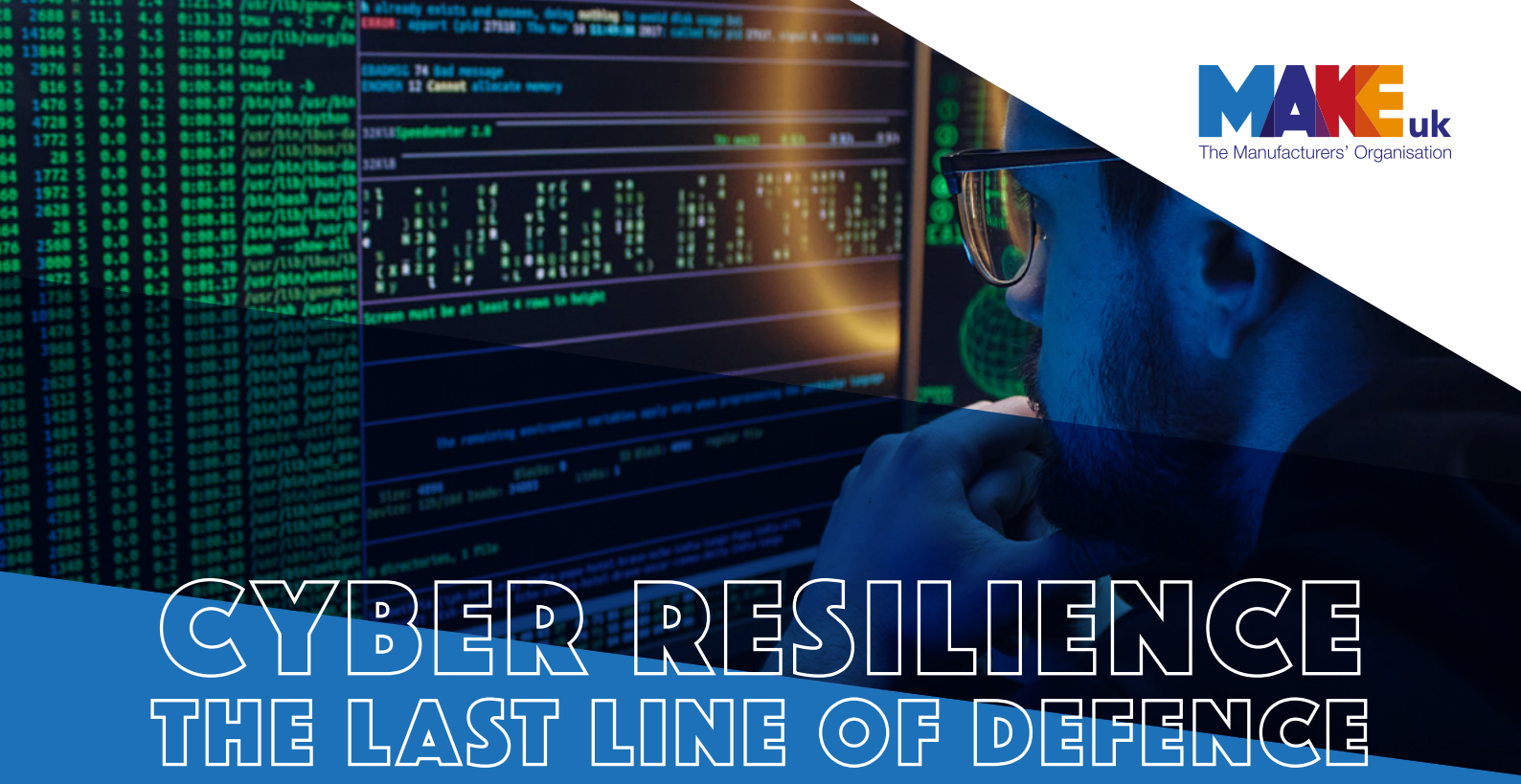


CYBER RESILIENCE
THE LAST LINE OF DEFENCE

EXECUTIVE SUMMARY

It is no secret that the manufacturing industry is undergoing a profound digital transformation. As manufacturers press ahead on their digital journey, they are reaping the benefits of becoming more productive, resilient, and sustainable. The Covid-19 pandemic undoubtedly pushed many businesses, including manufacturers, at speed towards remote ways of working. For office staff working at home is the new norm, accessing often sensitive files on hastily purchased laptops, while production staff have had to adjust to remote monitoring and production and virtual commissioning using mobile apps which can be vulnerable to unauthorised access.

Our latest figures show that just under half of manufacturers have been the victim of cyber-crime in the last 12 months. Of those companies that experienced an attack, 63% said it cost them up to £5,000 while almost a quarter (22%) revealed a cost to their business of between £5,000-25,000. But the good news is that British businesses are tackling cyber-crime like they have never before, with many now adopting effective tools and techniques to remain cyber secure and prevent and protect themselves from further strikes.

The acceleration of digital adoption, primarily by the pandemic, has propelled cyber risk to the forefront of Britain's boardrooms, with 61% of companies now having a board director responsible for cyber security. Make UK research from last year revealed manufacturers were accelerating the adoption of digital technologies with 14% now implementing digital processes (compared to just 4% in 2018) and just 11% still thinking about it (compared to 30% in 2018).[1] For the most part, companies have focused adoption on robotics, additive manufacturing along with the Internet of Things (IoT) and Artificial Intelligence (AI).

However, we know that barriers remain, with cyber security near the top of the list every time. Indeed, one in five (21%) manufacturers cited cyber as a barrier in 2020. It seems then that the needle has remained static for since our last survey in 2018 when cyber was cited as one of the key barriers to introducing digital technologies. Make UK's latest Cyber Security survey found that one in eight companies still agree that the risk of cyber-attacks are a primary deterrent from digital adoption[2].

1 IN 8 MANUFACTURERS AGREE CYBER-ATTACKS ARE DETERRING THEM FROM DIGITAL ADOPTION

But it is not just the adoption of industrial digital technologies that is bringing cyber-security back into the spotlight. As we move out of lockdown and into the 'new normal' it is increasingly clear that the new normal is one that brings with it more hybrid working and greater use of digital tools and technologies. Ensuring manufacturers are cyber-secure is a now not a nice-to-have but a necessity.

With financial cost, reputation and potential loss of data and intellectual property all at risk, this paper looks at the progress manufacturers have made to date, and where further progress could be made in order to be effectively cyber secure. Finally, it offers top tips from cyber experts for companies to ensure manufacturers remain cyber secure and puts forward considerations to Government on how it can support businesses particularly when it comes to accessing cyber-skills.

[1]Make UK, Innovation Monitor: Bouncing Back Smarter (2020)
[2]Make UK, Cyber Security Survey (2021)

THE IMPORTANCE OF CYBER SECURITY

The pandemic acted as a catalyst for business to look at their cyber resilience and resulted in plans being expedited in order for companies to remain operational. Overnight, companies were forced to switch to remote production, remote monitoring and office staff working from home on hastily supplied laptops.

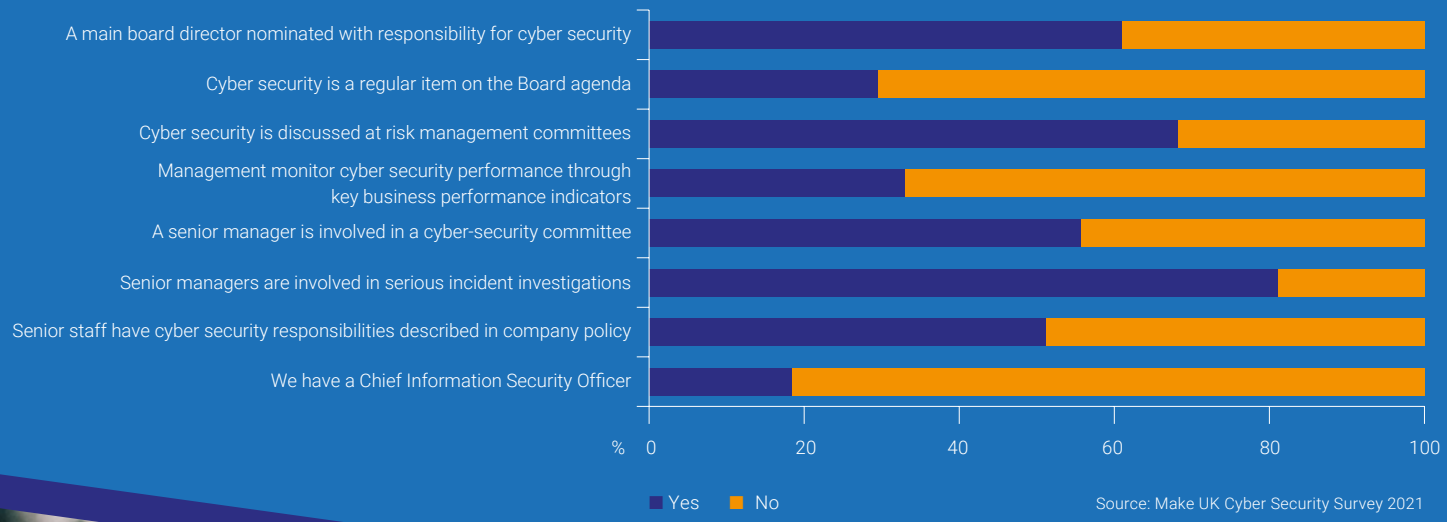
Cyber security was suddenly catapulted to the forefront of board agendas across the UK, with 50% of businesses saying cyber security has become a higher priority since the start of the pandemic. It is therefore reassuring that 61% of companies now have a main board director allocated the responsibility for cyber security, with boards across the country looking in detail at the measures in place to make sure that their businesses can operate safely. It is also encouraging that senior managers are involved in serious incident investigations resulting from cyber-incidents and that cyber-security is discussed at risk management committees at over two-thirds (68%) of manufacturing businesses.

Our survey also showed that every manufacturer questioned felt that cyber security measures are necessary for their company to operate smoothly. All companies see value in digitising to drive profitability, but the integration of more and more systems brings with it a huge increase in the risk of cyber-attacks.

It is reassuring that although cybercrimes are becoming more and more frequent companies are still ploughing ahead with digitising as the benefits of further digitisation outweigh the perceived risks. This is highlighted by 62% of companies that were surveyed stating that vulnerability to cyber-attacks real or perceived has not inhibited them from investing in technology. Digitalisation has been a key priority for the government as well as industry with the recent series of funding towards innovation and the long-awaited roll out of the Made Smarter programme to four regions. New digital technologies will use software and the majority of these then use big data that needs to be stored on the cloud. The need to be cyber-secure is vital. It is starting to become the norm that when companies begin planning for an increase or further integrating digital infrastructure that there is also a consideration around how this infrastructure will be secured.

Chart 1: Senior managers are increasingly involved in cyber-security

% companies citing involvement of senior managers in cyber security management



Source: Make UK Cyber Security Survey 2021

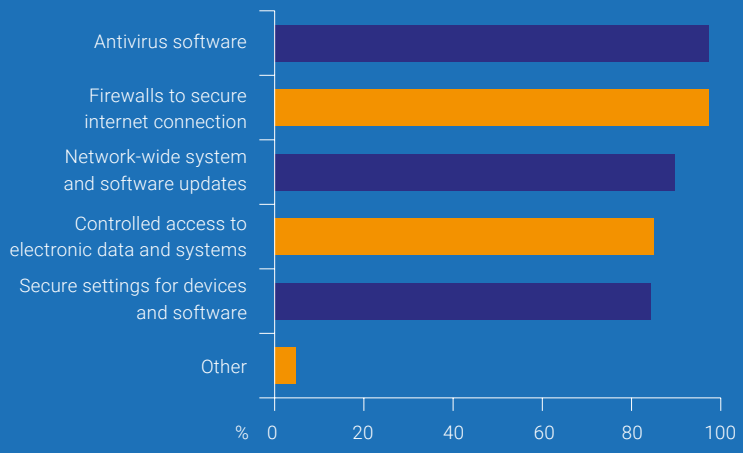
MANUFACTURERS SEE THEMSELVES AS CYBER-SECURE

Manufacturers view themselves as being relatively cyber-secure. Indeed, almost nine in ten (87%) are confident that their companies have the right tools, processes, and technologies in place to deal with a cyber security incident. Likewise, the overwhelming majority (91%) agree that their company has access to sufficient information and advice to assess the cyber security risk to their business.

Being equipped with the right tools and technologies is clearly at the top of manufacturers' agenda in order to remain cyber-secure and are adopting a range of these to prevent their businesses from a cyber-attack. Manufacturers are relying heavily on firewalls to secure internet connections (97%), antivirus software (97%) and network-wide system and software updates (90%).

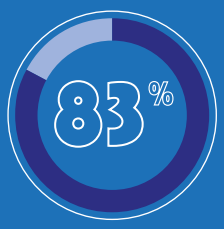
Chart 2: Manufacturers are using a range of tools and technologies to prevent or protect against a cyber security incident

% companies citing tools they are using



Source: Make UK Cyber Security Survey 2021

In a similar vein, manufacturers are broadly confident that they have the resource and expertise to assist with recovering from a cyber-security incident.

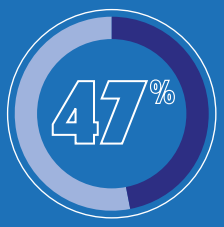


OF MANUFACTURERS SAY THEY HAVE THE RESOURCE AND EXPERTISE TO ASSIST IN RECOVERING FROM A CYBER-SECURITY INCIDENT

Manufacturers are seemingly confident in their ability to be cyber-secure having invested in various tools and techniques to both prevent and protect them from cyber-attacks. But the question remains, is this enough? Make UK research tells us that manufacturers are shifting towards more smarter manufacturing models. While this must be encouraged, businesses also need to be aware that increased digital connectivity can lead to increased vulnerability, particularly as connected products are often used to store and transmit sensitive data, sometimes outside of the business itself, opening opportunities for a cyber-attack, particularly around data theft. Moreover, cyber-attacks are themselves becoming more sophisticated, with businesses at risk of theft of data, Intellectual Property, and espionage. In the next part of this paper, we look at look at the extent to which the manufacturing industry has been subject to cyber-attacks and the cost and damage this does to a business.

CYBER ATTACKS REMAIN A REALITY FOR MANUFACTURERS

Cyber-crime remains a reality for many manufacturers with almost half of companies having experienced an attack in the past 12 months. Such incidents have come at a price. Some 63% of companies that have been subjected to an attack say the attack has cost them up to £5,000, while a further 26% have faced costs of between £5,000 and £50,000 associated with an attack. An additional 6% having to come to terms with a £100,000+ loss as a result of cybercrime. However, certain areas of manufacturing are particularly at risk - with automotive, chemicals and defence seeing a higher number of cyber incidents. While 47% of manufacturers have experienced a cyber-attack within the last 12months, 62% of UK automotive have been the victim of cybercrime over the same period.



OF MANUFACTURERS HAVE BEEN SUBJECT TO A CYBER-ATTACK OR CYBER-INCIDENT IN THE PAST 12 MONTHS

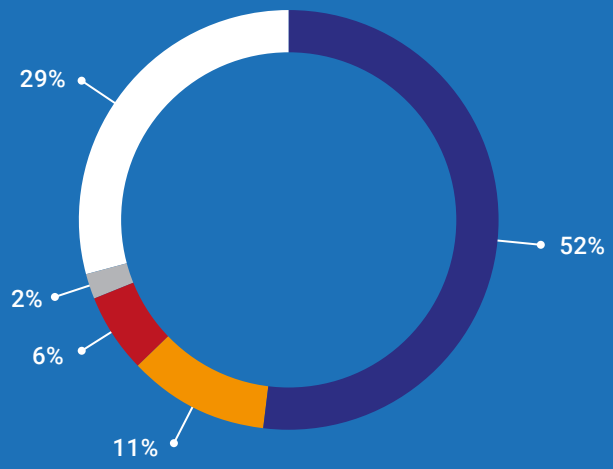
The attacks vary in seriousness and cost in monetary terms. Even the smallest of cyber invasions could potentially render a manufacturing company unable to operate for a time, lose critical IP or data and/or cause significant reputational damage. As the necessary drive to ever more digitisation continues, continuously evaluating the individual risks to manufacturing businesses is crucial.

1 THIRD
OF COMPANIES
WOULD NOT REPORT
A CYBER-ATTACK IF THEY HAD BEEN SUBJECTED TO ONE

To further mitigate against loss, our survey showed an increase in businesses looking at insurance providers to cover cyber-attacks, with 52% of businesses reporting they now have insurance to cover a loss due if they were to become victim to cybercrime. A further 10% told us they were considering investing in additional insurance to cover the loss associated with an attack as the importance of this sort of crime became every more business critical.

Chart 3: Manufacturers are insuring themselves against financial losses by cyber-attacks

% companies citing whether their business insures against the possibility of financial loss due to cyber-attack, including the legal implications of handling



- We have insurance to cover loss due to cyber attack
- We have considered but rejected insurance to cover loss due to cyber attack
- We are aware of, but not considered insurance to cover loss due to cyber attack
- We are unaware that such insurance products existed for businesses in the manufacturing sector
- Don't know

Source: Make UK Cyber Security Survey 2021

DEMAND FROM SUPPLIERS AND CUSTOMERS TO BE CYBER-SECURE

At the start of this paper we highlighted how the pandemic and move towards remote working, together with the accelerated pace of digital adoption is bringing cyber-security to the fore. But it is not just in-house demands companies need to consider, but also external considerations.

For example, two-fifths (43%) of manufacturers have been asked by a customer or supplier to demonstrate or guarantee the robustness of their cyber-security. One in five have themselves asked their customers or suppliers to demonstrate the robustness of their cyber-security. This may include requiring a business to hold a specific cyber security certification as well as demonstrating they have sufficient cyber protection.

Our survey also reveals that manufacturers have escalated cyber security up their list of business priorities. This has been demonstrated by the increasing number of companies with a nominated board director involved in cyber-security and the active role that senior managers play in cyber-security investigations. But the question remains – is this enough to demonstrate the level of robustness required?

The demands from customers and suppliers to demonstrate vigour in their cyber-security is only going to increase further in the near future, with a particular focus on the manufacturing supply chain. We know that manufacturers are taking some action, but this action can be deemed as limited in comparison to the potential threats and consequences of cyber-attacks. Manufacturers need to constantly review, measure and assess cyber risks not only in their business but also their supply chain.

PROTECTING YOUR BUSINESS WITH CYBER ESSENTIALS

"Cyber Essentials is a simple, low-cost government backed scheme that will allow manufacturers to demonstrate a robust approach to their cyber security. By implementing the five Cyber Essentials technical controls, an organisation protects itself against the most common internet-based threats. Going through the preparation and assessment process can ensure valuable information is protected from theft. Certification can also open new markets, help win new tenders and fulfil supply chain requirements from primes, many of whom are now mandating proof of cyber security."

Dr Emma Philpott MBE, CEO of The IASME Consortium

PROGRESS HAS BEEN MADE, BUT THERE IS STILL SOME WAY TO GO

Having highlighted the significant steps the sector has taken to become more cyber secure, there is however much work still to be done. As manufacturers continue to transition from analogue to digital and more and more systems and devices become interconnected, cyber-attacks too will evolve, becoming ever more sophisticated and harder to spot and or stop. To best mitigate against this growing risk, it is vital that all employees from CEO to machine operators on the factory floor have a good understanding of the risks to their business, and how to best protect against them.

With 44% of manufacturers still not offering cyber security training to their staff, many employees will still not have the necessary expertise to know the dangers to look for. To prevent an attack, it is important for employees to have the skills and tools recognise an attack is taking place in the first place and to know the emergency steps to take to prevent the company system being taken over completely.

CYBER SKILLS

Cyber skills are an important element in the wider landscape of becoming cyber secure. From one day training courses all the way through to degree level skills. It is important to have employees not only with digital skills but with cyber security skills in order to recognise and mitigate against cyber risks. Ensuring your employees are at least aware of the increased threat that comes with further digitising is key in avoiding cyber criminals gaining access to valuable IP/data. NCSC currently offer a great programme looking to entice the next generation called CyberFirst. CyberFirst look to develop the UK's next generation of cyber professionals through student bursaries, free courses for 11–17-year-olds and exciting competitions.

Our research revealed that 47% of companies do not even have a formal plan or process agreed in case of an attack. It is vital businesses and employees know how to respond to the attack immediately, through reporting mechanisms, identifying the origin of the incursion, and then taking quick responsive action. The research further uncovered another area where further work is needed. Understanding that cyber threats will never become less of a problem and that they will only become more and more sophisticated is a reality companies have to come to grips with and to ensure cyber security remains a priority. However, 66% of manufacturers report that cyber security does not have a regular slot on their board's monthly agenda.

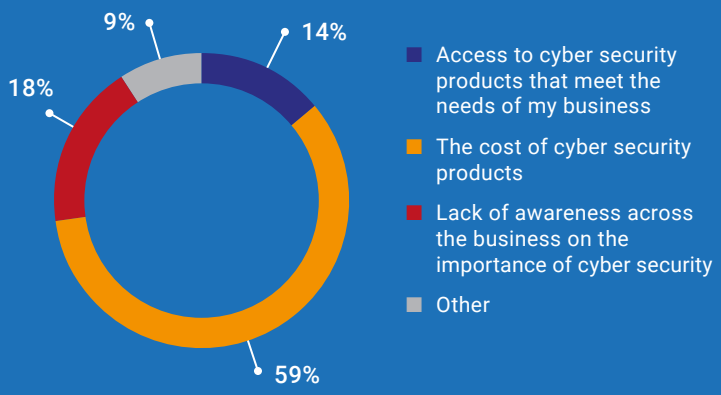
Along with tools and systems that will offer manufacturers protection, fostering a 'no blame' culture plays an equally important role. Employees should be empowered to report potential risks such as phishing emails, even if employees do click on emails they later find out are suspicious it's important to encourage reporting the potential risk at the earliest stage in order to prevent access being gained.

Whilst many manufacturers clearly see that putting in place adequate cyber security as a necessity, it is also worth considering the reasons some remain without sufficient – or indeed any – protection. A total of 59% of respondents cited cost as being the biggest barrier to becoming more cyber secure. However increasingly manufacturers are coming to understand the value add of a sophisticated cyber security system and the potential return on investment.

Moreover, companies do not need to spend a fortune to protect themselves.

Chart 4: The cost of cyber products is the main barrier for businesses to being cyber-secure

% companies citing the main barrier to being cyber secure



Source: Make UK Cyber Security Survey 2021

CONCLUSION

As manufacturers continue to digitise and with a growing number of the workforce working remotely, the importance to recognise the risk of a cyber-attack only grows greater. This should in no way prevent companies becoming more digital, but it is crucial to be aware and to put cyber security threats and prevention at the centre of any digital infrastructure plans. Cyber-attacks will inevitably evolve and so should cyber defences to protect valuable IP, data, and reputation.

While the term "smart" manufacturing is used constantly, "smart and secure" must become the new moniker as cyber risk can no longer be ignored.[3]

The barriers to being cyber secure need to be addressed if manufacturers are to continue to make progress in this area. The two main blocks cited were cost and understanding the importance of cyber security. As demonstrated, manufacturers can improve their cyber security by using the below ten tips which are not costly but will offer some additional layers of protection. Not all manufacturers need a sophisticated and costly cyber security system as each company will have individual security needs. Cyber security is not a one size fits all system. Therefore, Make UK urges manufacturers to adopt the top ten tips from the National Cyber Security to become cyber-secure in this increasingly digitised world.

NATIONAL CYBER SECURITY CENTRE, TOP 10 TIPS:

1) Set up your Risk Management Regime
Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

2) Network Security
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

3) User education and awareness
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

4) Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

5) Removable media controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

6) Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

[3]Global cybersecurity risks in the manufacturing industry - Willis Towers Watson

7) Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

8) Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

9) Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

10) Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

Among the many themes of our policy paper one that will strike a chord with many manufacturers is the need to ensure that their employees are sufficiently trained in an event of a cyber incident. This is particularly important for SMEs who are less likely to have a Chief Information Officer or similar role in their business.

To support manufacturers Government should take forward Make UK's calls for a lifelong digital skills account which would allow employees to access funds to undertake digital skills training, which in this case could include cyber-skills. Moreover, Government should consider how it could use its recently announced Help to Grow scheme to include cyber-skills within the digital skills element.

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.

For more information please contact:

Aaron Maran
Policy Manager
amaran@makeuk.org

Verity Davidge
Director of Policy
vdavidge@makeuk.org

MakeUK.org

MAKE BUSINESS MAKE VENUES UK STEEL NDI