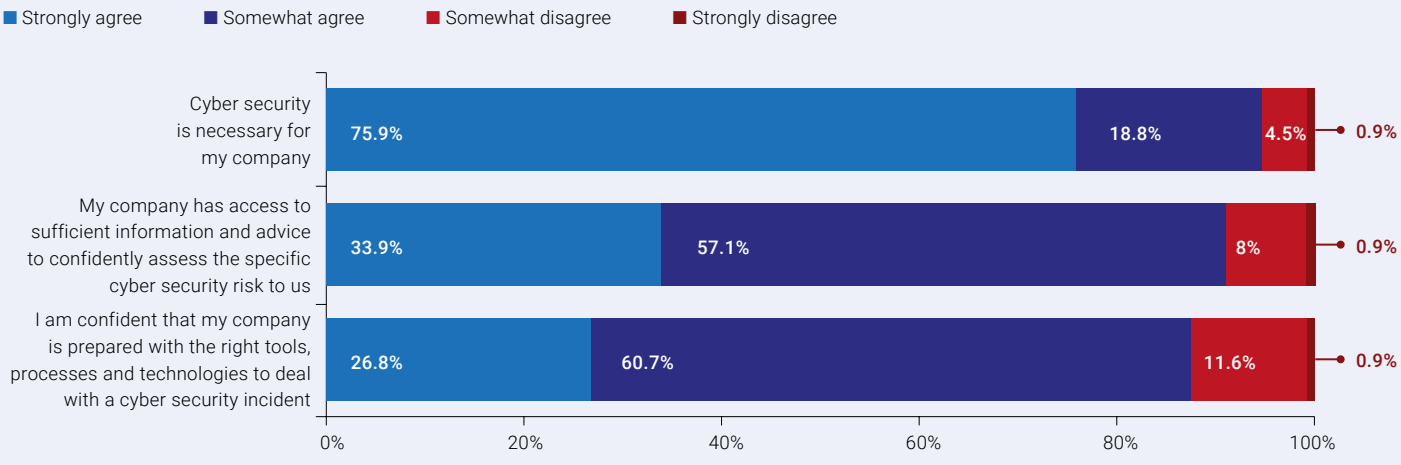
UK manufacturing is an advanced industry, with the challenging business environment over the past few years only accelerating the rate at which businesses have turned to technology to produce higher quality products with greater efficiency. From the back office to the beating heart of the shop floor, modern manufacturing processes have never been more digitally interconnected. However, with these advancements, comes an increased industry exposure to cyber security threats.

Despite the clear benefits brought by advancement in production technologies, manufacturers have also needed to mitigate the vulnerabilities that connected technologies bring to their business. Awareness of this threat is pervasive across the sector, with 95% of manufacturers reporting that cyber security is a necessary function of their operations. For firms with 500 or more employees, 100% report that cyber security is necessary for their business.

Nevertheless, the question of information and appropriate defence is more nuanced. While Chart 1 shows that 91% of manufacturing companies suggest they either agree or *somewhat* agree that they have access to sufficient information and advice to confidently assess the specific cyber risk that faces their business, the majority (57%) are at the lower end of the scale and only somewhat agree. Similarly, when considering whether their company is prepared with the right tools, processes and technologies to deal with a cyber security incident, 88% strongly/somewhat agree, but the figure that only somewhat agree is 61% of the industry. This is illustrated by the comparatively large middle sections seen in the lower two questions contained in Chart 1.

What this reveals is a confidence gap between UK manufacturers knowing that cyber security is of paramount importance to their businesses, but less certain in just how those risks present themselves and subsequently what the best forms of defence are for a given risk.

Chart 1: Strong confidence that Cyber Security is paramount, more uncertainty about risks and appropriate mitigations



Source: Make UK Cyber Security Survey 2022

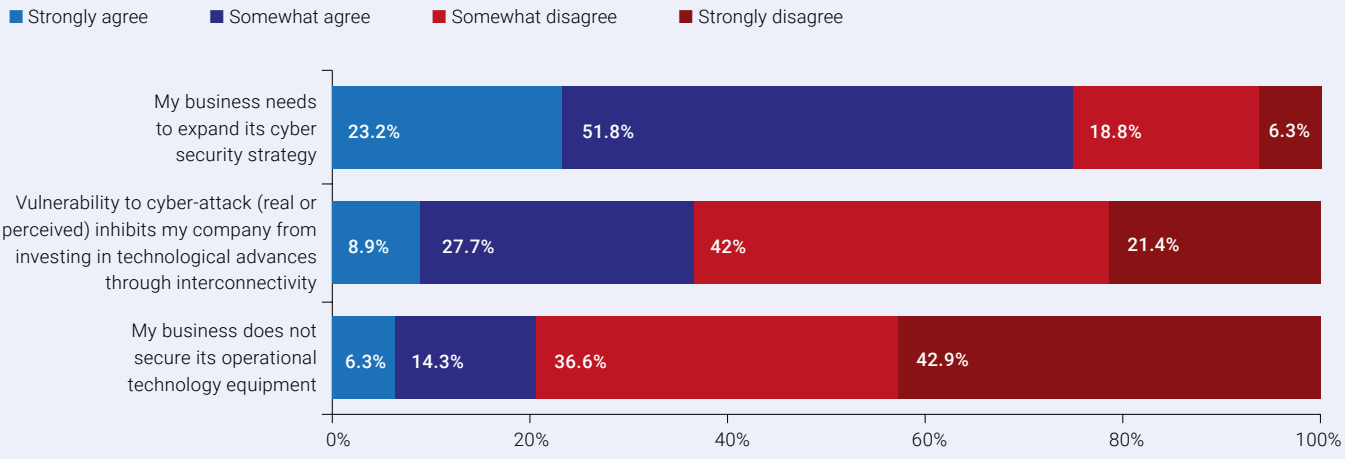
This uncertainty is driven by both manufacturers themselves and threat actors. In the first instance, continued digitalisation in the manufacturing industry opens up new vulnerabilities that require new mitigations – something, as the data suggests, that industry has a strong understanding of. Then there is the evolution of cyber threats posed to businesses which also develop over time, often in direct response to the security measures put in place to mitigate them.

Given this uncertainty, it follows then that UK manufacturers need to review and increase their cyber security posture in response to this ever-evolving threat. The data shows just this, with three out of four in the industry reporting that their business needs to expand its cyber security strategy. Only 6%, as measured by those businesses that suggest they 'strongly disagree' with this sentiment, of the industry are entirely satisfied with their cyber security strategy as it currently stands.

A little over a third (37%) say that it is this added vulnerability to cyber attacks, created by investing in modern technologies, that inhibits their company from investing in technological advances through interconnectivity. While in the minority, this group nonetheless highlights a key area where technological progress is being limited by the threat of cyber incidents. This inhibition will limit potential efficiency and, in turn, productivity gains readily available to this 37% of the industry that advancement might otherwise offer.

Despite an overwhelming proportion of industry suggesting that cyber security is important to their business, by comparison, a significant one in five manufacturers reports not securing their operational technology equipment. Again, this lends further evidence to the confidence gap, where the perception of cyber security importance is almost unilateral, but the actual reported deployment of these security measures in businesses falls below required levels.

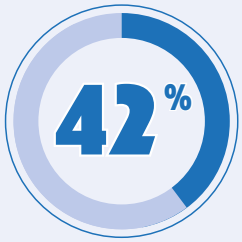
Chart 2: Industry reports that its cyber security strategy requires expansion



Source: Make UK Cyber Security Survey 2022

HOW OFTEN DO MANUFACTURERS BEAR WITNESS TO A CYBER ATTACK ON THEIR BUSINESS, AND DO BUSINESS' CYBER SECURITY STRATEGIES PROVE EFFECTIVE?

Over two-fifths (42%) of manufacturers report being subject to a cyber incident in the last 12 months, with the majority suggesting that the business impacts of any attack or incident were mitigated by the security measures they had in place. Of those that had endured a cyber incident of some form over the past 12 months, just under three quarters, 74%, say that their cyber security processes prevented any business impact, with the remaining 26% saying that they had sustained financial or other business losses due to the attack.



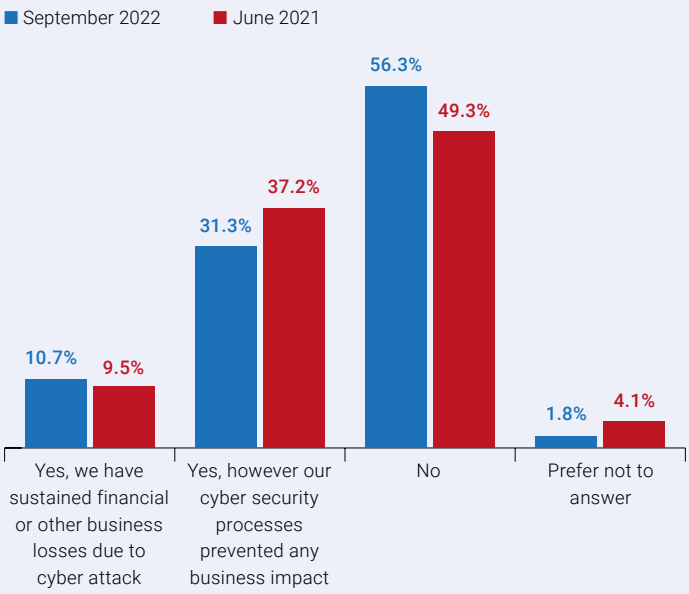
OF MANUFACTURERS REPORT ENDURING A CYBER INCIDENT IN THE PAST 12 MONTHS

However, those that have endured an attack, successfully or not, remain in the slight minority, as 56% of the industry report that they have not – or are not aware that they have – been subject to a cyber attack or incident in the past 12 months.

The prevalence of reported attacks has stayed roundly consistent between Make UK's 2021 research on cyber security and this 2022 report, as illustrated in Chart 3. Not only has the prevalence of attacks remained consistent, but the degree to which attack impact has been successfully mitigated has remained roughly consistent also, albeit with the caveat that there has been a 1.2% increase in those reporting attacks that have incurred financial or business losses. The largest shift between 2021 and 2022 has occurred in those reporting no cyber incidents or attacks in the past 12 months, with the proportion of industry suggesting as much down by 7% compared to last year.

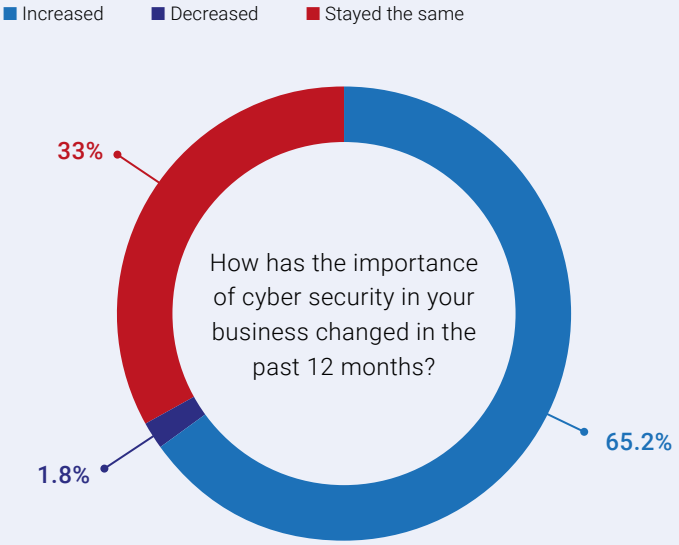
Nevertheless, the growth in the importance of cyber security in the past 12 months is significant. Just under two-thirds, 65%, of UK manufacturers say that the importance of cyber security in their business has increased in the past 12 months, with only a fractional 2% reporting that cyber security's importance has decreased in that same time.

Chart 3: Cyber security processes fend off the impact of the majority of reported attacks



Source: Make UK Cyber Security Survey 2022

Chart 4: Clear trajectory of the increase in the importance of cyber security throughout 2022

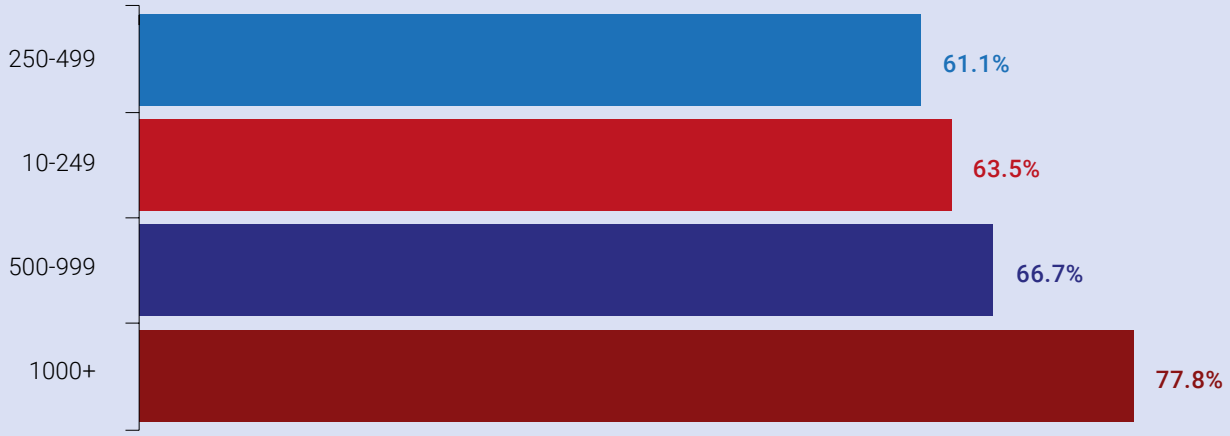


Source: Make UK Cyber Security Survey 2022

LARGEST OF COMPANIES SEE A GREATER FOCUS ON CYBER SECURITY

When we break down the data by company size, we see that it is those largest companies, with over a thousand employees, that have seen the importance of cyber security grow within their businesses the most. While other headcount bands remain close to the overall average of 65% that report seeing the importance of cyber security grow in their business over the last 12 months, 78% of companies which have a thousand employees or more report this to be true, which is 12% greater than the average.

Chart 5: % manufacturers reporting an increase in the importance of cyber security to their business in the last 12 months



Source: Make UK Cyber Security Survey 2022

Larger companies are more likely to have a greater amount of interconnected technologies within their business, and across multiple sites as well, which increases their businesses' attack surface area. It's this vulnerability which is driving the largest companies to put the greatest stock in their cyber security strategies compared to the average.

IDENTIFYING RISK, ITS DRIVERS, AND ITS CONSEQUENCES

UK manufacturers face a battery of cyber security risks, ranging from simple employee error all the way to complex targeted attacks. As part of this fieldwork, we set out to understand the hierarchy of these risks to manufacturers, and what the consequences to businesses are if these risks are realised.

MANUFACTURERS ORDER THE TOP THREE CYBER SECURITY RISKS TO THEIR BUSINESS:

45%

#1: MAINTAINING LEGACY IT

38%

#2: LIMITED CYBER SECURITY SKILLS WITHIN THE BUSINESS

33%

#3: PROVIDING ACCESS TO THIRD PARTIES FOR MONITORING AND MAINTENANCE

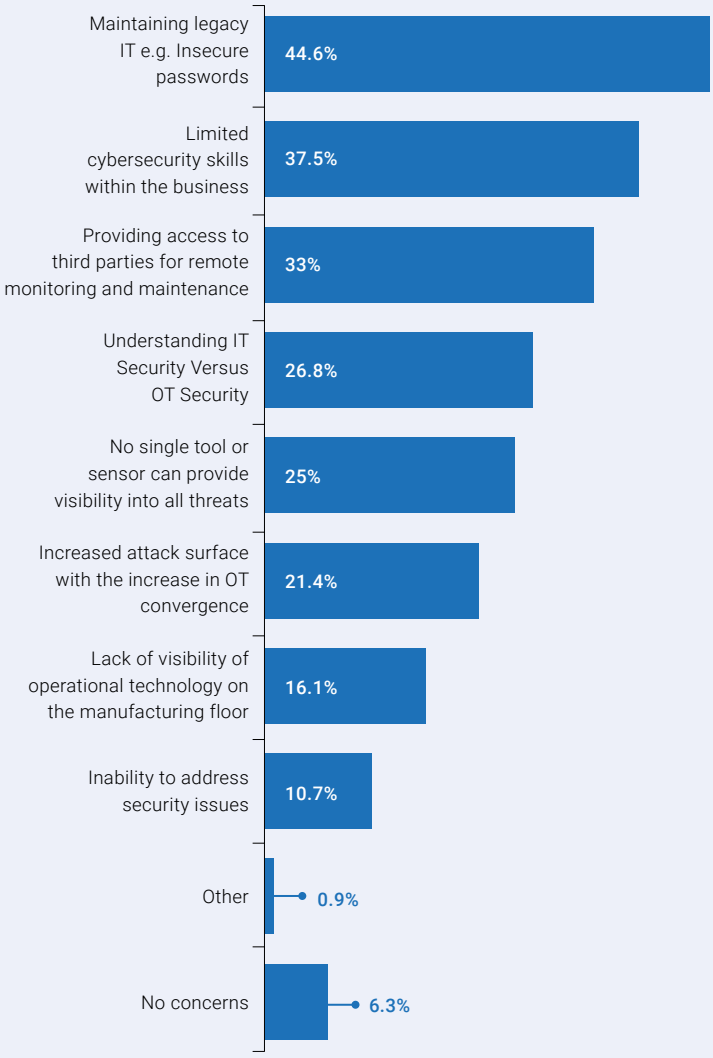
Despite continually evolving technology being implemented in manufacturers' processes as part of their journey towards digitalisation, maintaining legacy IT presents as the most prolific cyber security risk in UK industry. While this may seem counterintuitive at the outset, there is a clear rationale. Cyber security can sometimes, incorrectly, be seen as a static piece of defence that companies implement. However, a cyber security implementation that a business has put in five or even ten years ago, may be entirely defunct in the present day. This is because, while the implemented defence may not have faltered, the threat it was designed to combat has almost certainly evolved, perhaps even in direct response to the form of the very defence itself.

Legacy IT within businesses proves a cyber security threat because if developers are not actively patching software, there are still likely exploits to be found in the future. Whether it is because the software in use by a given manufacturer has been abandoned by its creators, or whether a business has chosen, or cannot afford, to keep up to date with the latest versions, the outcome is similar: software embedded in manufacturers' processes to which there are known exploits or exploits yet to be found, with no hope of the first party developer being able to remedy them.

Perhaps one of the most pervasive recent examples of this risk being realised was seen in the 2017 'WannaCry'[1] global ransomware attacks, which manifested as a 'cryptoworm' that would affect, almost exclusively, legacy versions of the Microsoft Windows operating system, encrypting data and demanding ransom in cryptocurrency for the files to be released. This attack came to national attention when the NHS was struck, causing pandemonium in the UK's healthcare system. One of the largest car manufacturers in the UK, was also struck by the same attack, and so too was Renault in France, where production stoppage was reported as a result.

[1]"Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland..." The Independent May 2017

Chart 6: Manufacturers reporting the main operational technology security concerns in their business (selecting three)



Source: Make UK Cyber Security Survey 2022

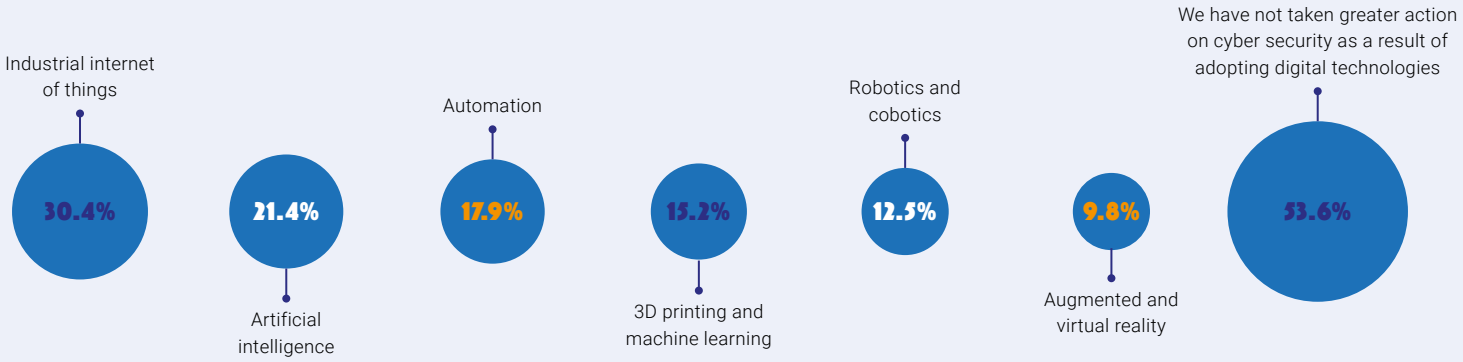
The second most cited cyber security risk is related to a business' employees themselves, with 38% of manufacturers reporting that it is limited cyber security skills within the business that poses a threat. This finding is juxtaposed with a later finding in the report in the business action section, which suggests that the majority of manufacturers do have cyber security training procedures in place for all employees. Nevertheless, human error and human exploits are common cyber threats many businesses face. Typically these risks present themselves in the form of emails containing malicious links, attachments or requests for information from imposters. However, in the extreme, it can range to complex social engineering attacks with the goal of compromising business systems.

As businesses adopt more digital technologies, the exposure to cyber security risks increases. In turn, manufacturers respond by reassessing or increasing their level of cyber security. But which of the most adopted digital technologies within manufacturing environments are driving the increased need for cyber security?

Businesses that have implemented the industrial internet of things (IoT) report it to be the biggest driver in increasing their overall level of organisational cyber security. IoT, in comparison to augmented and virtual reality, for example, can often lie closer to the heart of a manufacturing production process, and in turn become operationally critical. Whether it be sensors throughout the plant to ensure quality on the production line, or whole line units themselves, the criticality to manufacturers is evidenced by 30% of the industry reporting that implementing IoT within their businesses has subsequently led them to increase their level of cyber security.

The second largest driver of enhanced cyber security is artificial intelligence, with 21% of the industry saying it has driven an expansion in the cyber security strategy, followed by automation ranking as the third biggest driver with 18% reporting the same effect.

Chart 7: The industrial Internet of Things and artificial intelligence a revealed to be the most driving technologies for increasing cyber security within a manufacturing business



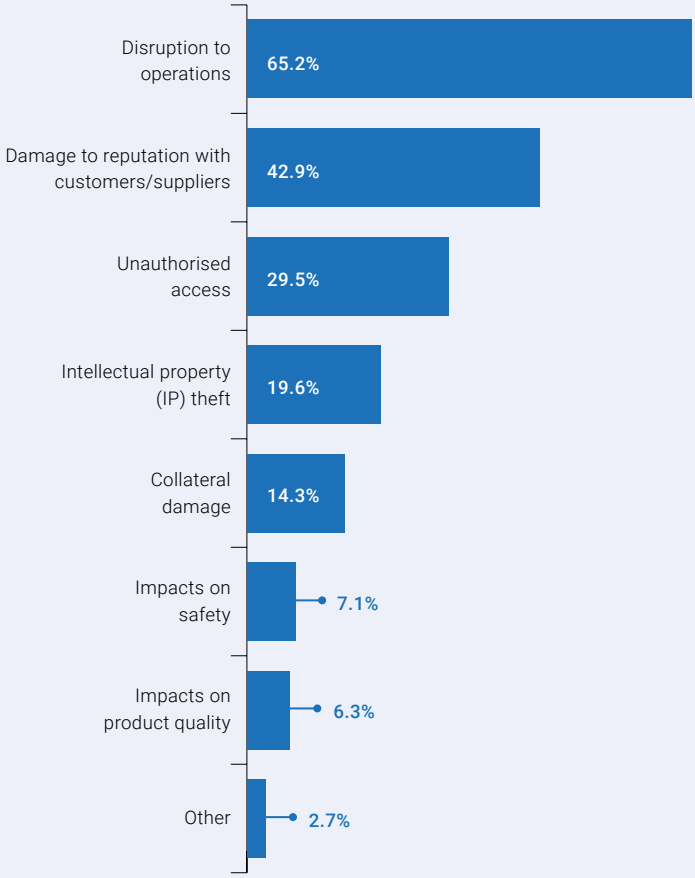
Source: Make UK Cyber Security Survey 2022

What are the business ramifications for a manufacturer that suffers a cyber-attack, and which consequences do businesses see as the most threatening? Two-thirds of industry (65%) report that disruption to operations, i.e. production stoppages, would be the most significant outcome of suffering a cyber attack. The second most cited consequence, and perhaps the most interesting as it is not directly related to the plant itself, is reputational damage. 43% of business respondents say that damage to reputation with customers or suppliers is a main concern of suffering an attack.

THE INDUSTRIAL INTERNET OF THINGS LEADS AS THE MOST SIGNIFICANT DRIVER OF GREATER ACTION IN BUSINESSES' CYBER SECURITY STRATEGIES

Chart 8: Operational disruption and reputational damage ranks as the most significant consequences of suffering a cyber-attack

% manufacturers reporting what they see as the primary fallout of suffering a cyber-attack (selecting two)

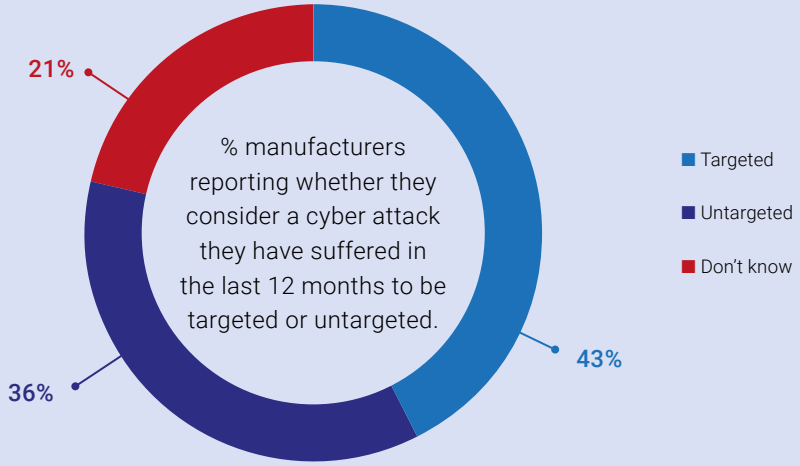


Source: Make UK Cyber Security Survey 2022

EASY TARGETS?

As part of the report's fieldwork, manufacturers were asked if they had been subject to an attack in the last 12 months, whether it was a targeted or untargeted attack. For clarity, we define a targeted attack as one where the aggressor has embarked to specifically attack the given target, for example, to access intellectual property unique to the victim company. By comparison, an example of an untargeted attack would be a compromised email attachment from a mass email that an employee brings into the firm's systems through error or ignorance.

Chart 9: Of those attacks able to be identified, targeted attacks are the most prevalent

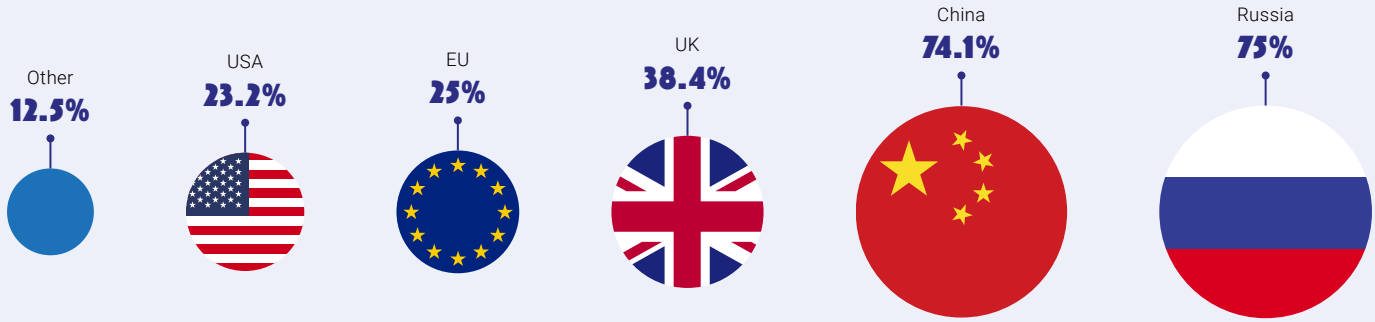


Source: Make UK Cyber Security Survey 2022

Most cyber attacks suffered by manufacturers in the past 12-months were specifically targeted at individual businesses, subsequently highlighting the importance of comprehensive cyber security strategies bespoke to individual firms' needs. This is particularly true in the case of companies with a headcount of 1000 or more, as companies within this category reported that 80% of any attacks endured in the last 12 months were targeted, which is 37% higher than the average across UK manufacturers of all sizes.

Chart 10: Manufacturers perceive the greatest cyber security threat originating from Russia and China compared to other regions by a factor of two

% manufacturers reporting which regions they perceive a cyber security threat from



Source: Make UK Cyber Security Survey 2022

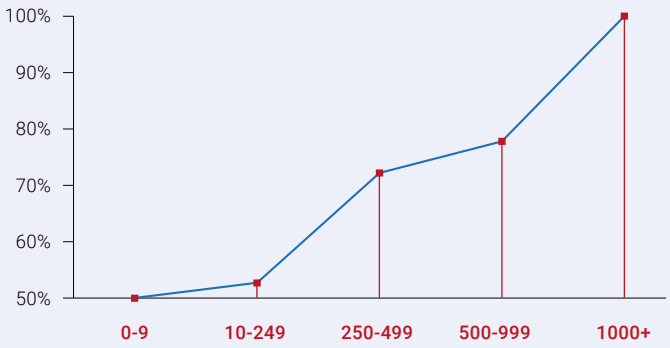
BUSINESS ACTION ON CYBER SECURITY

It's evident from our research that manufacturing businesses in the UK perceive cyber security as a critical element of organisational strategy, taking a range of measures to mitigate the threat. However, cyber strategies are rarely entirely impregnable, and identifying where shortfalls lie is important.

Particularly highlighted in this research is the human element of a business' cyber strategy. Manufacturers report that a majority, 62%, of the industry offers formal cyber security training to their employees. A very clear correlation between business size and the level of formal cyber security training for employees emerges when we cut the data by firm headcount bands. In the smallest band, 0-9 employees, only 50% of the industry report carrying out formal cyber security training for staff. There is a relatively consistent correlation for this relationship as we move up the company headcount size bands, right up to those companies with 1000+ employees, of which 100% of firms within this category report having formal cyber security training in place.

Chart 11: Strong correlation between company size and likelihood to deliver formal cyber security training

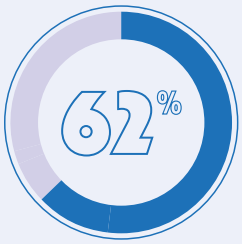
% manufacturers reporting whether they deliver mandatory cyber security training to employees, by company headcount



Source: Make UK Cyber Security Survey 2022

However, despite the majority of industry reporting that they have mandated formal cyber security training, manufacturers have already identified (cited earlier in this report) a lack of cybersecurity skills within the business as the second most prominent risk to their operational technology security. Clearly then, this highlights an insufficient level of formal training being offered to employees to suitably negate the threat of employee error in cyber security weakness.

In terms of procedure in the event of a cyber security incident, only 11% of the industry report not having a formal process to follow, with no plans to form one. By comparison, 62% do have a formal procedure. This leaves a final and significant group that report not having a formal procedure in place, but



OF MANUFACTURERS OFFER FORMAL CYBER SECURITY TRAINING TO EMPLOYEES

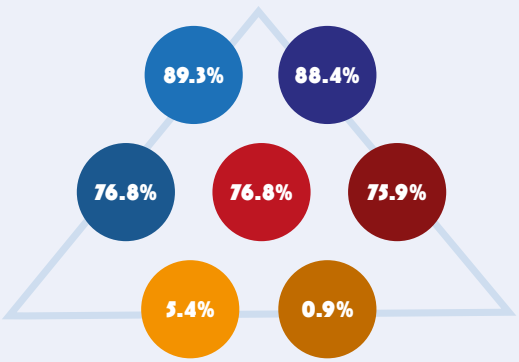
with intentions to form one, comprising 27% of the industry. This sizeable proportion of industry that intends to form a cybersecurity strategy reflects the growing importance of cybersecurity within modern manufacturing in the UK.

THE NUMBER OF MANUFACTURERS WHO HAVE A FORMAL CYBER SECURITY PROCEDURE IN THE EVENT OF AN INCIDENT HAS INCREASED BY 11% IN THE PAST YEAR

Testament to this is the increase in those reporting having a formal plan compared to Make UK's 2021 cyber security research in June, where only 51% reported having one. It shows there has been an 11% increase within only a year in the proportion of companies that have formal procedures in place to handle a cyber breach.

Chart 12: Widespread implementation of most common cyber security technologies

% manufacturers reporting what cyber technologies they have implemented within their businesses



- Antivirus software
- Firewalls to secure internet connection
- Secure settings for devices and software
- Network-wide system and software updates
- Controlled access to electronic data and systems
- Other
- We don't have any technical solutions to mitigate against the cyber security risk

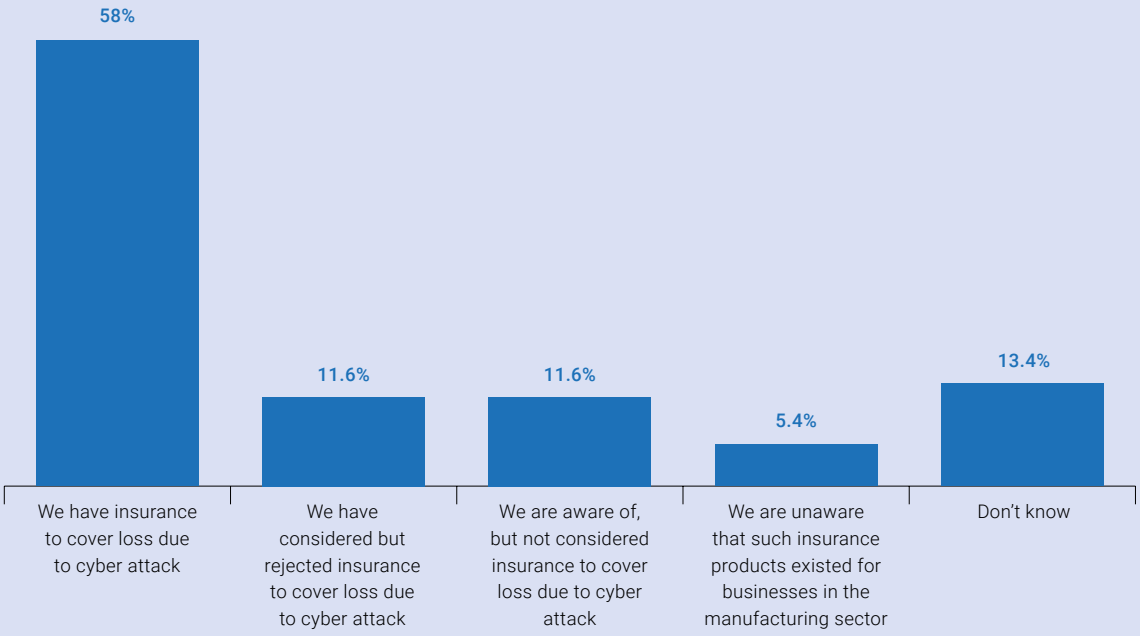
Source: Make UK Cyber Security Survey 2022

Uptake of frontline cyber security technologies is prevalent, as illustrated in Chart 12, with only <1% of respondents suggesting they do not have any technical solutions to mitigate cyber security risk within their business. While all options see significant uptake, there is a notable stratification between the two most common cyber security technologies: antivirus software and firewalls; and secure settings for devices, network-wide updates and controlled access to data.

The tightness of these two groupings suggests that there is a less secure group that only engages in the first two strategies of antivirus and firewalls, and does not go further. By taking the mean of the prevalence of these activities, we determine that approximately 12% of the industry implements this first line of defence, comprising of antivirus and firewalls, but has not, at least yet, gone further with implementing further, more robust cyber-secure technologies.

THE MAJORITY OF UK MANUFACTURERS ARE INSURED AGAINST CYBER ATTACKS

Chart 13: Manufacturers report whether they currently insure against the possibility of financial loss due to cyber-attack, including the legal implications of handling third-party data



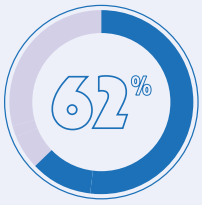
Source: Make UK Cyber Security Survey 2022

The majority of the manufacturing industry in the UK, 58%, are insured against any potential financial loss following a cyber attack. Awareness of cyber incident insurance is high, with only 5% of manufacturers reporting that they were unaware such insurance products existed for manufacturing firms. 12% have actively rejected insurance to cover cyber attacks and a further 12% have not yet considered cover despite being aware of its existence.

CYBER SECURITY IN THE CORPORATE STRUCTURE

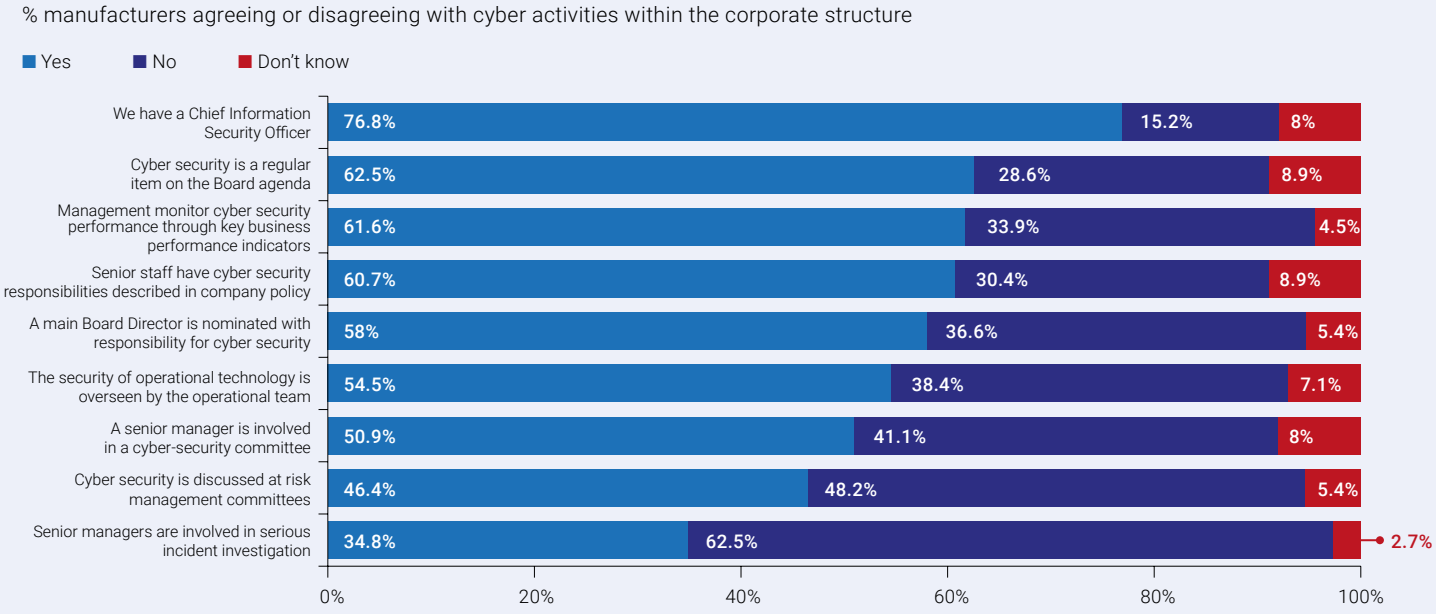
We have seen the specific actions manufacturers are taking concerning cyber security and the technologies being used. A further part of this research set out to understand how the remit of cyber security is placed within organisations' corporate structures.

77% of respondents say that a senior manager is involved in the investigation following a serious incident. While this indeed represents over three-quarters of the manufacturing base, the 15% that suggested that this is not the case can be seen to be insufficient with the diligence with which they address cyber incidents.



OF UK MANUFACTURERS REPORT HAVING A CYBER SECURITY COMMITTEE WITHIN THE BUSINESS

Chart 14: Manufacturers reveal who is responsible for cyber security in the businesses, and how it is managed



Source: Make UK Cyber Security Survey 2022

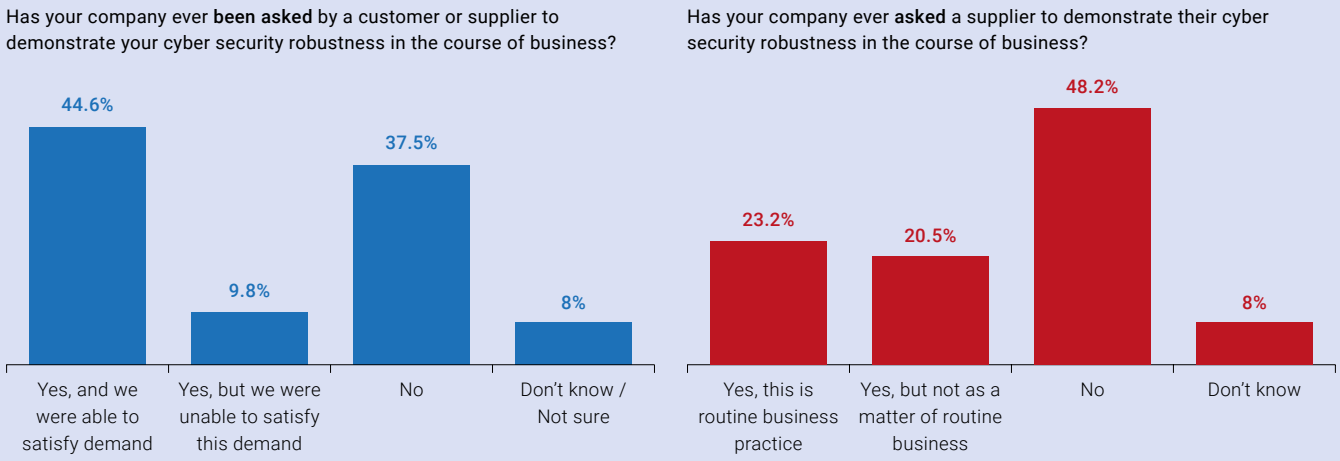
Encouragingly for the sector, 62% of the industry say that there is a senior manager involved in a cyber security committee, subsequently implying that this same proportion of the industry has such committees convene within their business. 58% say that a main board director is responsible for the cyber security of the business. The least prolific action, as part of this question, is seen in having a Chief Information Security officer, with just over a third, 35%, reporting to have one.

A question often arises as to which teams in the business are responsible for the security of operational technology. Our research shows that in 61% of businesses, the responsibility for the security of that technology lies with the operational team itself. However, there exists a correlation between business size and the likelihood of this being the case. For example, for those companies with 10-249 employees, this figure is 50%, but in those companies with 1000+ employees the figure rises right up to 89%.

DEMONSTRATING SECURITY AND BUILDING CONFIDENCE

Our research finds that it is more likely for a manufacturer to be asked to demonstrate sufficient levels of cyber security in their businesses than for manufacturers to make the same expectations of their suppliers. Together, this implies there is a bias in the supply chain, that as we move up toward the final original equipment manufacturer, or in other words, the 'final product' producer, a greater emphasis on supplier cyber security robustness exists.

Chart 15



Source: Make UK Cyber Security Survey 2022

Almost half (45%) of manufacturers report having been asked to demonstrate or guarantee the robustness of their cyber security processes as part of a contract or other business agreement, and successfully satisfying that request. 10% report having been asked, but failed to satisfy the challenge. However, only 23% of manufacturers report asking their suppliers to demonstrate the same cyber robustness as a routine part of business practice. 21% reported asking their suppliers as much as an extraordinary measure, with 48% indicating they had never challenged a supplier in such a way.

THE BARRIERS TO CYBER SECURITY

Manufacturers indicate that the most significant barrier to increasing their level of cyber protection is the cost of cyber security products. Just over 4 in 10 manufacturers say that the cost of cyber security is an issue. The second most cited barrier is cost related also, but in the broader sense of the time and cost incurred to the business by maintaining these security systems, with 35% of the industry suggesting so.

Compared to Make UK's work on cyber security in June of last year, a much smaller proportion of manufacturers suggest that there are no barriers to them becoming cyber secure. Last year, 62% of industry said there were no barriers to them increasing their cyber security, compared to now, where only 24% say the same. What this highlights, in tandem with our earlier findings on the increasing importance and scope of cyber security within manufacturing, is that manufacturers have been expanding their cyber security strategies over the past year, and in doing so, have discovered barriers that they had not recognised previously.

The third most cited barrier, a lack of training on cyber security for employees, also testifies to an earlier finding in the report that, despite generally widespread formal training offered to employees, it is insufficiently comprehensive to mitigate the employee-led cyber security risks in a business. 31% of manufacturers highlight this lack of cyber security training for employees as a barrier to their business' cyber security.

As the scope of necessary cyber security within businesses continues to increase in the coming months and years, continuing trends shown over the last 12 months by this report, manufacturers will need to balance the most cited barrier to cyber security – cost – with other business priorities. This is especially true as the industry endures, and will continue to endure, a cost of doing business challenge in the immediate future.

4 IN 10

MANUFACTURERS SAY THE COST OF CYBER SECURITY PRODUCTS IS A BARRIER TO THEM BECOMING MORE CYBER SECURE

Chart 16: Costs and training present as the most significant barriers to manufacturing businesses becoming cyber secure in 2022

% manufacturers selecting which barriers their business have come across in becoming cyber secure in the last 12 months.

#1 THE COST OF CYBER SECURITY PRODUCTS (41.1%)

#2 ADDED TIME OR COST IN MAINTAINING SECURITY SYSTEMS (34.8%)

#3 LACK OF TRAINING ON CYBER SECURITY FOR EMPLOYEES (31.3%)

#4 OTHER PRIORITIES WITHIN THE BUSINESS RIGHT NOW (29.5%)

#5 LACK OF AWARENESS ACROSS THE BUSINESS ON THE IMPORTANCE OF CYBER SECURITY (27.7%)

#6 NO BARRIERS (24.1%)

#7 ACCESS TO CYBER SECURITY PRODUCTS THAT MEET THE NEEDS OF MY BUSINESS (20.5%)

#8 OTHER (4.5%)

Source: Make UK Cyber Security Survey 2022

BlackBerry | Cybersecurity

VIEWPOINT

As industries move towards digitisation and automation, manufacturing sector organisations have little choice but to embrace new technologies, practices and connected IoT systems. The alternative is to risk losing competitiveness in a fast-paced world.

Data theft and malware are the dominant threats faced by the manufacturing industry. Cybercriminals are using a range of tactics – from old school phishing to more sophisticated malware – to gain entry for industrial espionage, data and patent theft. Particularly in today's tense global political environment, nation state actors want competitive advantage at any cost and will strike at the heart of key industries like manufacturing. In these times, a lack of focus on security comes at a price.

However, the overall complexity of an IoT system in a smart factory presents a challenge. It dramatically increases the number of potential points of exposure to a growing, and increasingly sophisticated, threat of cyberattack. From the Log4j attacks on Microsoft systems to scattergun phishing threats that rely on employees for access, there are no machines in the manufacturing environment that are off limits. This includes the systems that are operating as seemingly standalone, yet are often connected to a network or routed to the internet at some point.

This research has highlighted that the manufacturing industry is alert to the threat of cyberattacks. 95% of manufacturers report that cybersecurity is a necessary function of their operations, and 45% are keenly aware of the industry's core challenge – securing legacy and disparate technologies.

Sadly the adage "if it ain't broke, don't fix it" doesn't apply to cybersecurity. Legacy and disparate machines can quickly create vulnerabilities if not properly maintained with security software and regular updates against the ever-growing catalogue of threats. Though taking these machines offline for maintenance may be perceived as risky – and expensive – the greater threat is that of an attack that incurs unplanned production downtime, remediation costs and reputational impact.

In this environment, traditional firewalls and antivirus systems are not sufficient to effectively protect the complex IoT infrastructure. Despite our findings in this report showing that one in eight companies relying on this basic defence, in fact a successful deployment requires that each endpoint is properly secured to prevent opening the entire organisation to cybersecurity threat. AI-powered predictive protection such as BlackBerry CylancePROTECT can detect and prevent malicious attacks before they have chance to deploy in the network.

Without accurate visibility and protection across the entire operation, it could easily be that the 56% of industry that claim they have not been subject to a cyberattack in the last 12 months might instead by harbouring potential threat actors within their systems. It would not be uncommon for malware to reside, undetected in a legacy system or within the complexities of the main operating system, waiting for the right time to strike. This is a common tactic that manufacturing sector organisations would be advised to explore with a Compromise Assessment, which paves the way for assessing the appropriate cybersecurity protection and policies for the organisation to deploy.

Having the right expertise available is also a challenge. While the manufacturing sector's larger organisations may have cybersecurity professionals within their in-house team, for the majority the answer is more likely to be outsourcing. It's important to get a relationship established as a go-to resource in the event of a breach, to minimise panic and increase response speed when crisis hits.

Above all, OT cybersecurity should not be driven solely by fear. It should seen as a competitive advantage that leads to having secure, reliable and trustworthy products and services that enable greater business opportunity.

MAKE uk
The Manufacturers' Organisation

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:

James Brougham
Senior Economist
jbrougham@makeuk.org

Verity Davidge
Policy Director
vdavidge@makeuk.org

BlackBerry | Cybersecurity

BlackBerry is a leader in endpoint security, endpoint management, encryption, and embedded systems, protecting enterprises and governments around the world. Our end-to-end approach is deeply rooted in Cylance® AI and machine learning, providing continuous preventative protection, detection, and instant response. We extend protection for your organization against current and future cyberthreats by combining network and endpoint telemetry and by delivering innovative solutions in the areas of cybersecurity, safety, and data privacy.

www.blackberry.com/us/en/campaigns/2022/emea/operational-technology

For more information, please contact:

Joshua Oatts
Account Manager
BlackBerry
joatts@blackberry.com

Tony Howell
Account Manager
BlackBerry
thowell@blackberry.com

MAKE uk
The Manufacturers' Organisation

MAKE VENUES

UK STEEL

makeuk.org

22.11.POL.JB.NB