In partnership with:

VAUBAN GROUP

MAKE uk
The Manufacturers' Organisation

CYBER SECURITY AND MANUFACTURING

A BRIEFING FOR MANUFACTURERS BY MAKE UK

MakeUK.org

FOREWORD

A comprehensive approach to cyber security is not something that manufacturers can afford to ignore. Last year, for the first time, Make UK assessed the cyber security resilience of our sector across the UK. Our findings revealed a community increasingly alive to this risk, but with a hugely varying degree of preparedness in response. Since then the threat has continued to grow, but the response from manufacturers remains inconsistent.

In the intervening time Make UK has not only renewed our findings, but we have designed and launched a suite of services specifically designed for manufacturers to assess their cyber security risk and do something about it.

This is critical to our business. The 4th Industrial Revolution represents unprecedented opportunity through digitisation. But that very openness brings with it increased risk. The threat from cyber-attack is a major barrier to business and growth; threatening loss of data, theft of capital and intellectual property, disruption to business, and impact on trading reputation.

As the UK's voice of manufacturing, Make UK is playing its role in supporting our members in the face of this challenge. In partnership with Vauban Group, our new services are designed to help businesses quantify their cyber security risk and take affirmative action to mitigate against it. They will also help members demonstrate their cyber security safeguards to customers and suppliers, an ever more necessary requirement for businesses to operate in our sector.

Cyber security is not a threat that manufacturers can avoid by remaining analogue. In the digital age that is a certain road to uncompetitiveness. But it is a risk that, addressed from a position of knowledge, can be properly managed so that the benefits of digital connectivity can be felt in every factory up and down the country.

Stephen Phipson CBE
CEO
Make UK

EXECUTIVE SUMMARY

Manufacturing is a significant target for cyber-criminals. This can result in the theft of sensitive data, industrial espionage for competitive advantage, or the disruption of access to systems or operational technology. 60% of our members tell us they have at some time been subject to a cyber security incident, almost a third of whom suffered some financial loss or disruption to business as a result. There seems little doubt that many more attacks will have gone undetected.

As a result, the need to have demonstrable cyber security safeguards in place is becoming ever more necessary to operate in the business environment. 41% of manufacturers report that they have already been asked by a customer to demonstrate or guarantee the robustness of their cyber security processes, and 37% have asked the same of a business within their supply chain. For the 31% of manufacturers who report that they could not do this if asked to today, business will become increasingly challenging.

Cyber-related risks for manufacturers are only likely to deepen and broaden with increasing digitisation. While manufacturers are investing in digital technologies in readiness for the 4th Industrial Revolution, 35% consider that cyber-vulnerability is inhibiting them from doing so fully. This suggests that opportunities are being missed and some businesses risk falling behind in the race to digitise. The result must not be that the UK falls away from the vanguard of manufacturing excellence.

Nevertheless, sensible precautions and a proper cyber security business plan are in reach of all. Make UK's new cyber security services, launched in partnership with Vauban Group, are designed to provide our members with the confidence businesses need to invest in digitisation, and the credibility to operate in the sector as a trusted supplier.

1: CYBER SECURITY NOW - WHAT ARE MANUFACTURERS' TELLING US?

Cyber security incidents are seldom far from the news. According to Department for Digital, Culture, Media and Sport's Cyber Security Breaches Survey 2019, 32% of UK businesses had reported that they had experienced a cyber security breach in the last 12 months. Alarmingly, this probably represents only the tip of the iceberg; many cyber-attacks go unreported as individuals and businesses either fail to identify them or do not report them in order to avoid reputational damage.

Manufacturing is by no means immune to this trend. IBM's 2019 Global Threat Intelligence Index highlights that manufacturers are the target of 10% of all attacks and incidents in the business sector around the world.

Perhaps more alarmingly, while manufacturing was identified as only the fifth most targeted sector in 2019 - behind finance and insurance (19%), transportation services (13%), professional services (12%), retail (11%) – manufacturers were the third-most likely to experience a data breach. As this briefing will show, this reflects a sector in which the level of preparedness varies widely across businesses and many manufacturers are leaving themselves vulnerable to attack.

Compounded by the fact that incident reporting in our sector is comparatively low, due in part to the fact that a comparatively greater proportion of attacks in our sector do not involve compromised 3rd party information, we must conclude that the risk to Make UK members is even higher than the conclusions of IBM's report suggest.

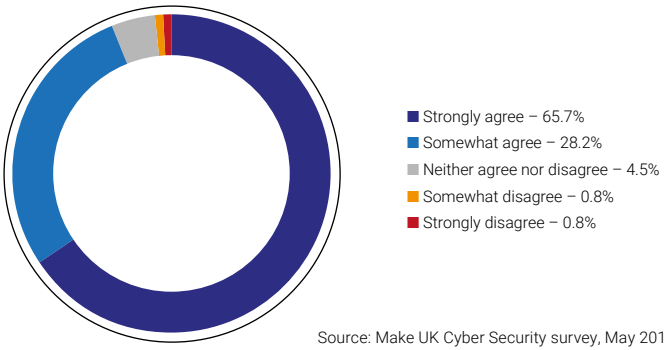
All manufacturers must therefore understand that a cyber-attack on their organisation is not a question of if, but when, by whom and to what degree.

Make UK surveys its members

In May 2019 Make UK conducted a survey of its members to determine the current cyber security landscape in the British manufacturing sector.

Encouragingly, 94% of our members told us that cyber security is necessary for their company. Clearly, the messages from government, trade associations and academia are being heard and awareness of the need for cyber resilience in our sector is growing.

Cyber security is necessary for my company

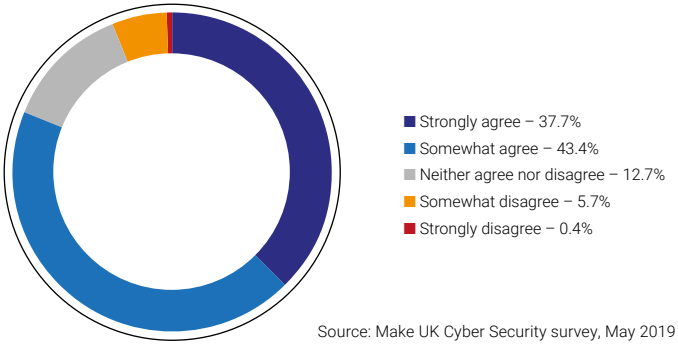


Source: Make UK Cyber Security survey, May 2019

The good news is that confidence also appears to be growing in our sector that the information and advice is out there for manufacturers to confidently assess their cyber security risk. More than 80% of our respondents agreed that this was true in

whole or part, significantly higher than the 55% who reported the same when we asked the question in 2018.

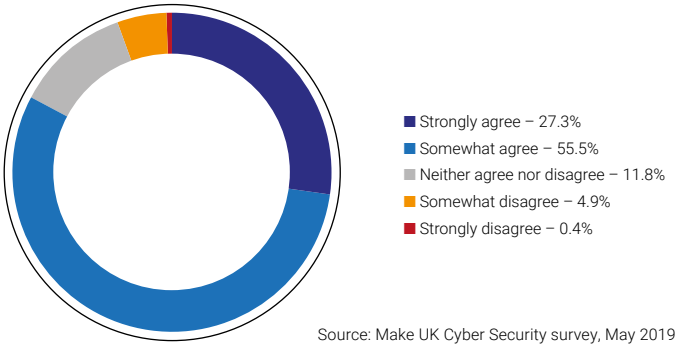
My company has access to sufficient information and advice to confidently assess the specific cyber security risk to us



Source: Make UK Cyber Security survey, May 2019

So what has changed? It appears that more manufacturers are now heeding the warnings and taking action to doing something to protect their cyber infrastructure. More than 80% of our respondents told us that – at least to some extent - that they are already employing tools and technologies to detect, protect against and recover from a cyber security incident.

I am confident that my company is prepared with the right tools, processes and technologies to deal with a cyber security incident



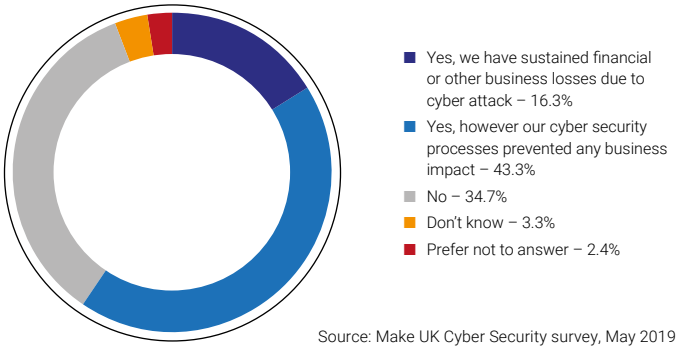
Source: Make UK Cyber Security survey, May 2019

However, this tells us only one side of the story. Whilst manufacturers' awareness of both the threat and the means to respond to it is growing, so too are the actual number of incidences. 60% of our members reported to us that they have themselves been subject to cyber-attack, of these;

27% told us that they had suffered financial or business losses as a result;

65% reported attacks having taken place in the last year.

Has your company ever been subject to a cyber-attack or other cyber security incident (including incidences where employee error has been an influencing factor)?



Source: Make UK Cyber Security survey, May 2019

The nature of the threat

The majority of cyber-attacks continue to be conducted either for direct financial gain or aim to disrupt or damage a target, normally as part of a blackmail campaign. For example, in a 'ransomware' attack, data is encrypted and is only made available again on payment of a ransom; ransomware is more the more prevalent method of cyber-attack and has a greater impact on the business. Similarly denial-of-service attacks, which impact on a customer's and/or supplier's ability to access a business, might be designed to undermine the credibility of that business.

Attack brings Norwegian aluminium producer to standstill

In March 2019 it was reported that one of the world's biggest aluminium producers had been forced to switch to manual operation following a 'severe' ransomware attack.

Norwegian company Hydro was forced to halt production at some facilities, with employees warned not to log in to their computers as connections infected by the virus has to be isolated from the main system.

At some factories, staff were forced to use printed order lists as they were unable to retrieve order data from their computers.

It is believed the attack used a ransomware virus known as LockerGoga that encrypts files on the victim's computers and demands money in order to decrypt them.

The financial effect on the company was estimated to be as much as NOK 350 million (£32m GBP), according to preliminary evaluations.

Encouragingly, most manufacturers tell us that they are employing one or more forms of tool or technology to prevent or protect themselves against cyber-attack;

88% have antivirus software

75% control access to electronic data and systems

85% use a firewall to secure their internet connection

75% update their network-wide systems and software

78% use secure settings for devices and software

Source: Make UK Cyber Security survey, May 2019

The comprehensive deployment of such measures will certainly help prevent businesses from falling victim to the most common forms of attack. These are still launched indiscriminately and in an industrial manner, to seek out victims whose vulnerabilities are dangerously exposed through a lack of even the most basic of protections.

Nevertheless, cyber security risk management is not solely about technology, but also relates to people and processes. The reality is that most successful hacks succeed because, at some point in the chain, human error results in a breach of defences. Ultimately, while technical solutions are a fundamental part of a business's protection, they are of limited value if not underpinned by a comprehensive business strategy.

While 84% of members reported that they have some form of strategy in place to assess and mitigate their cyber security threat (including that provided by an external service provider), that leaves 16% who have no processes in place at all. These businesses, which evidence suggests are mostly Small and Medium-Sized Enterprises (SMEs), represent the most vulnerable to a successful breach.

Digging deeper into the nature of these defences exposes vulnerabilities that run more prevalently across the sector. This means that many companies who might be confident in their cyber security posture are leaving themselves exposed due to the lack of a comprehensive strategy.

27% of manufacturers told us they do not have a risk register or mitigation plan limit the threat

33% do not provide awareness briefs or formal training to their employees

41% do not have a nominated lead for cyber security at board level

49% do not monitor cyber security performance through key business performance indicators

55% do not have insurance to cover loss due to cyber-attack

Source: Make UK Cyber Security survey, May 2019

In a large part, the lack of a comprehensive business strategy reflects a lack of understanding as to the nature of the threat.

Many manufacturers have indicated to us a lack of awareness and understanding at board level of the extent of the cyber security challenge to the business. This can make it difficult for those with this delegated responsibility to secure an appropriate operational focus and funding from senior leadership for cyber security risk management programmes.

Perhaps too often, part of this struggle to raise awareness reflects a perceived view that it is a complex and deeply technical subject, deterring some senior leaders from engaging with the risk of cyber-crime and other cyber security threats.

This perception permeates into many businesses, creating a barrier preventing the roll out of comprehensive cyber security awareness training to employees and most mitigation strategies. Such measures are an increasingly vital line of defence, engendering better security culture and behaviours through adherence to accepted and understood cyber security policies and procedures.

Securing the supply chain

While the majority of successful attacks in our sector may be indiscriminate, there is now a growing cyber security threat that is specifically targeting our sector. Not only is manufacturing considered by some criminals as an attractive target, as it is not regulated as comprehensively as other sectors, there are a growing number of attacks which are concerned with the theft of intellectual property and trade secrets. Particularly in the case of manufacturing, data might be stolen to gain competitive advantage, disrupt business operations, or to be sold on to competitors. There is a growing trend for criminals to target a company using weaknesses within their partner company or companies.

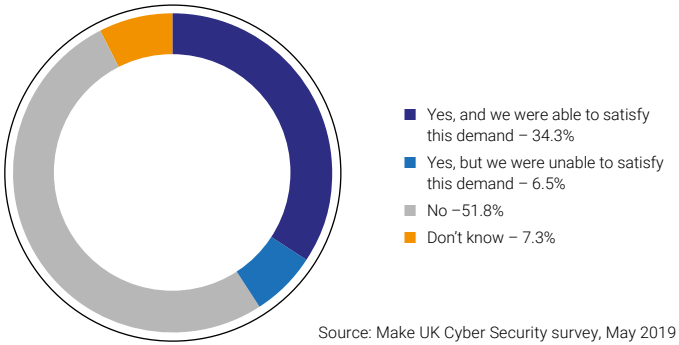
The result is that being able to demonstrate that certain cyber security measures are in place is going to become ever more necessary to operate in the sector, as businesses demand from their supply chain the ability to demonstrate or guarantee the robustness of their cyber security processes as part of the contracting process.

Company at risk, due to C Suite Management not prepared to invest

The head of IT at a north eastern manufacturer, volunteered to take our Cyber Security Assessment. He was very concerned that it identified significant vulnerabilities in the company and brought to light the lack of a co-ordinated risk management approach. In fact, many of the vulnerabilities lay outside IT's area of responsibility; he is unable to attract the attention of his Board as they are reluctant to invest in this area. The company remains at risk whilst it doesn't take action to protect its assets.

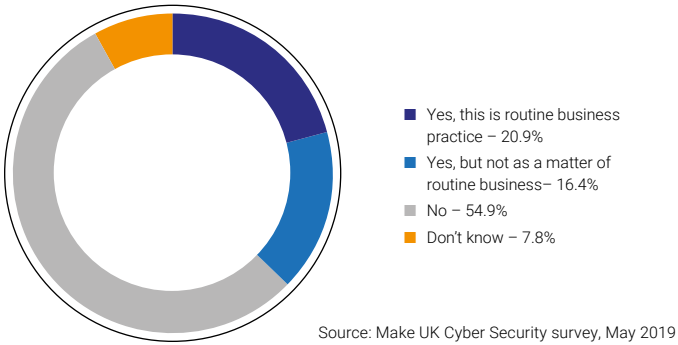
Some 41% of manufacturers reported to us that they have already been asked by a customer to demonstrate or guarantee the robustness of their cyber security processes, and 37% have asked the same of a business within their own supply chain. It is therefore increasingly important for the 31% of manufacturers who report that they did not have full confidence, as of today, that they could demonstrate cyber security resilience to a customer to provide assurance that adequate risk management processes are in place.

Has your company ever been asked by a customer to demonstrate or guarantee the robustness of your cyber security processes as part of a contract or other business agreement?



Source: Make UK Cyber Security survey, May 2019

Has your business ever asked a supplier to demonstrate or guarantee the robustness of their cyber security processes as part of a contract or other business agreement?



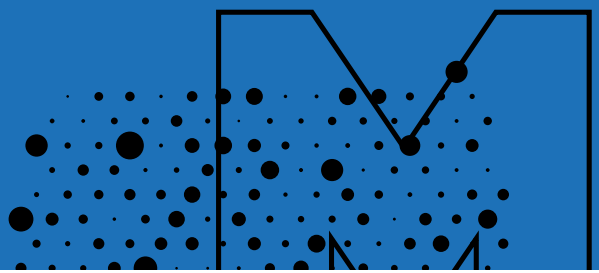
Source: Make UK Cyber Security survey, May 2019

MAKE UK PILOT

During the first half of 2019, Make UK and Vauban piloted our new Cyber Security Assessment tool. Designed by our new cyber security partner Vauban Group, the tool allows members to assess their cyber security maturity, it balances the need to be technically effective and enable members to *make decisions on how to protect their assets*. Launching in September 2019, further details can be found in the final chapter of this briefing.

108 Make UK members were offered the opportunity to trial the Assessment Tool; the following trends were identified among those members who participated:

- None had formalised Risk Management policies and processes with engagement of senior management
- More than two thirds had no formal Incident Management plan in place
- None had a regular testing regime in place
- Nearly all the companies used their IT staff to lead the Assessment and had little co-ordination from other areas of the business
- Some companies had issues with their Outsourced IT providers, whom they had to engage to complete the assessment
- Many companies recognised that they had little assurance of their supply chain
- Less than 10% of all those spoken to said they had achieved or were working towards Cyber Essentials of a similar accreditation scheme.



2: CYBER SECURITY FRAMEWORKS FOR MANUFACTURERS

Government has good reason to be concerned with the breadth and depth of cyber security best practice in the private sector and the establishment of the National Cyber Security Centre (NCSC) in 2016 is testimony to this. While the threat to an individual business or organisation might, in most circumstances, be of limited consequence on a national scale, sustained systematic or indiscriminate attack on business could potentially have damaging consequences for the health of the UK economy. In this sense cyber security is rightly considered a matter of national security.

One way in which Government might in future choose to induce good cyber security practice across the private sector is through the introduction of regulation. Indeed, the comparative private sector uptake of regulatory regimes vis-à-vis voluntary frameworks is compelling. While businesses signing up to schemes such as Cyber Essentials remain a small minority of the total number of businesses operating in the UK, the adoption of the EU General Data Protection Regulation (GDPR) in 2018 led to a comprehensive and sustained uptake of measures by business to secure personal data. That such regulation comes with a set of relatively punitive punishments for failures to comply can arguably be identified as the central motivation.

Of course, such an approach would be likely met with scepticism from industry, potentially with good reason. The blunt nature of regulatory regimes would be unlikely to incorporate the level of nuance required by most companies when building their specific cyber security posture. On these grounds Make UK does not advocate that Government takes this course of action, though we recognise that more needs to be done by businesses, including our members, to demonstrate sufficient business-wide uptake of good cyber security practice in order for this position to be sustainable.

Part of the challenge for many manufacturers, and small businesses in particular, is to navigate the marketplace. For businesses new to the topic, it can be difficult to identify what is essential, what is useful and what is completely unnecessary. This is not to discredit the wide variety of consumer solutions in the market place, but rather a reflection that cyber security is not a risk that can be mitigated by a standardised solution. However, for a business to understand its individual need it must first be able to assess its particular circumstances.

Basic cyber security risk management principles

The NCSC has released guidance on basic cyber security risk management principles intended as an introductory guide for small businesses, though the principles can be applied to all organisations, regardless of their size. Featuring five easy steps the aim is to significantly reduce the chances of a business becoming a victim of the most common types of cybercrime, usually intended for vulnerable targets.

Step 1 - Backing up your data
Regular and routine backing up of important data ensures that it can be restored in the event of system corruption.

Step 2 - Protecting your organisation from malware
Malicious software (also known as 'malware') can harm an organisation by infecting legitimate software, stealing data and corrupting systems.

Step 3 - Keeping your smartphones (and tablets) safe
Mobile technology means that more of our data is being stored away from the security of the office, with a commensurate increase in risk to the data contained within.

Step 4 - Using passwords to protect your data
Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised users accessing your devices.

Step 5 - Avoiding phishing attacks
Phishing emails rely on human fallibility and are getting harder to spot, and some will still get past even the most observant users.

Cyber Essentials

Beyond these basic steps, frameworks of cyber security standards are becoming increasingly prevalent. The government's Cyber Essentials scheme goes a step beyond the basic advice available from the NCSC and acts as a valuable starting point for businesses beginning their cyber security journey.

Cyber Essentials is a self-certified scheme that works on the principle that the vast majority of cyber-attacks are untargeted and unsophisticated, designed to prey upon systems without even the most rudimentary protection measures.

Cyber Essentials states that the first step for any organisation in cyber risk management is to compile a baseline of security controls. Featuring five easy steps the aim is to significantly reduce the chances of a business becoming a victim of the most common types of cybercrime, usually intended for vulnerable targets.

There are five technical controls in Cyber Essentials:

1. Use a firewall to secure your Internet connection
2. Choose the most secure settings for your devices and software
3. Control who has access to your data and services
4. Protect yourself from viruses and other malware by using antivirus software, only downloading apps manufacturer-approved stores, or running apps and programs in an isolated environment
5. Keep your devices and software up to date by patching regularly.

Cyber Essentials 'Plus' demands the same level of protection in order to be certified, but this time the verification is carried out independently by a certification body, providing additional reassurance to the successfully verified company.

Cyber Essentials Plus verification has the additional benefit of providing evidence that a minimum level of system protection has been achieved. This is increasingly important in the manufacturing supply chain.

Manufacturers active in the defence market will already be aware that, since January 2016, the Ministry of Defence (MOD) has mandated that, for all new contracts requiring the transfer or generation of MOD identifiable information, suppliers are mandated to hold a Cyber Essentials certificate, and for it to be renewed annually. This requirement must be flowed down the supply chain.

Due to the nature of their activities, it is little surprise that the MOD is leading in mandating cyber security standards on their suppliers. However, it is increasingly likely that other bodies in both public and private sector will follow suit. As a result, manufacturers will find this an increasingly necessary aspect of business readiness in order to trade.

ISO 27001

For businesses with a requirement to protect themselves against more sophisticated cyber-attacks, for instance those with sophisticated digital production facilities or those working with sensitive technologies, the next framework to consider aligning to beyond Cyber Essentials is ISO:27001

ISO 27001 (formally known as ISO/IEC 27001:2005 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system. The implementation of such a framework provides the business with policies and procedures that includes all legal, physical and technical controls involved in the management of information risk.

ISO: 27001 uses a top-down, risk-based approach and is technology-neutral. The specification defines a six-part planning process.

ISO: 27001 planning process

1. Define a security policy.
2. Define the scope of the ISMS.
3. Conduct a risk assessment.
4. Manage identified risks.
5. Select control objectives and controls to be implemented.
6. Prepare a statement of applicability.

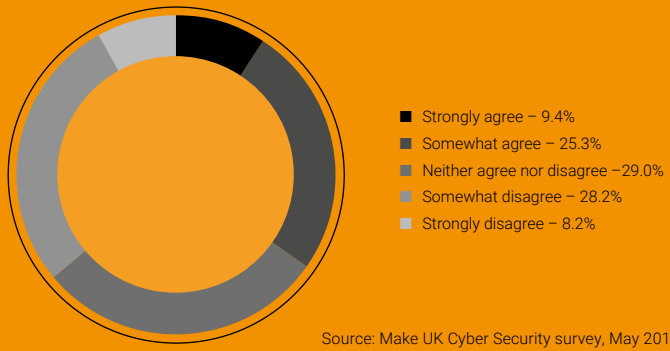
The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organisation.

3: CYBER SECURITY FOR MANUFACTURING'S DIGITAL AGE

If it is clear that there are vulnerabilities in the sector as it currently operates, then advances in artificial intelligence, the human-machine interface and the increasing connectivity of information and operational technologies will only increase the complexity of the challenge.

Make UK has long championed the rewards for UK manufacturing of being at the forefront of the 4th Industrial Revolution, a call that is being heeded by UK businesses. And yet, while the vast majority of manufacturers tell us they are investing in digital technologies, 35% of our members feel that vulnerability to cyber-attack, whether real or perceived, is inhibiting them from doing so fully.

Vulnerability to cyber-attack (real or perceived) inhibits my company from investing in technological advances through interconnectivity



Source: Make UK Cyber Security survey, May 2019

Of course, in a global market, UK manufacturers are most successful when they offer innovative solutions and cutting-edge technology, supplying products that are world-leading in their field. However, to view connectivity as a challenge that only the technology industry needs to keep pace with is to underestimate just how fundamental the revolution that stands before us will be.

Innovations such as artificial intelligence, robotics, automation, and big-data exploitation are more than simply means to deliver increasingly sophisticated products, as important as that is. These technologies are set to become the principal means for driving productivity and efficiency into the manufacturing process itself. Thus, the effect on businesses whatever they manufacture and wherever they sit in the supply chain will be both inevitable and profound. Ignorance is not an option.

Autonomous machines promise a near-future where little in the manufacturing process is touched by human hands. Products of every type will control their own fabrication processes, telling production machines what requirements they have and which production steps must be taken in what order and when.

For mass produced items and consumables such advances will guarantee near 100% production quality as well as increased production rates and lower manufacturing costs. Conversely, for low-volume and specialist production, automation combined with big-data will bring forth increasingly complex products that are delivered quicker and more economically as production systems optimise manufacturing processes in real time. In both scenarios the productivity dividend will be obvious.

Yet, for traditional businesses investing in the digitisation of their production systems, cyber security is a new and often poorly understood risk dynamic. In a factory where the production systems themselves have end-to-end connectivity, cyber security suddenly means much more than just securing your emails and the online activity of your staff.

Connectivity means that, whatever edge a manufacturer has that makes them successful, be that a more advanced product or a more efficient production process, all of it will be written into the data held in their network and, potentially, the network of their customers and suppliers. In some cases the very future of a business might be threatened if that data were to be compromised.

It is thus perhaps no surprise that cyber security vulnerabilities, or at least the perception of that risk, remains an inhibitor to full investment in digitisation. However, cyber security is not a threat that manufacturers can avoid by remaining analogue. In the digital age that is a certain road to loosing competitive advantage. That is bad news for industry and bad news for the economy; businesses that fall behind their competitors will not be afforded the opportunity to catch up.

But it is a risk that, addressed from a position of knowledge, can be properly managed so that the benefits of digital connectivity can be felt in every factory up and down the country.

4: HOW MAKE UK CAN HELP SECURE YOUR BUSINESS

Make UK Cyber Services
As this briefing note has outlined, a comprehensive approach to cyber security is of paramount importance to the continued success of manufacturers.

Make UK's new cyber security services are thus designed to help our members respond to the challenge of cyber-security threats and improve overall resilience to those threats.

We recognise that, for a business at the beginning of this journey, navigating a route to effective cyber security can be challenging. Cyber security management is different for every business and depends on many variables (e.g. business size and manufacturing sector). Nevertheless, in all cases, cyber is a business risk that needs to be mitigated on an ongoing basis.

Make UK's new services are intended to help our members do just that. Designed specifically with the needs of the manufacturing community in mind, they will help businesses quantify their cyber security risk and take affirmative action to mitigate it.

Our services will also help members demonstrate their cyber security safeguards to customers and suppliers, an increasingly crucial requirement for businesses to operate in our sector.

Make UK is working in partnership with Vauban Group to jointly design, develop and deliver our new Cyber Service. Vauban provides comprehensive cyber risk management services and solutions on an enterprise-wide basis and takes a holistic approach to identifying, protecting against, and preventing cyber-attacks.

Free assessment and advice
The first steps for a business building its cyber defence are to review their network and business processes, to assess what needs protecting, determine what mitigations are already in place and what further work might need to be carried out.

Make UK's service addresses this need directly by providing a free-to-use Assessment Tool, developed by Vauban, that will enable Make UK members to consider and assess their cyber security risks.

SME manages risk after using assessment tool

The owner of a small engineering design company in the north of England contacted us. For over a year now, they recognised that they ought to look at their cyber security vulnerabilities but have been frightened by the complexity and did not know where to start. As a first step, they completed our Cyber Security Assessment Tool and are on their way to managing their risks properly.

Accessed via the Make UK website, the easy-to-use Assessment Tool explores the processes and systems required to manage cyber security risks and their interaction with members' business processes.

The Assessment Tool, which takes the form of a questionnaire, uses simple, plain language, so that those with no or little IT experience can easily understand it. It takes only a short amount of time to complete (approximately 40 minutes for the basic version).

Participants can choose from two question sets, dependent on their situation: one (for less cyber mature members) is based upon the National Cyber Security Centre's Cyber Essentials scheme. The other (for those with a more mature posture) is based on the ISO:27001 principles.

Upon completion of the Assessment Tool, the results are displayed in a highly visual, easy-to-read display format, allowing members to quickly see where their strengths and weaknesses lie. Some members have commented on how useful the results are in briefing senior management and as a framework for taking necessary action.

As additional value to this free-to-member service, following completion of the online assessment, a member of Vauban's expert team will review the results and prepare a bespoke Summary Report, interpreting the results and giving specific advice and recommendations.

The Assessment and Summary Report will provide a company with a benchmarked roadmap, enabling them to work towards and successfully apply for Cyber Essentials or ISO:27001 accreditations from the relevant awarding bodies.

Vulnerability management

Assessing cyber risk management is the essential first step to building your cyber defence. But it is effective only if you then act on the findings. Yet, as the results of our survey have shown, cyber security can be a daunting subject for manufacturers, and one that requires a level of investment that can be seemingly difficult to quantify.

Busy IT engineer completes assessment tool

When a busy Senior IT engineer at a manufacturer of cooling equipment, in the south of England was asked to pilot the Assessment Tool he was reluctant. But after completing it, he said "the Assessment was very easy to complete, with simple, multi-choice options within the questionnaire. It addressed all areas of cyber risk management, has given us a good picture of what our strengths and weaknesses are and created an easy to follow framework with which to develop plans for improvements."

He also liked the clear infographics used to display the results; this made it much easier for him to present the findings to the Board. He also added "It is easy to make excuses not to look at cyber security; we are all very busy people. Most companies probably do not have dedicated cyber security staff, but this assessment is simple and quick to do and made identifying issues very easy."

The ambition of Make UK's cyber security programme is to demystify this challenge, demonstrating to our members that it need not be complex or expensive to address. There are simple steps that a manufacturing business of any size or type can take that will provide frontline defence, which can be built upon over time as required.

To this end, Make UK's Cyber Service extends beyond our free-to-use Assessment Tool to include services that assist members in managing their cyber risk. Our new services are based upon Vauban's Vulnerability Management Services™ (V2MS™) which has been tailored by Make UK to the specific needs of our membership community.

Cyber risk advisory services

Vauban's NCSC Certified Practitioners will work with the Make UK member company to put in place the identified mitigations required to manage their cyber risk. Bespoke services are tailored to specific company needs.

This includes, for example, a one-day visit of a Vauban NCSC Certified Cyber Practitioner, following the completion of our Assessment Tool and consists of: an onsite visit to the member company to interview stakeholders, gather further information relating to the company's risk; a briefing on the implications of the Assessment Tool results; and detailed advice on the options for the customer.

Other advisory services available include:

- formulating risk management policies and processes for the company
- developing and writing comprehensive incident response plans
- giving guidance and advice on ways to mitigate risks
- developing and delivering an action plan to achieve Cyber Essentials, Cyber Essentials Plus or ISO: 27001 accreditation

The length of time required to deliver these services will depend on the size and nature of the business, their infrastructure, the maturity of their cyber security posture and the member's attitude to risk.

Vulnerability assessment & penetration testing

Vulnerability analysis provides a comprehensive view of how prepared an organisation is to defend against cyber threats. It also offers expert advice on how to manage the risks uncovered by the analysis.

The approach considers not only where actual business risks lie, but also which vulnerabilities should be prioritised and how to address them effectively.

The vulnerability assessment is a process that aims to identify weaknesses. Further testing, exploiting these weaknesses, is conducted during Penetration Testing which is usually tightly focussed on a system or an application simulating irregular activities, emulating those of a determined malicious actor.

The nature and depth of the testing is driven by the customer's requirements. For example, a customer may require a vulnerability assessment to meet the requirements of the Cyber Essential Plus scheme, but may not require a deeper penetration test at that time.

This is a cost-effective way for a company to further improve their understanding of their specific cyber security risks and generate a workable action plan to put in place the right mitigations, including prioritising activity.

Enterprise Cyber Security Management® – ECSM®

In addition to developing the Assessment Tool and offering its Vulnerability Management Services, Vauban offers a suite of services via ECSM® that protect against cyber threats on an enterprise-wide basis.

A combination of V²MS™ and ECSM® expertly evaluates the risks posed by people, policies and business practices as well as those presented by partners, the supply chain and other third parties that interact with the business and can ultimately lead to Assured Cyber Protection™ (ACP™). Rather than looking solely at the strength of siloed technology, the combination of V²MS™ and ECSM® seeks to find the gaps that may exist when different cyber security products are used within a business but are not interconnected, leaving areas of exposure that are open to cyber-attacks.

Preferential pricing for Make UK members

Make UK and Vauban share the aim of helping manufacturers help themselves, providing affordable access to expert advice on how they can act to manage the risks that have been identified. An important part of the relationship is to ensure that Make UK members have access to top-quality service, with trusted advisors at a preferential rate.

We have based our pricing upon government consulting rates rather than commercial rates. Designed with SMEs in mind, our cyber security service are intended to be delivered with an incremental approach, prioritising activity on the most urgent risks and tailoring our service to meet the customer's requirements and limitations.

Make UK - The Manufacturers' Organisation, is the voice of manufacturing in the UK, representing all aspects of the manufacturing sector including engineering, aviation, defence, oil and gas, food and chemicals. Representing some 20,000 members employing almost one million workers, Make UK members operate in the UK, Europe and throughout the world in a dynamic and highly competitive environment.

Britain is one of the world's biggest manufacturing nations. Almost 3 million people work in our sector and deliver almost half of all UK exports. Our companies drive over 60 percent of all UK research and development. As a result of that investment, manufacturing as we know it is changing, adapting, and transforming each and every day.

We're at the cutting edge of innovation; leading the way in developing skills and driving competitive advantage for the UK. Make UK is focused on creating the most supportive environment for UK manufacturers to thrive, innovate and compete. We do this so that together, we can build a platform for the evolution of UK manufacturing.

MakeUK.org

To find out more about this report, contact:

Andrew Kinniburgh
Director General, NDI
020 7654 1534
akinniburgh@MakeUK.org

Sarah Stein
Head of Product Innovation
0207 654 1575
sstein@makeuk.org

MAKE uk
The Manufacturers' Organisation

MAKE BUSINESS
MAKE VENUES
UK STEEL
NDI

MakeUK.org