eef The manufacturers' organisation

CYBER SECURITY FOR MANUFACTURING

RUSI www.rusi.org

In partnership with: AIG

FOREWORD

Stephen Phipson CBE
Chief Executive, EEF

A comprehensive approach to cyber-security is not something that manufacturers can afford to ignore – with the sector now the third most targeted for attack. Only government systems and finance are more vulnerable, yet manufacturing is amongst the least protected against cyber-crime.

The 4th Industrial Revolution represents an unprecedented opportunity through interconnectivity. But that very openness brings with it increased risk. Cyber-vulnerability 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.

Manufacturers must urgently take appropriate steps to protect themselves. Our sector is already a significant target for malicious activity in cyberspace, which impacts businesses in a variety of ways. Increasing digitisation means that the challenge is likely to both broaden and deepen.

As the UK's voice for manufacturing and engineering, EEF has the potential to play a significant role in supporting our manufacturers in the face of this challenge. In partnership with AIG, a leading global insurance organisation, we have surveyed UK manufacturers and commissioned the Royal United Services Institute (RUSI) to conduct research with the EEF membership in order to develop an understanding of the sector's awareness of the issue and its readiness in the face of the existing challenges. This report sets out those findings.

RUSI's world-leading Cyber Security Research Programme is well established as a key independent voice in the battle to understand and counter the evolving cyber-security threat that modern businesses face. Their research on behalf of EEF has demonstrated that levels of cyber-security maturity varies considerably across the manufacturing sector. Some businesses have strong awareness and robust plans, processes and equipment in place to reduce the risk, and others have limited awareness and very few cyber-security controls in place. It is not always the case that the large, well resourced, business is better prepared than the SME. The digital age is already resulting in the evolution of risk within manufacturing and AIG is developing innovative solutions to help manufacturers understand their cyber-security exposures.

EEF is committed to both supporting and representing the manufacturing sector to address the cyber-security challenge as part of the 4th Industrial Revolution.

EXECUTIVE SUMMARY

Manufacturing is a significant target for cyber-criminals. This can result in the theft of sensitive data, the disruption of access to systems or operational technology, or industrial espionage for competitive advantage. In our survey of manufacturers, 48% said that they have at some time been subject to a cyber-security incident, half 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.

Moreover, cyber-related risks for manufacturers are only likely to deepen and broaden with increasing digitisation. While 91% of businesses surveyed say they 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.

Across our sector, maturity levels are highly varied both in terms of awareness of the cyber-security challenge and the implementation of appropriate risk mitigation measures. 41% of manufacturers don't believe they have access to sufficient information to confidently assess their specific risk, and 45% are not confident they are prepared with the right tools for the job. A worryingly large 12% of manufacturers surveyed have no process measures in place at all to mitigate against the threat.

EEF welcomes the steps the government is taking to improve national cyber-security resilience. But, to date, no priority has been given to the specific needs of manufacturing. This must change. There needs to be a particular focus on the requirements of our sector, recognising that a one-size-fits-all approach for business is insufficient and, equally as importantly, comprehensive security cannot be the exclusive domain of large businesses who can afford bespoke end-to-end protection.

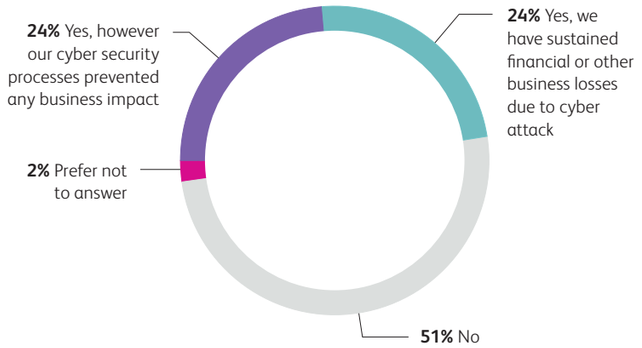
The impetus for change is coming from manufacturers themselves. The need to have demonstrable cyber-security safeguards in place is becoming ever more necessary to operate in the business environment. 59% of manufacturers report that they have already been asked by a customer to demonstrate or guarantee the robustness of their cyber-security processes, and 58% have asked the same of a business within their supply chain. For the 37% of manufacturers who report that they could not do this if asked to today, business will become increasingly challenging.

However, while some manufacturers are only at the beginning of their cyber-security journey, as this report shows, sensible precautions and a proper cyber-security business plan are in reach of all. These measures will provide the confidence businesses need to invest in digitisation, and the credibility to operate in the sector as a trusted supplier.

THE CYBER THREAT LANDSCAPE AND THE MANUFACTURING SECTOR

Seldom does a week go by without a report in the press of a cyber-security incident, with sectors from the health service through transportation to retail suffering data breaches, data losses or disruptions of service. The UK National Cyber Security Centre (NCSC) reported over 1000 cyber-attacks in its first year of operation with nearly 600 being classified as significant. At the same time the Office of National Statistics highlighted that 5.2 million incidents of cyber-crime were reported in the first half of 2017 for England and Wales alone. This represented nearly 50% of total reported crime for that period[1].

Chart 1: Half of manufacturers have suffered from cyber-attack



While these numbers are troubling in themselves, this probably represents only the tip of the iceberg; many cyber-attacks go unreported as individuals and businesses either fail to notice them or do not report them in order to avoid reputational damage. In EEF's cyber-security survey some 48% of manufacturers reported having been subject to cyber-attack, around half of whom said they had suffered loss as a result. Of course, this does not include those businesses who do not even realise that they have been subject to an attack.

When considering cyber-security threats there is an understandable tendency to focus on threat actors. The 2016 UK National Cyber Security Strategy (NCSS), for example, refers to 'script kiddies', hacktivists, cyber-criminals, terrorists and state/state-sponsored threats[2]. However, categorisation by threat actor is not particularly useful, as different actors often use similar attack methods as one another and have similar financial or political motivations.

"48% of manufacturers have been subject to cyber-attack"

In early 2016, hackers attempted to steal around US$ 950 million from the Bank of Bangladesh and eventually got away with around US$ 80 million. Although this incident initially appeared to be a case of straightforward cyber-crime, it was subsequently linked to an organisation known as the Lazarus Group, which has connections to the North Korean state. The Lazarus Group has also been linked to the WannaCry attack of May 2017, which caused significant disruption to the NHS, as well as individuals and businesses across the globe. Beyond alleged North Korean-backed activity, a destructive cyber-attack on the French television broadcaster TV5 Monde in 2015 was publicly claimed by the 'Cyber Caliphate', suggesting a link to the Islamic State, but was later tied to a hacker group linked to Russian military intelligence. At the same time there have been reports of Russian criminal group involvement in the theft of emails that were later used in an information campaign designed to disrupt the 2016 US presidential election.

Categorisation and identification of threat actors is also challenging owing to the technical difficulties associated with the attribution of responsibility for cyber-attacks. Difficulties with attribution has enabled states and other actors to adopt a position of 'plausible deniability' with regard to their actions. This challenge has been further complicated by the relatively easy availability of cyber-crime 'as a service' on the dark web, meaning that individuals and groups no longer require the technical skill necessary to undertake criminal activity in cyberspace. Instead, malicious actors can simply outsource that activity to others.

To understand threats to the manufacturing sector, it is preferable to consider the nature of these cyber-attacks, rather than the threat actors. Ultimately, the majority of cyber-attacks are conducted either for financial gain (including competitive advantage) or aim to disrupt or damage a target. For example, denial-of-service attacks, which impact on a customer's and/or supplier's ability to access a business, or the simple defacement of a business's website, might be designed to undermine the credibility of that business or be used as part of a blackmail campaign.

Similarly, in a 'ransomware' attack, data is encrypted and is only made available again on payment of a ransom. In some cases, data might be stolen to obtain personal information to be used for fraud or blackmail, or to obtain intellectual property to be sold on or used for competitive advantage. Particularly in the case of manufacturing, data might be stolen to gain personal competitive advantage, disrupt the business's operations, or to be sold on to competitors.

Lastly, increasing digitisation in the manufacturing sector is opening up new opportunities for cyber-criminals to target operational technology, including production lines and manufacturing equipment, with a view to damaging the infrastructure and production facilities of a business. In these instances, threat actors would usually be motivated to gain competitive

INDUSTRIAL CONTROL SYSTEM ATTACK IN SAUDI ARABIA

In August 2017, a petrochemical manufacturer in Saudi Arabia was infected with malware that investigators believe was not simply designed to steal data or shut down operations but potentially to cause a catastrophic explosion. Significantly, it targeted operational technology in the form of industrial control systems rather than the more traditional focus on information technology.

Whilst the identity of the company affected and the likely attackers remain unclear, it has been revealed that the target was part of the facility's safety system, designed to stop automated equipment going beyond safe operating conditions. The malware was designed to override this.

The attack was not intercepted by the cyber security measures in place and failed only because as the developers of the malware had made an error in the code that caused the systems to simply shut down safely. It is likely that the perpetrators will have since fixed this error.

[1] ONS Statistical Bulletin: Crime in England and Wales to June 2017
[2] UK National Cyber Security Strategy 2016-2021

advantage. A 2017 attack on the industrial control systems of a Saudi Arabian petrochemical company dramatically highlighted the need for businesses to factor risk to operational technology as well as information technology in their cyber risk assessment[3].

In its 2017 Threat Intelligence Index, IBM identified manufacturing as the third most attacked sector after Government and finance, based on data from publicly available reports and information from its own clients[4]. The attacks identified focused primarily on obtaining either intellectual property or internal operational information, although there were also examples of ransomware attacks and more traditional fraud for financial gain through phishing emails. Manufacturing is considered to be an attractive target by some as it is not a closely regulated industry compared to, for example, the financial sector and there are vulnerabilities in both operating systems and industrial control systems that can be easily exploited.

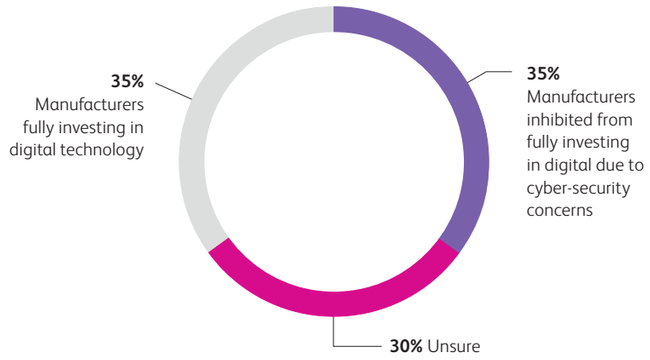
A particularly pertinent example occurred in 2014, when a steel mill in Germany was catastrophically damaged because of a cyber-attack. Focused on a vulnerability in an industrial control system, access was reportedly initially obtained through the business administration network. This again highlights the critical necessity for manufacturers to consider vulnerabilities in both operational and information technologies. Evidentially, this is not just a problem of securing IT systems, but understanding how production facilities and operational equipment interfaces with cyberspace in order that it too is hardened against attack. In this regard, it is worth noting that, in 2012, the oil company Saudi Aramco was subject to a simple attack that, due to uncontrolled contagion, wiped the data from some 30,000 administrative computers, almost bringing production and distribution to a complete halt.

GERMAN STEEL MILL MELTDOWN

While the exact details of the company involved are still unknown, the attacker used sophisticated social engineering and spear-phishing tactics to hack into the steel mill's office computer network. Crucial controls were tampered with, making it impossible to turn off the blast furnace. The result - massive damage to the foundry.

The attacker, likely an industry insider or someone working with an insider, had specific knowledge of the production processes involved so that maximum damage could be done to the normal workings of the mill. The company's systems were specifically vulnerable because the office network was connected to the industrial control system, meaning the attackers could effectively take control of production – and stop it from happening.

Chart 2: Cyber vulnerabilities inhibit over one-third of manufacturers from investing in digital technology



[3]IBM Report on Security Trends in the Manufacturing Industry
[4]IBM Report on Security Trends in the Manufacturing Industry

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. EEF 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. However, while 91% of manufacturers say they are investing, or intend to invest in digital technologies, our survey showed that 35% consider that cyber-vulnerability inhibits them from doing so fully. This suggests that opportunities to enhance productivity and growth are being missed and some businesses risk falling behind in the race to digitise. Yet many manufacturers are perhaps unaware that there are appropriate mitigations relating to processes, people and policies that can reduce the risk significantly. While security should be both designed and built-in from the outset of the 4th Industrial Revolution, evidence from the early days of the 'Internet of things' (e.g. the connection of devices such as fridges and baby alarms to the Internet) highlights the danger of treating cyber-security as an afterthought. Failure to change default security settings made it possible for these devices to be used to take down large sections of the Internet in a denial-of-service attack in 2016. One manufacturer of digital control systems has indicated that around 90% of their products do not have the default settings changed on installation[5]. Thus, the challenge posed by threats in cyberspace is unlikely to decrease any time soon for the manufacturing sector.

"91% of manufacturers are investing in digital – but 35% consider cyber vulnerabilities inhibit them from doing so fully"

[5]UK National Cyber Security Strategy 2016-2021

CYBER-SECURITY: A GOVERNMENT PRIORITY AND A COMMERCIAL NECESSITY

While the NCSS does not specifically identify manufacturing as a sector at risk it does commit the Government to an expanded role where it had previously assumed that the market would drive the necessary measures to improve cyber-security. At the heart of this change was the launch of the NCSC, initially staffed primarily by individuals from GCHQ. This was met with high expectations and some scepticism in relation to the NCSC's capacity to significantly change the UK's approach to cyber-security in relation to manufacturing.

Over the coming years, the NCSC will continue to establish its networks and build that capacity, but thus far it has been quick to deliver an impressive platform of cyber-security messaging, particularly through social media. At the heart of its approach is a strategy called 'Active Cyber Defence' that seeks to take measures to stop threats at the UK borders of cyberspace rather than allowing them to permeate the community. This is not the same as the infamous Great Firewall of China, which blocks anything perceived to be a threat to the People's Republic, but rather constitutes a series of measures that are designed to reduce the UK's overall vulnerability.

But recognising that, in order to be truly effective, cyber-security requires a particularly close relationship between the public and private sectors, the NCSC launched the 'Industry 100' programme. This programme is designed to bring skilled individuals from the commercial sector into the NCSC on secondment to boost the NCSC's capacity and to benefit the private

Chart 3: Half of manufacturers are reviewing their cyber-security arrangements due to GDPR

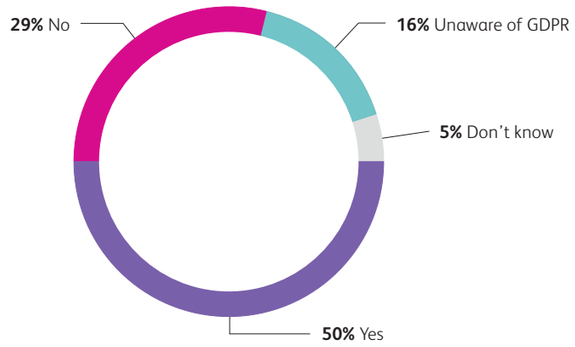
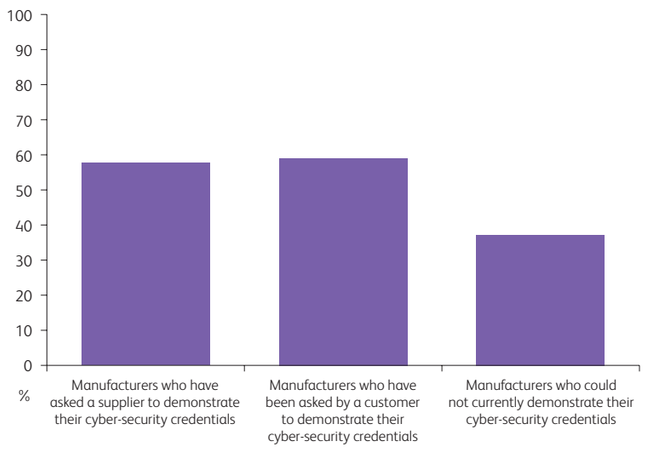


Chart 4: Manufacturers are increasingly being asked by customers to guarantee their cyber-security - and asking their suppliers to do the same



sector by providing unique skills and access to seconded employees.

Though there is no mandated regulatory standards governing cyber-security in manufacturing in the UK, the all-encompassing nature of digital technology means that much new regulation is having a direct impact on the business approach to cyber security. The EU General Data Protection Regulation (GDPR) is designed to secure personal data on EU citizens held by businesses globally and comes with a set of relatively punitive punishments for failures to do so. The relevant focal point in the UK Government for GDPR is the Information Commissioner. The regulation will clearly impact on the manufacturing sector's approach to cyber-security given the need to have appropriate measures in place to protect the personal data of both staff and customers. Some 50% of manufacturers indicated that the imminent application of GDPR had caused them to review their cyber-security arrangements. Regulation is likely to continue to be a key tool of UK Government intervention in cyber-security.

The landscape of cyber-security standards across the globe is complex in relation to both the definition and measurement of those standards and the benefits of adhering to them. A UK Government report of 2013 identified as many as 1,000 different standards worldwide in a complex array that makes it difficult for businesses to identify what fits best for them[6]. At home, the Government is increasingly driving the Cyber Essentials standard, which is now mandatory for some public-sector contracts.

However, while the scheme provides some very necessary protections, it is less clear that it is entirely suitable for the cyber-security environment of the manufacturing sector. Given the potential for linkages between the requirement for business to achieve certain cyber-security standards in order to be awarded contracts, the sector arguably needs a stronger input into Government thinking.

Yet change will not be driven by Government alone. As manufacturers, suppliers and customers are becoming increasingly aware of the challenges posed by cyber-crime, they are themselves the arbiters of change. As a result, the requirement to demonstrate that certain cyber-security measures are in place is going to become ever more necessary in order for businesses to operate in the sector. This is fast becoming a fundamental business requirement no matter how big the business and where it sits in the supply chain. Government's role must be to ensure that a conducive business environment exists.

As supply-chain issues become critical, some 59% of manufacturers reported that they have already been asked by a customer to demonstrate or guarantee the robustness of their cyber-security processes, and 58% have asked the same of a business within their own supply chain. Increasingly, this is becoming part of contractual arrangements. It is thus evermore important for the 37% of manufacturers who report that – as of today - they could not demonstrate good cyber-hygiene to arm themselves with the tools necessary to provide such assurances.

"37% of manufacturers are not certain they could demonstrate their cyber-security credentials to a customer"

[6]Department for Business, Industry and Skills – UK Cyber Security Standards Report November 2013

THE CHALLENGES FOR THE MANUFACTURERS

All companies should understand more than ever that a cyber-attack on their organisation is not a question of if, but when, by whom and to what degree. Although most large companies have strengthened their cyber-security capabilities in light of recent events, the research undertaken by RUSI did indicate that the extent of cyber-security maturity is highly varied among manufacturers, and some manufacturers are only at the beginning of their cyber-security journey. When queried further, manufacturers raised the following specific cyber-security challenges, many of which are interlinked.

- Almost half (**41%**) of manufacturers surveyed do not believe they have access to sufficient information and advice to confidently assess their specific cyber-security risk, whilst a similar number (**45%**) are not confident that they have the right tools, processes and technologies to mitigate the risk. It was notable that compared to relatively high uptakes for measures such as firewall and anti-malware software, only just over half of business regularly patched their systems.
- Cyber-security is not considered to be a principal risk on the risk register for many manufacturers, although some **60%** indicated that it was included to some extent. This reflects a lack of understanding about the potential threats from cyber-crime.
- Manufacturers face diverse cyber-security challenges and there are inevitable differences in cyber-security maturity, and the associated financial, human and technical resources available to organisations to manage and mitigate cyber-risk. Although **75%** of manufacturers reported that they monitor and protect their systems and software from cyber-attack, significantly fewer have a comprehensive business strategy in place, including risk registers and staff training. In a large part, this reflects a lack of understanding

Chart 5: Almost all manufacturers have some technical protections in place - but this isn't always comprehensive

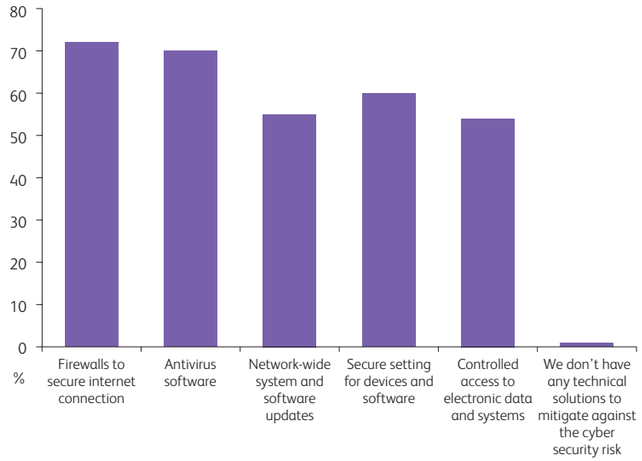
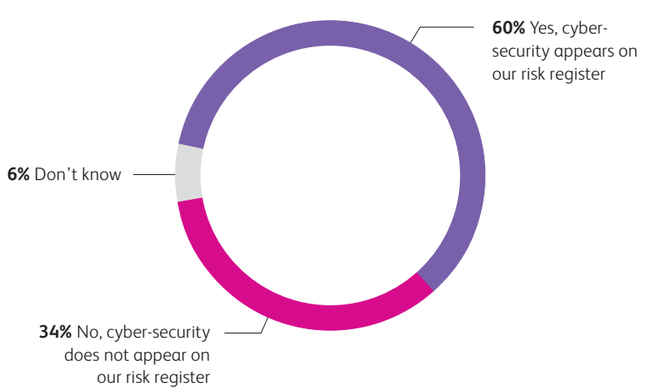


Chart 6: Only six in ten manufacturers include cyber-security on their risk register



"34% of manufacturers are not educating their staff in good cyber-security practice"

of the increased importance of cyber risk management.

- A significant number of manufacturers indicated that there was a lack of awareness and understanding at board level of the extent of the cyber-security challenge to the business, which made it difficult to secure an appropriate operational focus and funding from senior leadership for cyber-security risk management programmes.
- Some manufacturers highlighted that as part of the struggle to raise cyber-security awareness, this is sometimes perceived to be a complex and deeply technical subject which deterred some senior leaders from engaging with the risk of cyber-crime and other cyber-security threats.
- Most manufacturers believed that it was important for a business to follow a risk management framework that was actionable yet flexible. However, there was a concern that some existing cyber-security frameworks are too rigid to adhere to and not tailored for the challenges faced by the manufacturing sector.
- A worryingly large **12%** of manufacturers reported in the survey that they have no technical or managerial measures in place to either assess or mitigate against the threat from cyber-attack. Given that almost all the businesses reporting this are SMEs, there needs to be a particular focus on their requirements and perhaps support from larger businesses.
- The increasing convergence between operational technology and information systems is a specific cyber-security risk for the manufacturing sector. Operational technology might be old and not be supported or patched by suppliers. It is often designed to operate 24/7, so downtime to implement cyber-security solutions is undesirable for businesses.
- Cyber-security risk management is not solely about technology, but also relates to people and processes. Some manufacturers indicated a concern as to how to evaluate cyber-security awareness among employees,

Chart 7: Not all manufacturers have a board member who is accountable for cyber-security

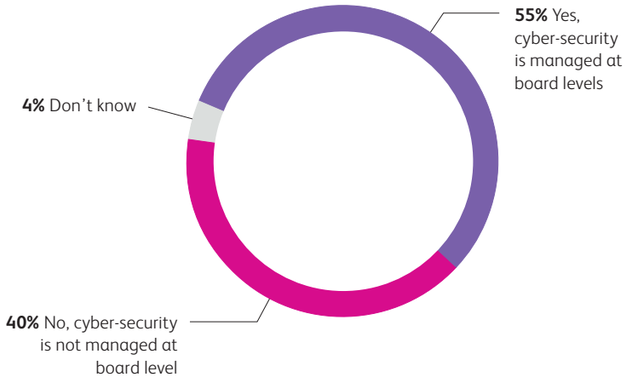
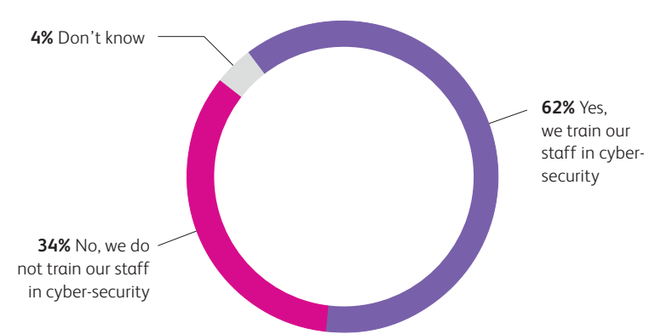


Chart 8: Employee training and evaluation in cyber-security is not universal



how to encourage a better security culture and behaviours, and how to design and implement improved cyber-security policies and procedures.

- Although the National Cyber Security Strategy (NCSS) consolidates many challenges, some manufacturers stated that it does not fully engage with the various threats and potential response strategies as they relate to the manufacturing sector. Business would like to see specific cyber-security guidance for the manufacturing sector.

CYBER-SECURITY RISK MANAGEMENT

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 from manufacturer-approved stores, or running apps and programs in an isolated environment
5. Continually ensure your operating systems and software are up-to-date and running the latest security patches

As most manufacturers are aware, there are various ways to deal with risk, you can avoid it completely; reduce it; accept it; or transfer it. The NCSC has released guidance on basic cyber-security risk management principles that can be applied to all organisations, regardless of their size. It states that the first step for any organisation in cyber risk management is to compile a baseline of security controls, such as those defined in Cyber Essentials, the Government backed scheme designed to help any business or organisation protect itself against the most common types of cyber-attack.

Cyber Essentials works on the principle that the vast majority of cyber-attacks are basic in nature, untargeted and unsophisticated. They are designed to prey upon systems without even the most rudimentary protection measures; the digital equivalent of a thief trying your front door to see if it's unlocked.

For a small fee, Cyber Essentials provides a tool for self-assessed certification, giving protection against these most basic of threats. This provides peace of mind to a business and evidence that a minimum level of system protection has been achieved. Moreover, it is particularly valuable when considering that vulnerability to simple attacks can identify a business for targeted attention from cyber-criminals. The more comprehensive 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.

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. Though, due to the nature of their business, the MOD are leading in mandating cyber-security standards on their suppliers, 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.

An effective risk management strategy must continuously assess which people, information, technologies and business processes are most critical to an organisation, so that these assets can be prioritised and protected by security controls. All organisations should also carry out scenario planning to predict the consequences of a cyber-security infrastructure or data breach. This will allow an organisation to work out where to deploy resources and how to effectively respond to an incident. A good risk management strategy will recognise that not all risks can be mitigated and instead, it should focus on those that the organisation can take practical steps to mitigate. There is no 'one size fits all' approach to cyber-security and the extent to which risk management standards and frameworks can be applied depend upon the specific requirements of each business. Finally, it is important to stress that cyber-security risk management should not be a one-off exercise. Any company's assessment of risk should be subject to a process of constant review.

"Manufacturers will find cyber-security standards an increasingly necessary aspect of business readiness in order to trade."

THE ROLE OF INSURANCE

When considering the current cyber-security landscape for the manufacturing sector, it is important to note the growing importance of the cyber-insurance market. Manufacturers should consider the utility of cyber insurance as a vehicle for improving cyber-security maturity. This is a developing market, but in order to receive cover, insurers can advise organisations on how to increase their cyber-security maturity. This can include advice on how to conduct risk assessments, ways to identify the appropriate products, processes and services to manage cyber risk, and possibly even the steps to take to achieve a specific cyber-security standard. Meeting the conditions of cover, and knowing that, in the event of a cyber-security breach, recovery support is at hand, can provide peace of mind to a manufacturer as well as providing valuable supporting evidence to customers that a business is cyber-mature.

There are some 77 insurers that offer insurance products against cyber-attack and the range and suitability of these products for manufacturers of all types and sizes is developing, recognising that there is no single model that will suit all. The insurance market undoubtedly offers a nuanced understanding of the general and specific risk to manufacturers from cyber-security breaches, including both the immediate impact and longer-term reputational damage. This market could also incentivise organisations to take cyber-security risk management more seriously. Nevertheless, our survey suggests that only one third of manufacturing businesses surveyed are currently insured against a cyber-breach to their business. This figure is only likely to grow as the market matures.

Chart 9: A growing role for cyber insurance

	Total
We have insurance to cover loss due to cyber attack	33%
We have considered but rejected insurance to cover loss due to cyber attack	25%
We are aware of, but not considered insurance to cover loss due to cyber attack	20%
We do not consider our risk to be sufficient to warrant insurance to cover loss due to cyber attack	14%
We are unaware that such insurance products existed for businesses in the manufacturing sector	2%
Don't know	5%

"Two-thirds of manufacturers are not insured against cyber-attack"

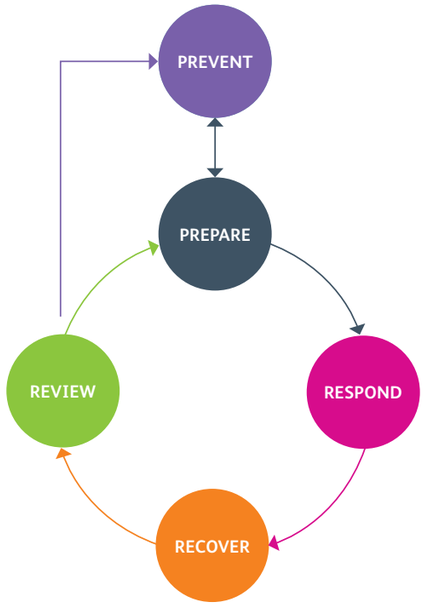
CYBER-SECURITY TOOLS AND SERVICES

Part of the challenge for manufacturers is to find their way through the huge range of cyber-security products and services available in the marketplace. Even for those who are cyber-aware, it can be difficult to identify what is essential, what is useful and what is completely unnecessary. This reflects both differences in the range of requirements for businesses and organisations, and the relative immaturity of the market place. There are very few standards against which to assess the quality of individual products which can also make it difficult to decide what is appropriate. This also links to a lack of detailed research that can demonstrate the cost-benefit balance of certain approaches to cyber-security, beyond the fact that doing nothing to mitigate the risk is not a viable option.

Frameworks of cyber-security standards are becoming increasingly important as the public sector and others in the supply chain demand that suppliers have achieved a certain standard in order to be contractually compliant. Perhaps the basic level of compliance at present is the Cyber Essentials scheme, although some manufacturers have indicated a concern as to its suitability for the manufacturing sector overall. However, it does remain a sound starting point for those beginning their cyber-security journey. Arguably the next level is the ISO 27000 series of standards which aim to help business manage data assets that relate to things such as financial information, IP and personal data. Whilst again this does not particularly focus on weaknesses in the operational systems element within the manufacturing sector, it does provide a sound basis for a business to develop its approach to cyber-security.

There are many businesses in the market place that will provide a range of integrated services by either offering packages of software and hardware, or consultancy services that assist with risk management and identify and implement the measures needed to achieve cyber-security standards. However, it can be difficult for a business to identify which if any of these providers is most appropriate and offers best value for money.

The cyber resilience lifecycle offers one way to manage any identified cyber-security risks. It is recommended that each element of the cyber resilience lifecycle is overseen by a nominated member of the board.



Prevent:
Seeking to avoid cyber-security breaches by introducing stronger cyber-security protections

Prepare:
Developing structure and plans to mitigate the impact of a potential cyber-security breach

Respond:
Convening all parts of the business to implement the incident management plan

Recover:
Reducing any residual cyber vulnerability and managing any resulting reputational damage

Review:
Taking stock of lessons learnt from any incident and incorporating these into a strategy

Source: British Retail Consortium: Cyber-security Toolkit

THE UK CYBER-SECURITY COMMUNITY

Effective cyber-security at both the national level, and for businesses, requires close cooperation between the public and private sectors. Unfortunately, the public sector cyber-security landscape can appear to be highly complex and fragmented. This reflects the pervasiveness of the challenge across all sectors of public life and the need for elements to deal with both the prevention of, and the response to, cyber-security incidents. The following outlines some of the key actors who can support a business in its cyber-security risk management effort.

Local Law Enforcement

Whilst the picture varies across the UK, almost all police forces now have a clearly identifiable point of contact for dealing with cyber-security issues. The depth of the crime-prevention advice and investigative response is varied, but manufacturers can expect to find specially trained officers who can provide advice on both cyber-security mitigation and response, particularly where there is a risk of criminal activity. The individual forces are supported by the Regional Organised Crime Units (ROCUs) who generally have more specialist officers available to provide support. Individual forces, often with the active support of the ROCUs, regularly run events to support business both in improving awareness of the threat and to suggest risk management and mitigation measures.

City of London Police and Action Fraud

Much of the cyber-security challenge manifests itself as criminal activity and in particular, fraud. In most cases this can represent a jurisdictional challenge with the criminals operating from one geographical location, whilst targeting another, and then perhaps accessing the proceeds of the crime in a third location. This illegal activity will spread across different locations in the UK and most likely, internationally. With the geographical challenge in mind, City of London Police host the National Fraud Intelligence Bureau (NFIB) and Action Fraud (AF). AF is the UK's national reporting centre for all fraud and cyber-crime and should be your first stop if you fear you have been subject to a cyber-attack with criminal intent. As well as taking the appropriate steps to address the investigation of the crime, AF will also initiate the targeted business receiving follow-up cyber-security advice either from City of London Police, the ROCU, or the local force depending upon the nature and severity of the incident.

National Crime Agency (NCA)

The NCA is home of the National Cyber Crime Unit (NCCU) which coordinates the national response to cyber-crime. It has the capacity to receive information from businesses to be used as intelligence rather than as evidence towards a prosecution. Any such material provided by an organisation is always handled in such a way as to protect business confidentiality which is important when considering the potential reputational damage to a business from a cyber-attack.

National Cyber Security Centre (NCSC)

The NCSC is increasingly providing a central leadership and coordination role in the public sector. In addition to delivering a coherent threat message through a range of media, it is also supporting and helping to prioritise the activities of the law enforcement agencies mentioned previously. It also runs the Cyber Security Information Sharing Partnership (CiSP) which is a joint industry and government initiative set up to exchange cyber-threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business. Joining CiSP is relatively straightforward and not only gives businesses access to national networks to share threat information, but also access to sub-groups which are focused regionally and by sector.

AIG VIEWPOINT

Romaney O'Malley
Head of Industrials Segment, AIG UK

Cyber incidents on the rise

At the beginning of 2017, AIG cyber experts predicted it would be a year of business interruption and extortion through cyber-crime, a prediction that proved correct. This year we expect that theme to continue, albeit in a more targeted way.

So what does this mean for manufacturing firms?

Over the past 12 months it has become clear the cyber threat landscape has evolved, with attacks becoming more sophisticated and more broadly disruptive. Our cyber claims statistics back this up, with encryption ransomware extortion and other extortions leading the way.

Widespread ransomware outbreaks were followed by the first of the much expected worm versions of ransomware in May; the high profile WannaCry and NotPetya ransomware incidents impacted businesses around the world, including a number in the manufacturing sector. Production in the automotive, oil and gas, farming and food industries were among those that were brought to a halt while companies worked around the clock to restore and recreate data that had been encrypted by the malware.

The attacks themselves were not necessarily motivated by financial gain, but by a desire to inflict damage and commotion. And it was this disruption that was responsible for the bulk of the cyber business interruption losses, with the cost of WannaCry estimated at $8 billion, according to cyber security firm Cyence. It was also a busy year for cloud services being hacked and data being held to ransom, or the company owning the data being extorted.

We are seeing an increasing state-sponsored element to the attacks between nation states, where companies infected by malware may be collateral damage rather than the direct target of an attack. However, while state-sponsored cyber crime might not always target a specific business, it is often aimed at the economic undermining of a rival.

Thus, private sector businesses, including manufacturers, will continue to be targetted by cyber attacks (both generally and specifically) and these are likely to get more sophisticated. This requires constant vigilance and evolving defence. Certainly, as 2018 progresses, we expect to see a refinement of these modes of attack.

Setting the cyber security agenda

As companies set their cyber security strategy, it is important to understand the changing threat environment and be clear which risks pose the biggest danger to your organisation. A quick glance at AIG's cyber claims for 2017 shows the prevalence of ransomware, data breaches due to hackers, security failures due to unauthorised access, impersonation fraud and finally data breaches due to employee negligence.

Many of these cyber risks have a human element and it is important to make sure staff are trained to identify security risks, such as phishing scams and signs of fraud. Statistics suggest that in excess of 80% of all cyber losses have a human element, whether malicious or erroneous, such as clicking on a link or losing a laptop.

In AIG's experience, manufacturer's vulnerabilities can be linked to the age of their equipment and the networked nature of production facilities. Just as sprinklers and fire doors are installed to prevent the spread of fire through your property, so too should strong security measures be taken to ensure a networked building cannot be hacked and exploited. A compromised thermostat could easily spoil food or pharmaceutical products if turned up by just a few degrees.

As discussed in this report, physical damage resulting from a cyber intrusion is an exposure for manufacturers. We know there are botnets out there scouring cyberspace for insecure devices, as demonstrated by the Dyn DDoS attack of 2016. We also know that many of the networked devices, collectively referred to as the Internet of Things (IoT), were not always designed with security in mind.

These vulnerabilities are further magnified by the average age of production equipment within many facilities. Industrial equipment that is ten years old - or older - was never designed to be part of a networked environment. These legacy components can exacerbate the threat as the production environment becomes ever more connected.

Time for a cyber healthcheck?

Cyber insurance is more than just an exercise in transferring risk to the insurer. Most cyber insurers offer a comprehensive package of pre-loss services to help you to carry out a cyber health check. These are important as they can assist in highlighting gaps in your cyber risk management and help identify what security measures should be prioritised; be they technical, processes or people (or a mixture). These also provide a measurable benchmark, which can be used as evidence of your cyber credentials and cyber risk maturity.

It is important to stress test your insurance policies in this way to see how they would respond to a cyber incident. It is possible, with support, to work through various cyber scenarios to determine where such gaps exist and whether a standalone cyber policy is needed.

It is worth going through the exercise, even if ultimately the decision is to take the risk on your balance sheet. Companies will be better placed to determine what cyber security best practice looks like for their organisation, bearing in mind that even with the right technology and employee practices cyber breaches will still occur; it is a case of when, not if.

The manufacturers' organisation

EEF, the manufacturers' organisation, is the representative voice of UK manufacturing, with offices in London, Brussels, Wales, and every English region.

Collectively we represent 20,000 companies of all sizes, from start-ups to multinationals, across engineering, manufacturing, technology and the wider industrial sector. We directly represent over 5,000 businesses who are members of EEF. Everything we do – from providing essential business support and training to championing manufacturing industry in the UK and the EU – is designed to help British manufacturers compete, innovate and grow.

From HR and employment law, health and safety to environmental and productivity improvement, our advice, expertise and influence enables businesses to remain safe, compliant and future-focused.

For further information contact:

Andrew Tüscher
Director of NDI
atuscher@eef.org.uk

Oliver Welch
Head of Defence, Aerospace and Security Policy
owelch@eef.org.uk

RUSI

The Royal United Services Institute (RUSI) is an independent think tank engaged in cutting edge defence and security research. A unique institution, founded in 1831 by the Duke of Wellington, RUSI embodies nearly two centuries of forward thinking, free discussion and careful reflection on defence and security matters.

For further information contact:

James Sullivan
Research Fellow in Cyber Threats and Cyber Security
jamess@rusi.org

AIG

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security.

Our Manufacturing Industry Group pulls together the strengths and capabilities of AIG together to focus intensely on the current and future needs of the Manufacturing sector. We have a strategic partnership with EEF, the leading Trade Industry Body for the sector to ensure we are at the forefront of the market in providing tailored and distinctive risk and insurance value propositions for a fast moving and developing sector. With the onset of 4IR (Fourth Industrial Revolution) and the evolution of risk within Manufacturing, our Cyber Health Check is an example of our innovative solutions to help our clients understand cyber exposures.

www.aig.co.uk

For further information contact:

Mark Camillo
Head of Cyber, EMEA
mark.camillo@aig.com

Martin Overton
Cyber Specialist, EMEA
martin.overton@aig.com

The manufacturers' organisation

We foster enterprise and evolution to keep your business competitive, dynamic and future focused

www.eef.org.uk

www.linkedin.com/company/eef

© EEF 2018