ROYAL
ACADEMY OF
ENGINEERING

Cyber safety and resilience

strengthening the digital systems that support the modern economy

March 2018

www.raeng.org.uk/cybersafety

ISBN: 978-1-909327-38-2

Published by
Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG

Tel: 020 7766 0600
www.raeng.org.uk

#RAEngDigital

Registered Charity Number: 293074

Contents

Foreword

The world we live in is becoming more connected. Infrastructure and other engineered systems that support our modern society are increasingly being linked together through digital connections. This offers great opportunities for both business and individuals. Connected systems underpin improved services, drive innovation, create wealth and help to tackle some of the most pressing social and environmental challenges. This was the conclusion of an earlier Academy and IET report *Connecting data: driving productivity and innovation*. The report, however, also highlighted that increasing the connectivity between physical and digital systems brings with it increased risks. It recommended that work be done to investigate measures needed to strengthen the safety and resilience of all connected systems, particularly critical infrastructure that society now depends so much on. This report takes up that challenge.

Improving cyber safety and resilience requires all stakeholders to act together at scale and in a coordinated way, including government, the engineering profession, system operators and industry leaders. This report will help each of these groups to better understand the new systems that are being created, the emerging vulnerabilities and how to address them. Drawing on the knowledge of Academy Fellows and other experts in the field, it presents a set of general recommendations on how the UK can take a lead on developing safe and resilient systems. It also recognises that, in many cases, solutions are sector-specific. To understand this better, it considers the connected health devices sector as a specific case study.

In my present position at Imperial College London and my previous position as the UK Government's Chief Scientific Advisor for National Security I understand very well the critical importance of the issues addressed in this report. Digital technologies are innovating fast and we rely on them more and more. We must work together to understand the risks and to build and operate safe and resilient systems that can unlock the benefits digital technologies offer.

Professor Nick Jennings CB FREng
Chair of the working group

Professor of Artificial Intelligence and Vice-Provost (Research and Enterprise)
Imperial College London

Executive summary

Cyber safety and resilience are essential properties of the increasingly complex and interdependent systems that support the modern economy. Cyber safety refers to the ability of digital systems to maintain adequate levels of safety during operation, including in the event of a cyberattack or accidental event, protecting life and property. Safety is a desirable property of a system during normal operation, whereas resilience describes the capacity of a system to handle disruptions to operation. Cyber resilience refers to the ability of digital systems to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events. It encompasses people-centred aspects of resilience such as reporting, crisis management and business continuity. This report presents the broad range of challenges that need to be addressed to improve the cyber safety and resilience of systems. The evolving nature of the challenges will require continual responsiveness and agility by government, regulators, organisations and their supply chains. The report identifies measures needed to address these challenges across all sectors. To help illustrate these general principles, the report shows how they can apply to connected health devices in the health sector.

The integration of physical and digital systems creates many opportunities for improved performance and innovation in the supporting systems of a modern economy, generating economic value and creating social and environmental benefits across all sectors. The government's industrial strategy White Paper[1] recognises the opportunities to exploit underpinning digital technologies, with 'artificial intelligence (AI) and the data-driven economy' named as one of four 'Grand Challenges'. The new government Office for AI will work initially with six priority business sectors, including cybersecurity. Digital technologies will also underpin the success of other Grand Challenges – clean growth, mobility and an ageing society – by enabling smart systems and greater resource efficiency, underpinning new business models in transport and driving innovations in health and care. The government's renewed focus on industrial strategy and its recognition of the importance of digital technologies is very welcome, but it needs to match the aspirations set out in the strategy with robust oversight, the necessary funding and changes to regulatory and legislative frameworks to support the strategy's delivery.

There is growing awareness of the risks associated with such 'systems of systems'. Systems may be under the control of different organisations, with differing objectives that may not be aligned. Systems can also span nations across the globe. For example, multinational companies may monitor sites remotely, or even control them, from another country. It is vital that risks are addressed so that serious incidents are avoided, trust in such systems is maintained and the potential benefits are realised. These risks are highlighted in the government's *National Cyber Security Strategy 2016 to 2021*[2] and the *National Risk Register of Civil Emergencies 2017*[3]. The National Cyber Security Centre (NCSC) focuses on addressing such risks.

The potential impact of a cyberattack or accidental failure determines what combination of measures and level of resource are appropriate to address cyber safety and resilience for a particular application. There is a spectrum of needs according to whether the application is safety-critical, for example, or has less stringent safety requirements. There are more stringent requirements for systems that are part of critical national infrastructure. Cyber safety and resilience of industrial sites that are not critical national infrastructure require consideration since there is potential to cause significant harm to workers and to the public if such sites are subject to cyberattack or accidental failure. As systems increasingly interact directly with people's lives, a focus on the cyber safety and resilience of building management systems and consumer products is also required. The physical protection of computing and control equipment is a crucial aspect of cyber safety and resilience, although is not addressed in this report[4].

ROBUST RISK MANAGEMENT PROCESSES HELP ORGANISATIONS PRIORITISE THE 'CYBER HYGIENE' MEASURES REQUIRED ACCORDING TO THEIR BUSINESS NEEDS.

An approach that ensures that components and systems are robust and secure, in proportion to the requirements of the application, might use a combination of regulation and standards alongside robust engineering methods, as is already done for a range of safety-critical applications. These methods help to ensure that hardware, software and systems are high quality and have good security functionality. In less critical applications, there may not be a sufficiently strong business case for such methods, and the effective use of regulation may be more challenging. Furthermore, existing systems such as industrial-based legacy systems may not have been designed with security as a requirement, since they were never intended to connect to the internet; however, once connected, vulnerabilities that reside in individual components or the systems that are created from these components may become exploitable in a cyberattack. For all applications, robust risk management processes help organisations that rely on systems to prioritise the 'cyber hygiene' measures required according to their business needs: a combination of policies and procedures; training and skills development; and technologies that are tailored to the level of risk. Cyber risk management guidance published by NCSC[5] is useful here.

Frameworks that are aligned to industry standards and common practices set out guiding principles for cyber risk management during design, operation and maintenance. Many critical sectors are already developing frameworks and standards, but there is a need to accelerate this process and speed up adoption. The mandatory use of frameworks should be considered for certain critical sectors and applications. Operational frameworks that are risk-based and proportionate are also useful for operators of non-critical industrial control systems[6]. Voluntary frameworks already exist, such as the government's Cyber Essentials[7] scheme and the US *National Institute of Standards and Technology (NIST) Cybersecurity Framework*[8]. These frameworks may need further development to ensure that risks associated with the supply chain are sufficiently addressed[9,10], in addition to internal organisational risks.

The development of an appropriate enabling structure – a combination of regulatory and non-regulatory measures that are suited to the application – would improve practice, while promoting innovation and ensuring safety and resilience. It would need to be developed in the light of the forthcoming European Union (EU) Directive on security of Networks and Information Systems (NIS Directive)[11], which will come into effect before the UK leaves the EU. The Directive will have a major impact on the UK, regardless of Brexit arrangements. Although it will only apply to operators of essential services above a certain size and digital service providers, it is likely to have a wider impact as requirements are passed down the supply chain. Any measures must also work within the existing regulatory context for individual sectors, and the global regulatory context. Cyber challenges cut across international boundaries, and large, multinational companies develop many of the software and hardware solutions. There is a very strong case for linking the best minds internationally to help develop measures to improve practice.

An understanding of the socio-technical aspects of cyber safety and resilience across different classes of user and organisation also informs which measures are appropriate, and how they can be made as effective as possible. The Academy welcomes NCSC's focus on this area and its support for socio-technical cybersecurity research. Socio-technical aspects of security are examined in Section 4.5 of this report and in a joint Academy and PETRAS report, *Internet of Things: realising the potential of a trusted smart world*[12], which is published alongside this report.

While recognising the multidimensional nature of cyber safety and resilience, this report focuses on the engineering approaches that may be appropriate for systems used in critical national infrastructure, or in other applications where the impact of cyberattack or accidental failure is high. It raises issues around supply chain vulnerabilities, regulation and legislation, knowledge and skills, and research. Recommendations in this report are aimed primarily at policymakers in government, NCSC, regulators and national funding bodies. The report also provides information for managers in industrial organisations that design, manufacture, procure, operate or maintain systems or components from both critical and non-critical sectors. Cybersecurity experts and researchers may be interested in non-technical policy issues that the report raises. The report identifies a role for the Royal Academy of Engineering (the Academy) and professional engineering institutions in supporting actions following the recommendations.

The key messages and recommendations are:

1. Organisations need to be more aware of the vulnerabilities in components and other products provided by their supply chain and need to demand that products are 'secure by default[13]'.

The market is not demanding software, hardware and systems with good security functionality and manufacturers are therefore not responding, although there are exceptions in some areas such as fintech or the mobile phone industry[14]. Companies need to better understand the risks of using products or components that have poor levels of security or other weaknesses. Companies should make use of the available tools, such as supply chain security guidance[15], to address the risks. Suppliers need ways of demonstrating that components and products have adequate security functionality – for example, that they are secure by default. One challenge is that SME suppliers may not have the capacity or incentives to address security and create components or products with sufficient security functionality, or they may view security as an additional cost.

Companies must develop the capability to assure the identity and provenance of products and components from their supply chain. In this regard, there is much to learn from safety-critical industries that already have considerable experience in addressing the issues around assuring provenance, such as the nuclear, rail and aerospace industries.

The General Data Protection Regulation (GDPR) and the forthcoming NIS Directive will help to ensure that company boards take security issues more seriously. The NIS Directive applies to certain companies, while GDPR applies to all companies. Companies that fall outside the scope of the NIS Directive may still operate devices or systems that are part of larger interconnected systems, and it is crucial that they have an awareness of security risks in their supply chain and an understanding of how to deal with them. SMEs will benefit from an awareness of security issues as it will enable them to do business with companies that are subject to the NIS Directive. The measures taken should be proportionate to the scale of the risks and clearly documented.

Recommendation 1. Every organisation should understand the cybersecurity risks that its suppliers may present and ensure that proportionate, auditable controls are in place that address the particular risks from each supplier. Existing authoritative guidance should be used as the benchmark for regulatory compliance. Where no suitable guidance exists, regulators, industry associations and other organisations should develop it urgently, based on the generic supply chain guidance from NCSC[16].

2. Stronger mechanisms are needed to ensure that cyber safety and resilience is maintained in all applications – both critical and non-critical – but there is no 'silver bullet'.

Identifying the best combination of levers is challenging and will require different solutions for different sectors and levels of criticality. If regulation is too tight, there is a risk that it restricts innovation; similarly, highly stringent procurement requirements could be challenging for small firms in the supply chain. However, tighter regulation may be more appropriate for critical applications. In safety-critical applications, better application of existing regulation is required. Security is essential in critical applications, so that systems are built right from the bottom up[17], with appropriate conditions on whether products can be connected.

All stakeholder organisations should identify which tools, for example, risk management frameworks, are the most appropriate to reduce the risk of harm, and review the effectiveness of the tools on an ongoing basis. Organisations need to be agile and responsive to changing threats and risks. Principle-based frameworks are emerging in the UK and internationally that should ideally work across international borders. The UK can provide a leadership role, promulgating frameworks it has developed so far, for example for the nuclear sector[18].

Government, industry, academia and regulators should work together on a sector-by-sector basis, addressing different levels of criticality, to debate solutions that improve cyber safety and resilience, while ensuring that innovation and value generation are not adversely affected in proportion to the risk. Each sector needs a process that maps the scale of potential impact of a cyberattack or inadvertent failure against the range of applications, although this is challenging because of the interconnected nature of systems. While a sector focus is useful, it is also important to identify generic approaches to avoid duplication and support multi-sector supply chains. The Academy will support government and industry in tackling these challenges and, as a first step, has convened relevant stakeholders at a workshop to debate the cyber safety and resilience of connected health devices (see Section 5).

Recommendation 2a: There should be a clear owner of the cyber safety and resilience agenda in government, with oversight of sector-specific and common issues, and oversight of where the necessary interactions need to occur between the different sectors and stakeholders. Lead government departments, with the support of NCSC and Centre for the Protection of National Infrastructure (CPNI), should continue to convene the appropriate stakeholders to tackle the cyber safety and resilience of key sectors and levels of criticality, and to create a mutually supportive direction of travel. For some sectors, it may be more appropriate for NCSC to take the lead, while in other sectors where the regulator has deep experience of safety issues, it may be more appropriate for the regulator to take the lead. Ongoing dialogue is needed as threats are evolving over time.

Recommendation 2b: Where sector-specific frameworks already exist, NCSC and relevant government departments should ensure that they are sufficiently robust and are adopted and operationalised across the relevant sector stakeholders. They should identify where further guidance is needed to allow them to be operationalised. Government and industry sectors should adapt and operationalise general frameworks, tailored to their specific requirements and developed to include guidance on supply chain risks where they have not already done so.

Recommendation 2c: Government should encourage the adoption of sector-specific frameworks in both the public and private sectors through procurement, by incorporating the use of frameworks in project specifications.

Recommendation 2d: The Academy greatly welcomes the formation of NCSC and the broadening of its remit to tackle the cyber security of all digital systems utilised by society for civil, commercial or personal purposes. NCSC has a leadership role in a broad area and it is likely that its success will bring new demands, as will a changing landscape. A periodic review of NCSC's structure and capacity would ensure that it is able to address effectively emerging issues in future. The review should consider how cross-cutting issues such as cyber safety are most effectively addressed between the various agencies and lead government departments.

3. Many existing regulations are no longer fit for purpose as systems evolve and the threat level changes. Greater focus is needed on cyber safety and resilience. In future, regulations must integrate safety, security and resilience and protect consumers.

It will be particularly important to adapt regulations to integrate safety, security and resilience in critical sectors that are using increasingly digitalised systems and Internet of Things (IoT), and to ensure that regulations are compatible and useable. Some sectors will need new approaches to regulation, as well as greater collaboration between regulatory bodies,

GOVERNMENT SHOULD ENSURE THAT THE UK MAINTAINS ITS INFLUENCE ON THE DEVELOPMENT OF IMPROVED REGULATION THAT INTEGRATES SAFETY, SECURITY AND RESILIENCE.

cybersecurity agencies and industry. In addition, the existing legislative frameworks needs strengthening, building on existing legislation such as data protection law, cybercrime legislation and product liability law.

The UK must be outward-facing and sensitive to the various international regulatory contexts that vary by sector. It must aim to retain as much influence as possible on the development of regulations and international standards after the UK exits from the EU. It will be important to identify what the UK's niche is and where the UK can be a leader.

Recommendation 3a: Government should ensure that the UK can maintain its influence on the development of improved regulations that integrate safety, security and resilience, particularly in sectors that are important to the UK economy. It should also maintain an influence on the development of international standards. It should review and extend existing safety regulations to take account of cyber safety and resilience. Government, NCSC and regulators need to work with their international counterparts to ensure that international standards are sufficiently robust to help deliver safe and resilient systems.

Recommendation 3b: Government should convene a task force to address how the existing legislative frameworks can be strengthened, including in the areas of product liability and cybercrime. The frameworks should incentivise the production of software, hardware and systems of higher quality, and ensure that accountability lies with those who can make improvements.

Recommendation 3c: Government should focus resources on strengthening cybersecurity expertise in regulators, using part of the budget for the UK's cybersecurity programme. It should consider how regulators can ensure standards and regulations address cyber safety and resilience as part of their duties.

Recommendation 3d: Following the introduction of the NIS Directive in May 2018, government should ensure that expertise and resources are available for individual government departments taking on the role of 'competent authority' on behalf of individual sectors.

4. The UK has world-class expertise in safety-critical systems that should be transferred to other sectors and applications.

The UK has world-class centres of excellence in safety-critical systems and has developed a range of tools and methods to produce and assure high quality software[19]. These include scientific methods such as formal specification and verification, as well as engineering design and development methods, system monitoring, incident investigation, disaster recovery and methods of assurance. There is potential to transfer expertise from the safety-critical software community to other domains if the benefits can be demonstrated and the approaches adapted to the scale and pace demanded by these new application areas. There are emerging examples that demonstrate best practice in one part of the solution, such as in specification, assurance or the use of formal methods. Case studies that illustrate best practice applications of IoT and robust approaches to safety and resilience would allow sharing of best practice, as would sharing learning from problems.

Recommendation 4: Professional engineering institutions, with the support the Academy, should publish case studies to illustrate robust applications of IoT in which cyber safety and resilience have been successfully addressed. This would allow best practice to be disseminated to other sectors and applications. Case studies should identify the technological, business and operational practices that contribute to cyber safety and resilience including, where relevant, the use of safety-critical systems tools and methods, and the use of IoT to monitor safety and security. The case studies should highlight strengths, weaknesses and business benefits of such practices.

5. Methods for assuring complex systems of systems require further research.

Support for the research ecosystem, including academia, SMEs and government agencies, will accelerate the development of solutions for assuring complex systems and inform policy. Research will enable the development of new methods to reduce vulnerabilities, and it will need to deal with the challenge of new vulnerabilities appearing all the time. The need for new methods of assurance arises from the increasing complexity of systems, and from systems beginning to use AI technologies in decision-making.

Policy, as well as emerging frameworks, tools and guidance for different sectors and applications, must be based on the best scientific knowledge available and reflect scientific and commercial realities. Frameworks and tools should be well integrated into engineering processes and not just a box-ticking exercise. The challenges require a multidisciplinary approach. Diffuse research areas such as cybersecurity, IoT, AI, hardware security and tools and methods for software engineering will need support, with strong links to industry and real-world application. An international outlook is also needed, since hardware and software solutions, which are shaped by market forces in combination with international regulation, are dominated by big technology multinationals such as Intel, Samsung, IBM, Cisco, Microsoft and Google.

Recommendation 5a: UKRI and other research funders should target funding towards outstanding challenges and gaps in knowledge around assuring complex systems and improving existing systems and solutions. This must be done in the context of real-world applications and include strategic areas of growth for the UK, including the Grand Challenges identified in the industrial strategy White Paper. Research should build on the UK's world-class research expertise in cybersecurity, safety-critical systems, software engineering, hardware security and AI.

Recommendation 5b: Given the urgency with which improvements are needed, cyber safety and resilience should be considered as a proposal for wave three of the Industrial Strategy Challenge Fund, with funding targeted at challenge-led programmes of research and application. The programmes could involve major manufacturers, SMEs, the Catapults and Innovate UK.

Recommendation 5c: Government funding for new technologies and systems should include requirements to address the cyber safety and resilience issues associated with the technologies and systems.

Recommendation 5d: Outstanding challenges and gaps in knowledge in complex systems should be a focus in the government's Cyber Security Science and Technology Strategy. Key challenges include understanding the long-term risks as systems and businesses evolve, balancing the commercial realities of risk management against the level of risk that society is willing to tolerate for critical national infrastructure, and investigating the resilience that society expects and how to deliver it.

RESEARCH SHOULD BUILD ON THE UK'S WORLD-CLASS RESEARCH EXPERTISE IN CYBER SECURITY, SAFETY-CRITICAL SYSTEMS, SOFTWARE ENGINEERING, HARDWARE SECURITY AND ARTIFICIAL INTELLIGENCE.

A sector-specific focus – connected health devices

Digital health, including the use of connected health devices[20] in both clinical and non-clinical settings, offers opportunities to transform health and social care best practice in the 21st century, creating economic and social benefits.

However, there are many cybersecurity risks in the healthcare domain, ranging from ransomware attacks that cause disruption and affect the delivery of care[21], to data breaches from malicious or inadvertent action[22], which risk the privacy and integrity of patient data. Cyberattacks on connected health devices are increasingly a concern as they could have severe, or even life-threatening, consequences on patient safety. Ever greater numbers of health devices have been identified as being at risk in recent years[23]. The rapid growth in consumer, wearable and mobile technologies used for health and wellbeing brings additional risks with it[24]. Although the risks associated with connected health devices are growing, there is still a lack of awareness in the sector of how to manage them, or even that they exist. Much of the focus is on the secure storage of patient data, which is distinct from the considerations for interconnected and embedded medical electronic systems. Many other sectors are more advanced in terms of awareness, governance and resource. For these reasons, the Academy chose connected health devices to illustrate the general principles discussed earlier in the report.

Key messages and recommendations:

The health sector and other sectors can learn from each other in developing an approach to creating high quality devices and systems, and to other measures such as risk management. For example, there are similarities between connected health devices and industrial control systems, although the difference in potential impacts of a cyberattack will necessitate differing responses to address risks. In particular, in the health sector, a large number of people may have access to devices, and there may be direct impacts on patient safety if the operation of devices is compromised. Related applications, such as smart homes and assisted living, may in turn be able to learn from the health sector. As with other sectors, there is a spectrum of potential impacts depending on the application, from wellness monitors to critical life-support systems. The resources required for risk mitigation depend on how the attack might scale and how the impacts might scale as a result of interdependencies. However, there is little robust evidence or quantification of the current security risks and potential impacts in the NHS for connected health devices, or more broadly, upon which to base solutions. There is a need to start measuring the problem before solutions can be identified.

In the EU, there is a regulatory framework for medical devices that aims to ensure that devices are safe for patients, but it has not fully considered the possible impacts of poor cybersecurity on patient safety or privacy. Furthermore, there is not a consistent international regulatory approach to cybersecurity as the US regulatory regime deals with cybersecurity much more explicitly. It is, however, less robust on telecoms standards and privacy, which has implications for telehealth and telecare. Incompatible regulation between different jurisdictions has important implications for the international supply chain and international trade.

As with other sectors, those procuring health devices need a greater awareness of supply chain risks, and need to demand products with adequate security functionality. There is also a need for good cyber-hygiene practices that are balanced with the level of risk, healthcare priorities and practical constraints on healthcare professionals, patients and others.

It will also be vital to develop regulation for medical devices that blends safety, security and resilience, alongside other measures to improve practice. Non-critical uses of IoT in the health sector may require a less stringent approach. The existing regulatory framework provides a means of getting other measures, such as standards or cyber labels, into the field, which would help consumers and healthcare providers to demand good security from manufacturers. However, the risks of creating unintended consequences from such schemes must be addressed. Standards and cyber labels should be considered alongside risk-based approaches.

The report presents the recommendations for the health sector below, which have been developed from the general recommendations presented earlier. They use the same numbering to clarify how the two sets of recommendations are linked. While many of the recommendations apply to all sectors, the size and complexity of the NHS and the broader health ecosystem makes their implementation a particular challenge. The report discusses additional aspects that are specific to the health sector in Section 5.

EVERY HEALTH ORGANISATION SHOULD UNDERSTAND THE CYBER SECURITY RISKS THAT ITS SUPPLIERS MAY PRESENT AND ENSURE THAT PROPORTIONATE, AUDITABLE CONTROLS ARE IN PLACE THAT ADDRESS THE PARTICULAR RISKS FROM EACH SUPPLIER.

Recommendations:

1. Health providers need to be more aware of the vulnerabilities that exist in components and other products provided by their supply chain and need to demand that products are 'secure by default'.

Recommendation 1: Every health provider should understand the cybersecurity risks that its suppliers may present and ensure that proportionate, auditable controls are in place that address the particular risks from each supplier. Authoritative guidance should be developed and used as the benchmark for regulatory compliance. Organisations including the Medicines and Healthcare products Regulatory Agency (MHRA), NHS Digital and health industry associations should work together to develop guidance based on the generic supply chain guidance from NCSC[25].

2. Stronger mechanisms are urgently needed to ensure that cyber safety and resilience is maintained in health applications but there is no 'silver bullet'.

Recommendation 2a: NCSC, in conjunction with the Department of Health and Social Care, NHS Digital[26] and MHRA, should continue to convene the appropriate stakeholders to tackle the cyber safety and resilience of the health sector, and to create a mutually supportive direction of travel. In addition, there is a pressing need to clarify roles and responsibilities for cyber safety and resilience within the NHS governance structure at both local and national level.

Recommendation 2b: Working with the medical device industry, the Department of Health and Social Care and NCSC should adapt and operationalise a general cybersecurity risk-management framework, tailored to the health sector's specific requirements.

Recommendation 2c: The Department of Health and Social Care and NHS organisations should encourage the adoption of the framework through procurement, by incorporating the use of the framework in project specifications.

3. Medical device regulations will no longer be fit for purpose as systems evolve and the threat level changes. Greater focus is needed on cyber safety and resilience. In future, regulations must integrate safety, security and resilience and protect consumers.

Recommendation 3a: Government should ensure that the UK maintains its influence on the development of improved medical device regulations that integrate safety, security and resilience, and link to data protection regulation. It should also maintain influence on the development of international standards. It should review and extend existing safety regulations to better take account of issues associated with cyber safety and resilience. Government, NCSC and MHRA should work with their international counterparts to ensure that international standards are sufficiently robust to help deliver cybersecurity policies.

Recommendation 3b: FDA and MHRA should be part of a task force convened by government to consider how the existing legislative frameworks can be strengthened, including in the areas of product liability and cybercrime. The frameworks should incentivise the production of software, hardware and systems of higher quality, and to ensure that accountability lies with those who can make improvements.

Recommendation 3c: Government should focus resources on strengthening cybersecurity expertise in MHRA, using part of the budget for the UK's cybersecurity programme. It should consider how MHRA can ensure standards and regulations address cyber safety and resilience as part of its duties.

Recommendation 3d: Following the introduction of the NIS Directive in May 2018, government should ensure that expertise and resources are available for the Department of Health and Social Care and NHS Digital[27] in taking on the functions of 'competent authority'. Sufficient resources will also need to be provided to the relevant bodies in Wales, Scotland and Northern Ireland.

4. The UK has world-class expertise in safety-critical systems that should be transferred to connected health devices and systems.

Recommendation 4: Professional engineering institutions, with the support of the Academy and health organisations, should publish case studies of relevance to the health sector, which illustrate robust applications of IoT where cyber safety and resilience have been successfully addressed. Case studies should investigate technological, business and operational practices that contribute to cyber safety and resilience including, the use of safety-critical systems tools and methods where relevant, and the use of IoT to monitor safety and security. The case studies should highlight the strengths and weaknesses of such applications, including business benefits to the NHS and other healthcare providers. Similarly, case studies of robust applications in the NHS should be identified and disseminated to other disciplines.

5. Methods for assuring complex systems of systems require further research.

Recommendation 5a: UKRI and other research funders should target funding towards outstanding challenges and gaps in knowledge around assuring complex health systems and connected health devices, and improving existing health systems. This must be done in the context of real-world health applications, including the Grand Challenge identified in the industrial strategy White Paper: 'harness the power of innovation to help meet the needs of an ageing society'. Of relevance to this is the need for research on the assurance of systems that use AI for decision-making. It is critical that research is undertaken with the major suppliers of medical devices as they provide the solutions.

Recommendation 5b: Outstanding challenges and gaps in knowledge in complex health systems should be a focus in the government's Cyber Security Science and Technology Strategy. The Academy welcomes the focus on medical devices in the strategy.

1. Introduction

The integration of physical and digital systems creates many opportunities for improved performance and innovation in the supporting systems of a modern economy, generating economic value and creating social and environmental benefits. In *Connecting data: driving productivity and innovation*[28], the Academy and the Institution of Engineering and Technology (IET) illustrated the myriad opportunities that such systems and their underpinning technologies, such as data analytics, advanced connectivity and IoT, will provide across sectors of the economy, including advanced manufacturing, built environment, energy, transport, health, aerospace, defence and insurance. It showed how organisations and sectors will be able to improve products and processes, and innovate, leading to an improvement in the UK's productivity. Others have estimated that big data analytics and the Internet of Things (IoT) combined could add £322 billion to the UK economy between 2015 to 2020[29].

However, there is a growing awareness of the risks associated with the increasingly complex and interdependent systems of systems that are being created as a result of the integration of digital and physical systems[30,31,32]. Such systems are at risk of unanticipated emergent behaviour, including cascades of failure. Vulnerabilities may be pre-existing, may arise from the digital technologies themselves, or from the creation of new interdependencies between digital technologies and the physical system[33]. For example, the operation of digital communications infrastructure such as mobile phone networks and the internet are entirely dependent on electricity[34], and in turn the operation of industrial control systems used in electricity generation plants are increasingly dependent on digital communications and other digital technologies. As cars become more connected, self-driving mechanisms and entertainment systems may introduce vulnerabilities[35]. Building management systems are becoming increasingly intelligent and connected to the internet, so that heating and fire alarm systems may be more at risk of sabotage[36] or failure.

Vulnerabilities in the digital technologies arise from software, hardware and systems that are not sufficiently well-designed in terms of security functionality as well as other aspects of performance[37]. The security vulnerabilities recently discovered in Intel, Arm and AMD processors were caused by hardware-level weaknesses[38,39], while software defects have caused system failures, such as in cars and aircraft[40], that put people at risk of harm[41].

Both deliberate and non-deliberate[42] threats put systems at risk: deliberate threats include cyberattacks[43], while non-deliberate threats include the failure or malfunction of components and systems, natural hazards and human error. For example, flooding in Lancaster in 2015 caused an electricity black-out, with the resulting failure of various related systems[44]. The failure of the baggage-handling system at Heathrow in 2017 was initiated by a power outage in a data centre, followed by damage to equipment when power was reinstated in an uncontrolled way. This then resulted in massive disruption to passengers and costs to British Airways[45]. The evolution in the scale and nature of deliberate threats over recent years, and the increasing complexity and interconnection of digital systems, has resulted in a greater number of vulnerabilities that can be targeted. More traditional threats – for example, external drives such as USB sticks – are also still present.

While it may be impossible to design systems that are entirely secure or free from the risk of failure, appropriate levels of cyber resilience and safety are necessary. Cyber safety refers to the ability of systems to maintain adequate levels of safety during operation, including in the event of a cyberattack or accidental event, protecting life and property. Current approaches to safety need to be extended to address malicious, as well as accidental, threats. Safety is a desirable property of a system during normal operation, whereas resilience describes the capacity of a system to handle disruptions to operation. One aspect of cyber resilience is the ability to 'prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world'[46]. However, in addition to attacks via the internet, there

HIGHER LEVELS OF CYBER SAFETY AND RESILIENCE ARE NEEDED FOR SYSTEMS THAT ARE PART OF CRITICAL NATIONAL INFRASTRUCTURE, SUCH AS THE ELECTRICITY GRID AND THE TRANSPORT SYSTEM, OR SAFETY-CRITICAL SYSTEMS, SUCH AS NUCLEAR POWER STATIONS AND AIRCRAFT.

may be other ways of carrying out attacks, such as by using radio transmitters or lasers[47]. Addressing broader issues such as supply chain risks and people-centred aspects will contribute to ensuring cyber resilience. Resilience thinking needs to be embedded more deeply into systems[48].

Higher levels of cyber safety and resilience are needed for systems that are part of critical national infrastructure, such as the electricity grid and the transport system, or safety-critical systems, such as nuclear power stations and aircraft. Indeed, as systems become more interdependent, elements that were not previously considered critical increasingly become so, and the consequences of failure in one part of a system could have more far-reaching consequences. Such systems of systems need new approaches to cyber safety and resilience. Cyber safety and resilience of industrial sites that are not critical national infrastructure should also be addressed since there is potential to cause significant harm to workers and the public they are subject to cyberattack or accidental failure. As integrated physical and digital systems increasingly interact directly with people's lives, a focus on the cyber safety and resilience of consumer products such as autonomous vehicles and medical devices is also required.

2. The challenges for critical and non-critical infrastructure

2.1 What systems are being created?

This report focuses on the complex, interconnected systems that result from integrating physical and digital systems. It covers the important systems that support the modern economy, including critical national infrastructure[49]. It also includes discussion on IoT[50], which both industrial and consumer sectors are increasingly adopting, increasing interconnectivity in the future.

Industrial control systems are used in numerous applications including transportation, electricity and gas distribution, water treatment, chemical processes, oil refining and other manufacturing processes. For example, highways use industrial control systems to control and monitor tunnel ventilation[51] or in moving bridge systems. Industrial control systems are used in aviation and maritime applications. They are also used in electricity generation, transmission and distribution, and infrastructure assets. In turn, they are dependent on digital communications infrastructure that may be used to connect remote field sites, for example[52]. They may be part of critical national infrastructure. However, there are also many industrial sites that are not critical national infrastructure but are in critical national infrastructure sectors such as chemicals and energy. They have the potential to cause significant harm to workers and the public if there is a cyberattack or accidental failure[53], and should also be a focus in the National Cyber Security Strategy.

Industrial control systems may comprise embedded computing devices that have vulnerabilities, such as remote terminal units[54] or programmable logic controllers[55]. They may also contain sensors and actuators that provide real-time feedback for automation or optimisation. The adoption of IoT in industrial applications will increase the number of devices and the degree of interconnectivity in the future, with multiple benefits[56] but also greater risks. The risks of connecting industrial control systems are well documented, along with examples of cyberattacks on industrial equipment[57,58]. For example, during the Wannacry attack in 2017, the car manufacturers Renault and Nissan[59] were affected, even though the malware was not targeted specifically at industrial control systems.

Cyber safety and resilience of networked building management systems also requires consideration. Building management systems are increasingly interconnected and a cyberattack or inadvertent failure may impact on safety and security, as well as business continuity through disruption to heating or chilling systems, access control and surveillance systems, fire systems, power supply, lift systems and lighting.

IoT enables enhanced real-time control, or can be used alongside data analytics to inform actions. The technology could potentially underpin a range of 'smart' applications across many sectors including e-health, smart homes, cities and infrastructure, connected cars and autonomous vehicles. If there was a step-change in adoption, the economic, social and environmental benefits that could result are widely recognised, alongside the risks[60,61,62,63,64]. Benefits include improved health and wellbeing, better-informed consumers, more efficient services, reduction of traffic congestion and improvements in the use of energy and water. For example, the introduction of smart meters will empower consumers to reduce their energy usage, while informing the planning and operation of the electricity grid. Connected cars will contribute to improved road safety, more effective vehicle maintenance and allow drivers to plan journeys better. Technologies including IoT can help to improve the way the UK operates infrastructure, maintains existing assets, and enhances the capacity and resilience of its networks[65]. As IoT technologies are adopted, there will be more devices and more interconnectivity in applications such as the energy and transport systems. The scale of adoption is expected to be huge, with tens of billions of IoT devices connected to the internet by 2020[66]. However, following the distributed denial-

of-service attack through insecure devices on a major provider of internet infrastructure in October 2016[67], awareness of cybersecurity risks associated with IoT is growing .

2.2 What vulnerabilities exist?

Poor quality components and the way that they are integrated into communications networks compromise the cyber safety and resilience of systems. Cheap, unsophisticated sensors with little or no security are prevalent, making systems vulnerable to inaccuracies in sensor readings, delayed feedback or cyberattack. The trustworthiness of the software behind these devices is also of concern. As devices are low-power, applications with small footprints[68] are being written but it is hard to know whether they are trustworthy, resilient or tamper-proof. Devices have much shorter lifecycles than the infrastructure systems in which they are embedded and replacing them during the lifecycle of the infrastructure should be considered. Battery-powered devices are susceptible to power failure with ensuing implications if the system has not been designed with that in mind. Components are often commercial off-the-shelf (COTS) for ease and cheapness, and it is possible that design errors are introduced when they are integrated into systems if component information is limited.

The supply chain is now considered to be susceptible to a range of hardware-based threats, particularly in relation to consumer products. Counterfeiting and the emerging threat of hardware Trojans may introduce modifications to hardware. With the globalisation of supply chains, the design and manufacture of today's electronic devices is now distributed worldwide, through overseas foundries, third party intellectual property (IP) and third party test facilities. Many different untrusted entities may be involved in the design and assembly phases and it is becoming increasingly difficult to ensure the integrity and authenticity of devices. Maintaining confidence in security and the supply chain throughout the development process and the product lifecycle is one of the main research challenges being investigated under the new Research Institute in Secure Hardware and Embedded Systems[69].

Both corporate information technology (IT) systems and operational technology[70] (OT) systems are at risk of cyberattack. Cyber security is a particular challenge in organisations where both exist and are integrated, as they have had very different technological and functional characteristics[71] in the past. Legacy industrial control systems were designed to be closed, but become open once connected to the internet and face threats that they were not designed for. It is questionable whether security patches (updates to improve the software) are appropriate for these systems, and it is also possible that new faults could be introduced that lead to unanticipated behaviour.

Where wireless technologies replace wired technologies, they become vulnerable to jamming and interference. Communications networks are being created without sufficient concern for how they will operate in an open state. Greater understanding of how to identify and secure weak links is needed. A major concern is the potential for damage or disruption to essential services from a cyberattack.

IoT is a communications infrastructure that may be a target for attack in its own right, but it also is bearer or store for data. The security of data at rest or in transit is an important consideration. Security is needed to protect its integrity and availability and to reduce the risk that it may be used for hostile purposes.

CYBER ATTACKS THAT COMPROMISE DATA INTEGRITY, SUCH AS CONSISTENT SPOOFING OF DATA REPORTED BY SENSORS, CAN REMAIN UNDETECTED FOR A LONG TIME YET HAVE POTENTIALLY SEVERE CONSEQUENCES.

The diversity of classes of hardware devices and software systems that are emerging, and the speed at which the middleware[72] on which they run is changing, means that it is hard for experts to identify how future use cases will emerge. Furthermore, the systems themselves are changing as a result of new connections, new or updated software, or the systems changing from their originally intended use.

Systems are also vulnerable as a consequence of poor cyber hygiene[73,74,75]. Organisations can improve cyber hygiene by strengthening the activities used to keep the organisation, or a particular function within the organisation, safe and secure. For example, they might include raising awareness of supply chain risks, improving system assurance and patching[76] processes, or planning how to recover if there is an incident. A planned, flexible human response is often the first step in any recovery, regardless of the technical nature of the incident. A strategy that could potentially mitigate many cyber incidents[77] is patch management, which should be an important consideration. Using principles from human-factors engineering in the design and operation of software, hardware and systems is also an important aspect.

New risks are also emerging as systems become increasingly data-driven, with decisions often based entirely on the data held by systems. Thinking about how data (as opposed to software or hardware) should be managed, controlled and processed in a safety-related context may also be of use to applications that are not safety critical. Guidance produced by the Safety Critical Systems Club[78] focuses on how organisations might identify, analyse, evaluate and treat data-related risks, thus reducing the likelihood of data-related issues causing harm in the future. One such risk is that data integrity is compromised, either inadvertently or by a cyberattack. Cyberattacks that compromise data integrity, such as consistent spoofing of data reported by sensors, can remain undetected for a long time yet have potentially severe consequences. Technical approaches to identity and access management provide a form of data-centric security, helping to maintain privacy or protect the integrity of data[79].

3. Policy context

3.1 Cybersecurity – a key component of UK national security

UK strategies for national security and cybersecurity

The UK's *National Security Strategy 2015*[80] identifies 'the impact of technology, especially cyber threats; and wider technological developments' as one of four main challenges that will drive UK security priorities over the coming decade. It pledges to ensure that the UK remains a world leader in cybersecurity. The *National Security Risk Assessment 2015*[81] includes the disruption of critical national infrastructure as it becomes more networked and dependent on technology as a Tier One risk. This includes networks and data held overseas as well as hostile cyberattacks or major cyber crimes that do not involve critical national infrastructure. The National Security Risk Assessment points out that cyber risks underpin many of the other risks the UK faces.

Between 2011 and 2016, the UK government invested £860 million in a National Cyber Security Programme that improved the cyber resilience of national critical infrastructure, including the development of plans to manage cyber risk with infrastructure owners and operators[82].

The *National Cyber Security Strategy 2016 to 2021*[83] scales up the activities required to ensure the UK is resilient and secure, recognising that IoT and industrial control processes in critical systems are increasingly at risk of attack. The strategy aims to address the root causes of vulnerabilities, as well as reducing the ability of malicious actors to attack. The government has increased investment to £1.9 billion over a five-year period to deliver the strategy. The government is focusing its efforts on other key areas including cybersecurity skills[84] and strengthening the UK's cybersecurity industry to support economic growth[85,86]. Government has also put significant investment into support for innovation centres, such as the GCHQ Cyber Accelerator[87] and the forthcoming cybersecurity innovation centre in London[88].

Fourteen UK universities have been recognised as academic centres of excellence in cybersecurity research[89], and research institutes have been created in strategically important areas[90], including the trustworthiness of industrial control systems[91].

In November 2017, government published its *Interim Cyber Security Science and Technology Strategy*[92] that sets out how it will develop a strategy to ensure the UK has the capability and expertise in cybersecurity science and technology to meet security needs and inform policymaking. All aspects of policymaking will be considered, including research, growth and innovation, creating secure and trusted systems, public awareness of cybersecurity and cyber skills and expertise. The interim strategy establishes the National Cyber Security Centre (NCSC) as the single authoritative UK government voice for cybersecurity and technology. The report puts forward the key technology trends that will affect the cybersecurity of the UK in future, including IoT and smart cities, data and information, automation, machine learning and AI, and human computer interaction. It also recognises the opportunity for the UK to be a world leader, capitalising on expertise in cybersecurity and using security as a competitive advantage.

Cybersecurity and regulation

In July 2016, as a part of the Digital Single Market, the UK adopted the EU Directive on security of Networks and Information Systems (NIS Directive)[93], which applies to operators of essential services and digital services providers. It aims to ensure that cybersecurity capabilities are at the same level of development in all the EU member states and that exchanges of information and cooperation are efficient, including at cross-border level. Member states will need to incorporate this directive into their laws and, since the UK will not have left the EU by 2018, it will need to be applied in the UK. Nevertheless, as the UK will continue to trade with the EU after 2019, closely comparable cybersecurity laws will be necessary to avoid barriers to trade. In January 2018, NCSC published guidance on the Directive as did the European Commission in September 2017[94].

In December 2016, the UK government said that it will improve cyber-risk management in the wider economy through its implementation of the forthcoming GDPR[95]. The Data Protection Bill 2017, which will implement GDPR standards across all general data processing, was announced in June 2017 and introduced to the House of Lords in September 2017[96]. The government will not pursue further general cybersecurity regulation for the wider economy over and above the GDPR, although this could be reviewed in future. The government is separately considering whether additional regulation might be necessary for critical sectors, including in the context of the NIS Directive as well as wider national infrastructure considerations[97]. The report discusses existing regulation around safety and resilience in more detail in Section 3.2.

Cybersecurity and industrial strategy

Alongside the government's cybersecurity strategy, other opportunities to strengthen the UK's capabilities in cybersecurity are present. In November 2017, the government published its industrial strategy White Paper[98], which recognises the importance of innovation and the need to develop and exploit underpinning digital technologies. 'AI and the data-driven economy' is one of four 'Grand Challenges' announced in the White Paper that the Industrial Strategy Challenge Fund will support, matched by commercial investment. Digital technologies will also support the success of other Grand Challenges, such as clean growth, mobility and an ageing society, by enabling smart systems and greater resource efficiency, underpinning new business models in transport and innovations in health and care. Such technologies will also be important for increasing the productivity of sectors, supported by sector deals in life sciences, construction and the automotive sector.

The industrial strategy White Paper pledges to build on the UK's strengths in cybersecurity and to support rapid adoption of AI technologies at scale. The cybersecurity sector is one of six priority business sectors that the new government Office for AI will initially work with. The White Paper also recognises the need to create infrastructure systems that are both resilient and efficient, by setting high standards in cyber and climate change resilience for UK infrastructure projects.

National Cyber Security Centre (NCSC)

To help deliver the cybersecurity strategy, NCSC has brought together stakeholders from industry, academia and government and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI), CESG[99], the Centre for Cyber Assessment and CERT UK[100]. It provides an authoritative voice on information security in the UK, aiming to transform how the UK tackles cybersecurity issues[101]. The NCSC's remit includes ensuring the online safety of individuals, public and private sector organisations, and critical national infrastructure of the UK. In its annual report published in October 2017 (its first anniversary), the NCSC explains its role in supporting owners, operators and suppliers in the critical national infrastructure sector, in partnership

SECURITY- AND SAFETY-FOCUSED PRINCIPLES AND GUIDANCE ARE EMERGING IN THE UK AND ABROAD FOR THE AUTOMOTIVE SECTOR AS WELL AS OTHER SAFETY-RELATED SECTORS.

with lead government departments and the Centre for the Protection of National Infrastructure. The report also describes how NCSC has taken steps to widen its remit to all sectors of the economy, including the voluntary sector, SMEs and educational institutions. An important part of its role is in issuing guidance if a new vulnerability or form of attack emerges.

Cybersecurity frameworks and guidance

NCSC's Cyber Essentials scheme is a voluntary scheme that provides guidance to all organisations on the basic technical controls for mitigating the most common threats, and allows organisations to demonstrate they comply through certification[102]. The scheme targets enterprise IT and is based around a simple risk scenario[103]. NCSC publishes guidance that is generally applicable, but also relevant to national critical infrastructure. This includes, for example, guidance on cybersecurity in operational technology environments[104] and risk management[105]. Guidance specifically aimed at protecting critical infrastructure also exists, for example, on security for industrial control systems[106].

European and US government agencies are also producing guidance for critical national infrastructure[107,108,109]. In the US, much of the guidance builds on the *NIST Cybersecurity Framework* for critical infrastructure[110], which various US sectors have adapted to suit their specific requirements and increasingly adopted. The financial services sector in the UK has reportedly also adopted it. A number of tools exist to help organisations implement the framework such as the Cybersecurity Capability Maturity Model (C2M2)[111].

In the automotive sector, security- and safety-focused principles and guidance are emerging in the UK and abroad, as well as other safety-related sectors. These include principles for connected and autonomous vehicles[112,113,114] and the rail[115,116] and nuclear[117] sectors.

Cybersecurity testing

Cybersecurity testing is a tool that informs risk management. It evaluates the security of a system through an authorised simulated attack. It should be noted that cybersecurity testing cannot provide full assurance that a system is secure, because some vulnerabilities may not have been identified. In 2014, UK financial authorities introduced CBEST, an intelligence-led testing framework for sharing detailed threat intelligence and delivering cybersecurity tests and benchmarking for UK financial services providers[118]. Financial services have led the way in ensuring that they are resilient to cyberattack, and other sectors such as telecoms are likely to follow suit.

The European Commission's approach to cybersecurity

In September 2017, the European Commission published its proposed approach to improving cybersecurity in the EU[119], which focuses on building cyber-resilience and strategic autonomy with a strong Single Market, advances in technological capability and an increase in skilled experts. It includes a proposal to set up an EU cybersecurity certification framework that would cover products, services and/or systems, and that adapts the level of assurance depending on whether it applies to critical infrastructure or consumer devices. The framework's schemes are voluntary and would not create any immediate regulatory obligations on vendors or service providers. The proposal recognises the need for specific sectors to develop their own approach, with general cybersecurity strategies complemented by sector-specific strategies. The Commission is also examining implications of liability raised by new digital technologies as part of the proposal, and this work is due to conclude in June 2018.

US bill to secure IoT devices

In the US, a new bill has been introduced that aims to better secure IoT devices and protect security researchers who attempt to find vulnerabilities in devices[120]. Manufacturers that supply the US government with connected devices will need to comply with industry-wide security practices through the Internet of Things Cybersecurity Improvement Act 2017[121].

3.2 Cyber safety and resilience – the legal and regulatory environment

3.2.1 Cyber safety

Rapid advances in technologies and changes in the way that systems are created and networked mean that the legal and regulatory environment has not always kept up. It is worth questioning whether traditional legal and regulatory principles still work. In particular, do they need to change to ensure that levels of cyber safety are adequate for increasingly complex and interdependent systems of systems?

Existing regulations will need updating. Currently, certain manufactured products have specific safety regulations, for example, medical devices, toys and electrical products must have a CE mark to demonstrate that they meet safety requirements set out in relevant European Directives. However, safety regulations do not

AWARENESS OF THE IMPORTANCE OF RESILIENCE IS INCREASING, AND OF THE FAR-REACHING IMPACT OF FAILURE IN ONE SYSTEM CAUSED BY INTERDEPENDENCIES BETWEEN DIFFERENT SYSTEMS.

need products to be secure by default. For safety-critical systems, regulations require a 'safety case'[122], which is evidence that the system is safe, and that appropriate safety assessment and risk management procedures are in place. These are required in sectors such as commercial aviation, automotive, defence, nuclear, petrochemical and railways, and provide a means of dealing with the technical complexity of the systems under scrutiny[123]. This report discusses the challenges of applying safety case approaches to systems that are changing over time in Section 4.3.

There are challenges around risk management, particularly in relation to the use of 'as low as reasonably practicable' (ALARP)[124]. The interface between judgements of ALARP and cyber risk assessments needs to be addressed. Assessing the risk necessary for ALARP decisions in terms of consequence and likelihood is problematic as it involves judgements of the likelihood of attack. There are unresolved questions such as: can a risk statement be conditional on threat assumptions? is a government liable for the safety risks if it provides threat intelligence? and, how can the licensee or responsible party reasonably assess such statements? Any solution must have regulatory, legal and technical elements.

Vulnerabilities in poor quality software, hardware and systems often contribute to safety hazards from hacking, malware or other types of threat[125]. However, the existing law does not incentivise suppliers to ensure that their products are always fit for purpose. Further debate is required on the need for legislative changes to improve the quality and safety of these types of product, for example on whether product liability law needs overhaul[126]. This issue is discussed further in Section 4.4.

3.2.2 Cyber resilience

Awareness of the importance of resilience is increasing. Failure in one system caused by interdependencies between different systems can have far reaching impacts[127]. A system's ability to operate may be compromised if there is a loss of internet connection, for example, and fall-backs and risk management procedures will be needed to reduce the risk of the event occurring. Future approaches to cyber resilience will need to respond to new threats and vulnerabilities. Cyber threat changes the requirements for resilience substantially, because it can no longer be assumed that major incidents will occur independently or that the response system will not also be attacked. It may be desirable to combine redundancy with diversity of systems, because if identical systems are used to provide redundancy then they could be compromised through the same attack.

These approaches will also need to define the levels of cyber resilience that society and the economy demands from these systems.

At a national level, the UK government has overall responsibility for the national response to civil emergencies, identifying risks, and planning for and responding to them[128]. The National Risk Assessment (NRA) identifies relevant risks, and sector resilience plans[129] are used to set out the resilience of critical sectors and create a programme of measures to improve resilience where necessary. The NRA now has a dedicated cyber sub-group and is starting to systematically address the issues across all government departments. While there are accepted processes for establishing what levels of safety are tolerable, and how it varies across sectors, the appropriate level of resilience society implicitly expects or is prepared to pay for needs to be considered. Interdependencies between sectors make this a challenging cross-sector problem.

Each regulated sector has a lead government department with overall responsibility for its resilience. Other departments are also involved in resilience to varying degrees, such as the devolved national governments, Home Office, Cabinet Office, Ministry of Housing, Communities and Local Government (MHCLG), and the CPNI[130]. Regulators have duties related to resilience, and the detail and maturity of these varies greatly, as does the range of powers available to discharge them, and no specific cross-sector resilience duties exist[131]. The electricity sector's work on resilience is probably the most mature and has been a subject for inquiry by the House of Lords[132]. For example, as part of its resilience planning, the sector has developed procedures to recover from a total or partial shutdown of the transmission system[133].

In some instances, EU regulatory frameworks have required higher levels of cyber resilience. For example, in the telecommunications industry, the framework governing communications regulation has evolved from a focus on market supply and competition to ensuring providers are taking appropriate measures to manage the security and resilience of their networks[134]. This requirement is legislated in the UK through the Communications Act 2003. The proposed EU NIS Directive addresses the key role that electronic communication and computer networks now play in all infrastructure sectors and may require regulators in critical sectors to take on additional duties around cyber resilience[135]. Companies in these sectors may also be required to assess the risks they face and adopt appropriate and proportionate measures to ensure cyber resilience[136].

4. Addressing the challenges

4.1 Supply chain vulnerabilities

Organisations need to be more aware of the vulnerabilities in components and other products provided by their supply chain and need to demand that products are 'secure by default'.

The number of successful cyberattacks resulting in data breaches[137] or impacts on industrial equipment[138] is rising, but despite this evidence, many company boards are not doing enough to improve cybersecurity. Companies need to be more aware of possible vulnerabilities in their supply chain and to understand the implications of using individual components that may have poor levels of cybersecurity or are at risk of failure. They need to demand that products are 'secure by default', and suppliers need to demonstrate that components and products have adequate security functionality. Companies can help to manage supply chain security risks using guidance such as that published by CPNI[139].

Companies must develop the ability to assure the identity and provenance of products and components from their supply chain. There is potential to learn from safety-critical industries that already assure provenance as standard practice, for example, the rail industry has developed supplier assurance programmes that benefit both suppliers and industry[140]. There is also potential to use emerging technologies such as distributed ledgers to help ensure transparency and traceability in supply chains, and to combat counterfeiting[141].

In the case of industrial control systems, the ICT and control engineering communities are largely distinct, each with its own discipline, culture and approach, and with conflicting standards that become more apparent once systems are interconnected. This creates a barrier to improving practice.

The market is currently not solving the problem by itself, although some companies are taking action when incentives to improve cybersecurity are sufficiently aligned with business objectives. Firms such as Apple and Google have their own ecosystem of cybersecurity activities to ensure that their products are secure[142]. Some companies are introducing formal methods for software development, that improve the quality of software and reduce vulnerabilities caused by software defects. For example, Siemens has used formal methods for the Paris Metro and other projects, while Microsoft and Facebook have introduced them to improve security, speed up development and reduce costs[143]. Some sectors such as fintech have more robust security practices. Certain engineering consultancies are increasingly concerned about achieving the same level of quality of software as other engineering activities, particularly those with a strong ethos as learning organisations. Initiatives similar to the Building Security In Maturity Model (BSIMM)[144] could be developed for embedded systems and infrastructure. However other industries may need additional incentives to address cybersecurity with the same commitment.

Supply chain issues should be considered as part of the industrial strategy. The UK might need to ensure self-sufficiency in some component and system sectors (both hardware and software) to enable critical systems to be assured as cybersecure to a higher integrity than can be achieved by incorporating components sourced from abroad. This approach would also require that the toolchain for software (linked software development tools) or the manufacturing chain for hardware was in the UK.

The General Data Protection Regulation (GDPR) and the forthcoming NIS Directive are welcome as they will help to ensure that company boards take cybersecurity issues more seriously. Companies will be obliged to push security requirements down their supply chain. However, not all companies fall under the scope of the NIS Directive.

Recommendation 1

Every organisation should understand the cybersecurity risks that its suppliers may present and ensure that proportionate, auditable controls are in place that address the particular risks from each supplier. Existing authoritative guidance should be used as the benchmark for regulatory compliance. Where no suitable guidance exists, regulators, industry associations and other organisations should develop it urgently, based on the generic supply chain guidance from NCSC[145].

4.2 What is the right combination of mechanisms?

Stronger mechanisms are needed to ensure that cyber safety and resilience is maintained in all applications – both critical and non-critical – but there is no 'silver bullet'.

4.2.1 Government's role

Government needs to consider the full range of possible levers for improving cyber safety and resilience, including regulatory and non-regulatory measures. These include procurement, auditing, education and information-sharing, and insurance[146], as well as regulation. However, there is no 'silver bullet' as the challenges are not homogeneous across different sectors and levels of criticality. While there may be common principles, different approaches will need to consider institutional bodies and existing regulatory frameworks.

If regulation is too tight, there is a risk that investors will shift their focus to other countries. Similarly, highly stringent procurement requirements could be challenging for small firms in the supply chain. Conversely, if manufacturers view the UK's regulatory system as strong but realistic, they will want their systems accepted and assessed in the UK. This is because they will seek to align with the strongest requirements if it helps them comply with requirements from markets elsewhere in the world. This is illustrated in Section 5 in the context of the health sector: many countries accept medical devices if certified in Europe or the US. The degree of advice and support given to manufacturers to achieve compliance is an important factor that affects the success of regulation.

A loss of trust in systems that have poor levels of cyber safety and resilience could have a damaging impact. It requires an urgent improvement in practice, particularly if the UK is to realise the economic and social benefits from innovative technologies used in such systems.

Other industries comply with exacting regulation, which has not affected their competitiveness. For example, the children's toy industry and the electrical product industry are subject to strict liability in relation to the safety of their products. Better regulatory impact analysis is required to understand the impact of regulation on innovation and value generation. The UK should be outward facing and take a lead internationally in creating incentives for companies to improve their security engineering, to help avoid the risk that manufacturers might move to markets with weaker regulation.

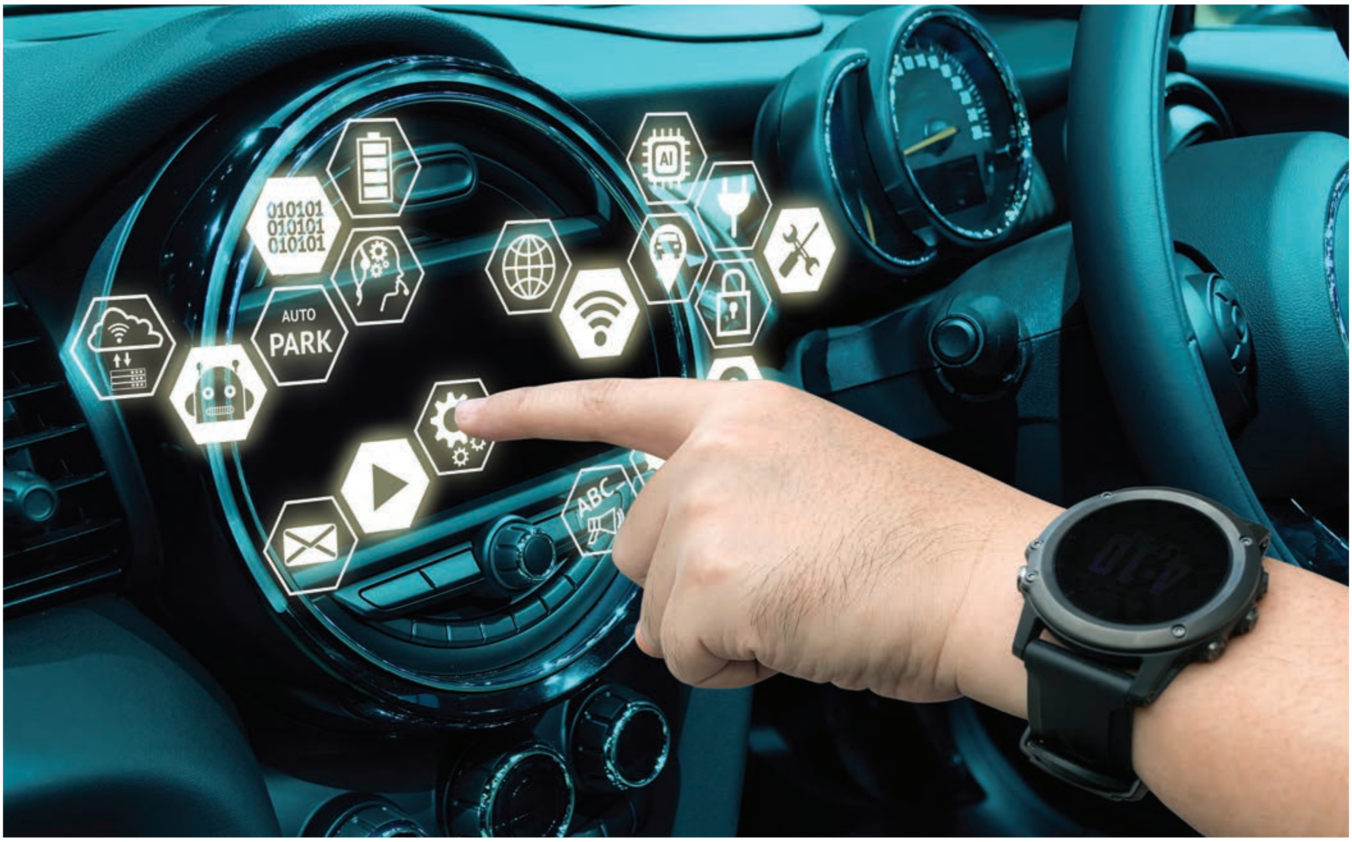
The shift from the risk of physical attack to cyberattack requires a concomitant change in government's mindset. There is a need for government to consider policy and procurement alongside technology to understand the nature of the technologies and take a leadership role. Government requires a change in culture and better knowledge to understand security when making commercial decisions. Government guidance[147,148,149] is helping organisations, including government organisations, understand how they can protect themselves.

Government, industry, academia and regulators should work together on a sector-by-sector basis to debate solutions that improve cyber safety and resilience at different levels of criticality. These solutions need to ensure that innovation and value generation are not adversely affected in proportion to the risk. In certain situations, value generation could be enhanced rather than adversely affected. While a sector focus is useful, it is also important to identify generic approaches to avoid duplications and support multi-sector supply chains.

4.2.2 Market-led interventions

One question is whether companies at the top of the supply chain that are not subject to the NIS Directive should be responsible for the cybersecurity of components that suppliers provide. For example, companies could require that all critical components, subsystems or software are warranted as secure by their suppliers. Alternatively, a supplier may need to fulfil certain conditions before they are allowed to connect into an existing network. For example, a supplier connecting to an IoT ecosystem may need to fulfil conditions around the encryption of data in transit and at rest, and other key management and distribution processes[150].

Codes of professional practice could be created, or industry-led specifications could be commissioned such as the BSI's Publicly Available Specification (PAS) that was commissioned by the CPNI to improve security practices in the built environment sector[151]. For consumer IoT, the Department for Digital, Culture, Media and



Sport (DCMS) are due to publish a report which sets out how government will work with industry to address the challenges of insecure consumer IoT products and services. The report's recommendations were compiled through close collaboration with industry and NCSC. The report will include a draft Code of Practice for industry containing thirteen practical steps to improve the cyber security of consumer IoT.

Incentives such as kite marks or other kinds of quality rating could be considered for certain products. This provides a visible rating of cybersecurity at the point of sale, allowing consumers and organisations to take cybersecurity into account when purchasing a product. However, kite marks tend to apply to individual products, and their suitability for systems is uncertain.

4.2.3 The role of system operators

Operational frameworks

Operational frameworks, supported by technical guidance – are an important tool in risk management for operational systems. In the longer term, international standards would support the frameworks. They allow a common understanding of risks, and the necessary controls and management systems to mitigate risks, agreed by all relevant parties including operators, vendors, regulators, government departments, institutions and academia. There are key elements that robust frameworks should include.

Risk assessment techniques that are practicable, achievable and used for proportionate outcomes is one key element, such as those provided by HSE in its operational guide[152]. System specifications should include security as well as safety, which will help to address poor security functionality in software and hardware. Risk-based specifications for design, operation and maintenance will provide a common framework for all in the supply chain, around which end users can procure equipment. It can also underpin independent certification of equipment. Operators should integrate cybersecurity into their and the supply chain's overall risk management systems, so that it is an integral part and not a 'bolt on'. Good information about what to include in cyber risk management already exists[153], and this is where the benefits can be realised in the short term. Frameworks may require research in specific areas such as how risk assessment can achieve proportionality, architectures, and how robust security measures for software can be created such as software that does not require patching. Funding for these areas of research is required.

This report discusses the need for competency frameworks to ensure effective implementation of operational systems in Section 4.2.4.

Addressing legacy systems

The challenge of how to address legacy systems is the most immediate issue for many system operators. As many of the controls recommended for new systems will not be suitable, different approaches will be needed to mitigate risks in legacy systems. Measures that would help to reduce cybersecurity risks include ensuring staff have the appropriate competencies, creating an asset register of equipment that is susceptible to cyber risks, ensuring management systems are put in

THE ENGINEERING PROFESSION HAS A VITAL PART TO PLAY IN CYBER SECURITY EDUCATION WITHIN ENGINEERING COURSES AND AS PART OF CONTINUING PROFESSIONAL DEVELOPMENT, GIVEN THE SKILLS GAP IN THIS AREA.

place to reduce risks from maintenance activities and reducing risks at source. For example, understanding the benefits versus the risks of connecting systems to the internet, and introducing 'air gaps' where necessary. Some systems may need to be upgraded if the risk is not reduced to a tolerable level.

Addressing vulnerabilities caused by equipment replacement

Vulnerabilities may be introduced when equipment such as instrumentation is replaced. For example, the embedded software in a device may not be the same if it has been upgraded or tampered with intentionally, although it is often possible to ensure that it is upward compatible and will not cause unintended consequences. Counterfeit equipment could go undetected and introduce malware if there are not systems in place to provide assurance that equipment is genuine. The issue of counterfeiting is discussed in Section 4.1.

4.2.4 The role of the engineering profession

The engineering profession, supported by the Academy and the professional engineering institutions, has a role to play in influencing practice. It can help to develop the knowledge and skills needed to create high quality software, hardware and systems using scientific and engineering methods that are appropriate to the business case. Through its industrial and academic members, the profession has knowledge and expertise that can inform policymaking and the development of standards and regulations.

More broadly, the profession has a vital part to play in cybersecurity education within engineering courses and as part of continuing professional development, given the skills gap in this area. More software and systems engineers with expertise in cybersecurity will be needed. As physical systems become increasingly digitalised, other engineering disciplines will also need a degree of cybersecurity knowledge[154]. Like computer scientists, engineers will need skills that allow them to apply core principles in an environment in which technologies are rapidly changing[155]. They will need to develop the softer skills needed to understand the role of people and processes alongside technologies in cybersecurity.

The Academy welcomes the initiative by the Information Assurance Advisory Council (IAAC) and other organisations to create a 'Cybersecurity skills alliance' that will help develop a flow of cybersecurity professionals, and provide an identified career path with associated qualifications and training for them[156]. This body of cybersecurity professionals would benefit from resources that enable sharing of best practice. Broader efforts to encourage schoolchildren and older students to consider a career in cybersecurity are also welcome[157,158]. There is also a need to broaden skills training to cover cybersecurity in relation to embedded systems and interconnected physical and digital systems, which goes beyond the more prevalent skills training in software vulnerabilities, malware and the protection of data.

The appropriate competencies are also needed to ensure that operational systems are implemented effectively. Operators, vendors, designers and regulators each have their own competency set as they have different responsibilities. The competencies for a designer, for example, are different from a person that operates and maintains the systems. Government, alongside the relevant professional bodies, has a role to play to ensure cybersecurity competency frameworks are developed and that proper targeted training is available.

Recommendation 2a

There should be a clear owner of the cyber safety and resilience agenda in government, with oversight of sector-specific and common issues, and oversight of where the necessary interactions need to occur between the different sectors and stakeholders. Lead government departments, with the support of NCSC and CPNI, should continue to convene the appropriate stakeholders to tackle the cyber safety and resilience of key sectors and levels of criticality, and to create a mutually supportive direction of travel. For some sectors, it may be more appropriate for NCSC to take the lead, while in other sectors where the regulator has deep experience of safety issues, it may be more appropriate for the regulator to take the lead. Ongoing dialogue is needed as threats are evolving over time.

Recommendation 2b

Where sector-specific frameworks already exist, NCSC and relevant government departments should ensure that they are sufficiently robust and are adopted and operationalised across the relevant sector stakeholders. They should identify where further guidance is needed to allow them to be operationalised. Government and industry sectors should adapt and operationalise general frameworks, tailored to their specific requirements and developed to include guidance on supply chain risks where they have not already done so.

Recommendation 2c

Government should encourage the adoption of sector-specific frameworks in both the public and private sectors through procurement, by incorporating the use of frameworks in project specifications.

Recommendation 2d

The Academy greatly welcomes the formation of NCSC and the broadening of its remit to tackle the cyber security of all digital systems utilised by society for civil, commercial or personal purposes. NCSC has a leadership role in a broad area and it is likely that its success will bring new demands, as will a changing landscape. A periodic review of NCSC's structure and capacity would ensure that it is able to address effectively emerging issues in future. The review should consider how cross-cutting issues such as cyber safety are most effectively addressed between the various agencies and lead government departments.

4.3 Integrating safety, security and resilience in regulation

Many existing regulations are no longer fit for purpose as systems evolve and the threat level changes. Greater focus is needed on cyber safety and resilience. In future, regulations must integrate safety, security and resilience and protect consumers.

A major challenge is how to adapt regulations to integrate safety, security and resilience[159]. This is a challenge for systems that are changing because of updating software (a necessity of patching security vulnerabilities) or connecting with new components or systems. This is because many products require 'type approval' (certification against technical standards) that is invalidated if the original specification for the product changes. One such example is the EU Directive for cars[160] that relates to the approval of whole vehicles, vehicle systems, and separate components[161], which the UK will need to conform to until it has left the EU. There is currently uncertainty about how UK will take forward regulations after its exit from the EU.

There are particular challenges around cybersecurity[162] for safety-critical systems that require a safety case. One challenge is that cyberattacks invalidate the assumption that failures in independent safety functions will occur independently, which is a critical assumption in many safety cases. Another challenge is that once a vulnerability is discovered in software, the length of time needed to update the safety case before a software update is applied provides a window for an attack before the vulnerability has been removed. Safety and security may also conflict in other ways as security often restricts access whereas safety requires it to be available, such as in an emergency. For example, in a medical emergency, access to sensors and data may be required.

The separate approaches to regulations and directives by different sectors and agencies works against an integrated or systems view of cyber safety and resilience. Where directives are not aligned, there are conflicts that create a barrier to the development of innovations, including poor understanding by companies of directives, delays to innovation and increased costs. For example, there are conflicts in directives on medical devices for e-health, connected cars and autonomous vehicles[163]. Companies may try to work round the directives by designing products that fit one directive only[164] or not obtaining full type approval for their products, which breaks safety rules in some cases. Directives need to be compatible and useable to ensure that security is adequately addressed. However the UK decides to develop regulations following its exit from the EU, the principle of avoiding conflict between different regulations applies. In industries such as aviation and healthcare where there is a well-developed safety culture, regulations need to be reviewed and extended to consider cyber safety and resilience. These industries have often developed sophisticated models for dealing with human factors in system design and operation, which could be drawn across into analyses of the cyber safety and resilience of systems.

A research report to the European Commission in 2016 highlighted that many EU agencies now need access to cybersecurity advice when formulating safety policy in the industries they regulate[165]. In 2017, the Commission duly gave the European Union Agency for Network and Information Security (ENISA) a policy role in addition to its existing role of coordinating Member States' defensive actions[166]. Better coordination between stakeholders such as government and vendors of software products and services is also needed when vulnerabilities are discovered, so that appropriate action is taken to protect users. A project to investigate a future multi-industry regime for IoT vulnerability disclosure and incident reporting is underway[167]. Safety regulations often recommend the disclosure of safety incidents, for example, when life has been put at risk, whereas in cybersecurity the focus is on the reporting of vulnerabilities. It will become even more important to report cybersecurity incidents and not just vulnerabilities with the development of IoT, as the attack surface is becoming larger.

UNDER THE NIS DIRECTIVE, REGULATORY RESPONSIBILITIES WILL BE HELD BY SECTOR-SPECIFIC 'COMPETENT AUTHORITIES' FOR WHICH CYBERSECURITY EXPERTISE IS NEEDED.

Cybersecurity agencies often have a different motivation and focus from regulatory bodies. They need to be more aware of consumer issues such as safety and privacy, and conversely regulatory bodies need to be more engaged with cybersecurity issues. Any regulatory impact analysis should consider the linkage of regulation. Regulators will also need to consider new approaches, so that safety and resilience can be assured. For example, in the case of medical devices, an engineering 'safety case' approach may be more suitable than the randomised control trial (RCT) methods that have traditionally been used in this sector[168,169], as long it can accommodate the process of updating software.

One barrier to creating robust regulations that address the requirements adequately is the lack of sufficient technical expertise within regulators. For example, safety regulators may not have the cybersecurity expertise needed to review safety regulations in the light of security threats. Regulators also need expertise to discharge resilience duties. Under the NIS Directive, regulatory responsibilities will be held by sector-specific 'competent authorities', usually the Secretary of State for the lead government department. Cybersecurity expertise will be needed for duties such as auditing, monitoring and providing guidance.

4.4 Strengthening the existing legislative framework

Improvements to legislation that build on existing legislative frameworks around product liability, data protection law and cybercrime will be needed to combat current weaknesses in the law. The complexity of legal agreements underpinning existing products that use IoT technologies can create unfairness for consumers, because of the difficulty of communicating such complex agreements and because of contradictions in the agreements themselves. Tighter product liability laws that establish accountability for manufacturers of software, hardware and systems should be considered. This would provide an incentive for improving the quality of products. Lowering the evidential barrier for bringing action against manufacturers of these products would improve consumer protection. Tighter requirements for companies would ensure that networks and products are updated with security patches. Accountability should lie with those who have the power to make changes.

The development of liability rules for autonomous vehicles in Germany provides an interesting example. Germany is pushing ahead with draft legislation to ensure that its autonomous vehicle industry is competitive[170]. It will provide the legal basis for temporary, full transfer of the driver's control to the automated driving system. The proposed legislation requires vehicles with automated driving systems to be equipped with black boxes that record journey data. This data will be used to evaluate whether the driver or the system is at fault in case of an accident. If the manufacturer of the system is responsible, it will be liable without limitation. However, it will still be a challenge to determine whether the manufacturer was negligent or whether the cause was something that could have been reasonably predicted.

As with other types of regulation, the possible impact of tighter product liability laws on smaller companies and on innovation should be considered. The law could protect companies in several ways. For example, a 'state-of-the-art' defence uses the argument that the manufacturer could not have known about a particular danger or hazard in a product by using the scientific or technical knowledge available at the time the product was made or sold. When software updates are an integral part of a product, the legal terms dictate that if the consumer does not take the updates then the manufacturer is not liable for the non-updated product, although this raises the question of residual liability when support is withdrawn.

Health and safety legislation[171] provides an example of a goal-based approach. The means of achieving compliance is not prescribed but goals are set that allow alternative ways of achieving compliance. Similarly, an environment could be created where those who create the security risk are liable for the consequences of that security risk. They would be able to demonstrate that the risk had been managed proportionately by following the appropriate guidance.

Recommendation 3a

Government should ensure that the UK can maintain its influence on the development of improved regulations that integrate safety, security and resilience, particularly in sectors that are important to the UK economy. It should also maintain an influence on the development of international standards. It should review and extend existing safety regulations to take account of cyber safety and resilience. Government, NCSC and regulators need to work with their international counterparts to ensure that international standards are sufficiently robust to help deliver safe and resilient systems.

Recommendation 3b

Government should convene a task force to address how the existing legislative frameworks can be strengthened, including in the areas of product liability and cybercrime. The frameworks should incentivise the production of software, hardware and systems of higher quality, and ensure that accountability lies with those who can make improvements.

Recommendation 3c

Government should focus resources on strengthening cybersecurity expertise in regulators, using part of the budget for the UK's cybersecurity programme. It should consider how regulators can ensure standards and regulations address cyber safety and resilience as part of their duties.

Recommendation 3d

Following the introduction of the NIS Directive in May 2018, government should ensure that expertise and resources are available for individual government departments taking on the role of 'competent authority' on behalf of individual sectors.

4.5 Transferring expertise in safety-critical systems

The UK has world-class expertise in safety-critical systems that should be transferred to other sectors and applications.

Socio-technical systems approaches

Socio-technical systems are composed of people, processes and technology. To work effectively and efficiently, all three need to be designed to work together. While some systems in cybersecurity are autonomous, the majority support production processes and involve people. Security measures must not block production processes or cause friction that significantly lowers productivity. Security measures that people interact with must be usable and acceptable. The NCSC is promoting the need to design security as a socio-technical system in the UK. For example, guidance on passwords[172] and phishing[173] show how the coordination of technical measures, organisational processes, and guidance and support for staff and customers can help to ensure threats are managed more effectively than isolated measures.

There are differences between safety and security. In safety, active attacks, acts of sabotage and vandalism, are relatively rare, while in cybersecurity, active attacks are frequent. Nevertheless, the history of safety provides lessons for cybersecurity, and basic safety engineering principles can be applied to immediate effect. Historically, safety engineers learned that blaming humans, such as pilots or nuclear power plant operators, for mistakes that caused accidents did little to improve safety. This is because humans are put in an impossible position at the end of a chain of latent failures in technology or processes. If a well-trained pilot attempts to stop a plane crashing, but the information presented is insufficient to guide the necessary action, the root cause lies in design of the technology. If nuclear power plant operators have not been trained regularly on how to handle rare events and conflicting information, the root cause lies in insufficient processes.

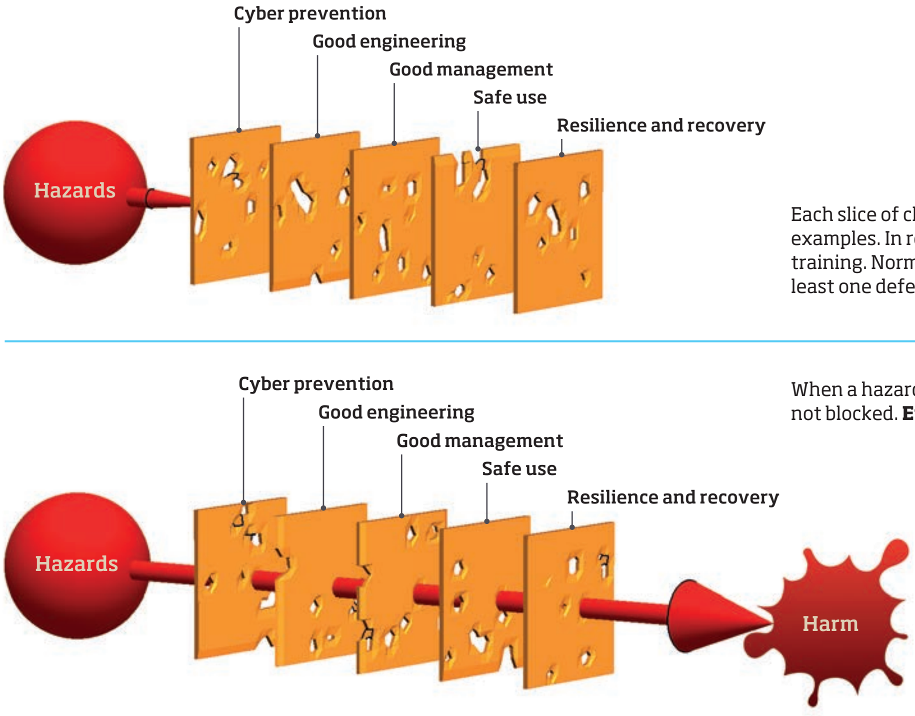
Immediate improvements that can be made to the design of technology, processes and training can be identified by socio-technical systems-based safety frameworks[174]. Safety and security are secondary tasks in productive organisations, so the workload and complexity of those tasks needs to be audited and reduced as much as possible. In addition to ensuring security technology is usable, the 'right' behaviours need to become habits. People also need to be empowered to identify security mechanisms they cannot use, or processes that do not work in the context of their tasks. Security practitioners need to emphasise the positive aspects of security, and be approachable and willing to negotiate 'fixing security together' with employees[175,176]. The work of James Reason[177] also offers principles for preparing people for recovery and 'heroics', the ability to handle unexpected events. Given the speed at which new attacks emerge, this will be particularly important for cybersecurity.

Good cyber safety requires organisations to have robust defences at every level. These should include cyber prevention, well-engineered and well-managed devices and systems that are used safely, good resilience and the ability to recover from adverse incidents. This is illustrated in Figure 1 on page 28, which uses Reason's 'Swiss Cheese' model to explain accident causation that in turn impacts on cyber safety. The model makes very clear that there is no single 'root cause' for problems and blaming individuals misses the point.

Engineering tools and methods

The UK has world-class centres of excellence in safety-critical systems. It has developed tools and methods to produce and assure software with extremely low defect density and tools to ensure communications are secured across networks. These methods can help improve the cyber safety and resilience of systems. They include formal specification and verification methods[178], functional programming[179], engineering design and development methods[180], system monitoring, incident

Figure 1. Reason's Swiss Cheese model of accident causation. Explanatory text provided by Professor Harold Thimbleby, Swansea University



Each slice of cheese is a defence; the slices shown are examples. In reality there will be more, such as cybersecurity training. Normally, each possible hazard is blocked by at least one defence, but no defence is perfect, hence the holes.

When a hazard aligns with defects in every defence, harm is not blocked. **Every defence has failed.**

investigation, disaster recovery and methods of assurance. For example, the latest air traffic control system for National Air Traffic Services (NATS) in the UK, iFACTS[181], was developed and safety-assured using formal methods that have enabled NATS to increase the traffic densities in UK controlled airspace. In the process industry, hazard identification, operability and management are very well established processes and there is also much to learn from high hazard environments.

There is also potential to transfer expertise from the safety-critical software community. However, it is qualitatively a separate discipline and embraces a different mindset from other communities that are more concerned with time-to-market, as it develops products that are quickly outmoded. The use of tools and methods from the safety-critical community by other domains will need to be justified by a commercial case.

Current mature and robust applications of IoT could be identified in which the cyber safety and resilience of the systems involved have been successfully addressed, such as in aircraft engines where real-time diagnostics informs operational decisions. It would be useful to analyse business, technological and update practices, for example, and how safety case regulation is applied to engines. It would also be interesting to consider the liability issues surrounding real-time analysis of data and how decisions are made based on the data are also of interest. How safety-critical systems tools and methods have been applied to help with cyber safety and resilience is also of interest, as are applications of IoT to monitor security and safety. This would inform improvements to emerging applications of IoT.

Recommendation 4

Professional engineering institutions, with the support the Academy, should publish case studies to illustrate robust applications of IoT in which cyber safety and resilience have been successfully addressed. This would allow best practice to be disseminated to other sectors and applications. Case studies should identify the technological, business and operational practices that contribute to cyber safety and resilience including, where relevant, the use of safety-critical systems tools and methods, and the use of IoT to monitor safety and security. The case studies should highlight strengths, weaknesses and business benefits of such practices.

4.6 Research on systems assurance

Methods for assuring complex systems of systems require further research.

Existing formal verification methods may be applied to an embedded device or system of devices for systems such as aeroplanes. Different approaches to evaluation are needed in the case of a more complex system of systems such as IoT, which has many different companies and players involved in the system. It is possible to analyse an individual component and what it does, as well as its interface with the rest of the system. However, there may be things that the component is capable of outside its specification that are unknown, but could impact on the rest of the system. New approaches may focus on the interactions between different components

DIFFUSE RESEARCH AREAS SUCH AS CYBER SECURITY, IoT, ARTIFICIAL INTELLIGENCE, HARDWARE SECURITY AND TOOLS AND METHODS FOR SOFTWARE ENGINEERING WILL NEED SUPPORT, WITH STRONG LINKS TO INDUSTRY AND REAL-WORLD APPLICATION.

and systems, or use run-time checking to detect errors that only become apparent during execution of a software application rather than checking solely during development.

The safety case can be invalidated if a safety-critical system is changed, for example, if it is patched with a software update. Where the cost of preparing a new safety case is prohibitive, it is likely that systems operators are refraining from patch management. One issue is whether it is possible to get approval for an updated safety case by valuing and communicating new risks sufficiently quickly. A second issue is whether systems can be designed that can be updated without the safety case being compromised. A further issue is whether it is possible to procure and manage large-scale systems with COTS on a stronger engineering footing. There is some debate about whether it is possible to create systems with the correct large-scale behaviours from insecure components. These include emerging properties and behaviour under failure or attack conditions. The need for safety assurance imposes constraints on how systems should be designed and commissioned to make the risks containable.

New ways of thinking about risk are needed. Dynamic risk assessments would allow risk to be assessed for systems that change over time due to new components. In many cases, using new approaches to risk such as machine learning may be more suitable than deterministic, proof-based approaches. Risk models must consider both the benefits, such as the efficiencies and improvements in security created through digitisation, and risks. In aggregate, even large scale-deployment of insecure devices such as COTS may result in better physical security.

Once the system reaches a certain level of complexity, it may not be possible to prove that it will not fail. Resilience mechanisms that keep different parts of the system independent to prevent cascades of failure through system compartmentalisation and system recovery techniques may be possible.

The increasing complexity of systems and innovative systems that use AI technologies in decision-making create the need for new methods of assurance. While autonomous systems that use AI techniques require new methods of assurance, there is also the potential to use AI and machine learning approaches in assuring systems. This requires further research. The provenance of security patches also needs to be assured, with secure channels as deployed by organisations such as Apple and Microsoft manifesting best practice.

Support for the research ecosystem, including academia, SMEs and government agencies, would accelerate the development of solutions, which may be partial until complete understanding is achieved. Policymakers and regulators need to be aware of these outstanding academic challenges so that policy and regulation is based on the best possible scientific knowledge, and reflect scientific and commercial realities. Best possible scientific knowledge should inform emerging frameworks, tools and guidance for different sectors and applications. These challenges need a multidisciplinary approach. Diffuse research areas such as cybersecurity, IoT, AI, hardware security, and tools and methods for software engineering will need support, with strong links to industry and real-world application.

Recommendation 5a

UKRI and other research funders should target funding towards outstanding challenges and gaps in knowledge around assuring complex systems and improving existing systems and solutions. This must be done in the context of real-world applications and include strategic areas of growth for the UK, including the Grand Challenges identified in the industrial strategy White Paper. Research should build on the UK's world-class research expertise in cybersecurity, safety-critical systems, software engineering, hardware security and AI.

Recommendation 5b

Given the urgency with which improvements are needed, cyber safety and resilience should be considered as a proposal for wave three of the Industrial Strategy Challenge Fund, with funding targeted at challenge-led programmes of research and application. The programmes could involve major manufacturers, SMEs, the Catapults and Innovate UK.

Recommendation 5c

Government funding for new technologies and systems should include requirements to address the cyber safety and resilience issues associated with the technologies and systems.

Recommendation 5d

Outstanding challenges and gaps in knowledge in complex systems should be a focus in the government's Cyber Security Science and Technology Strategy. Key challenges include understanding the long-term risks as systems and businesses evolve, balancing the commercial realities of risk management against the level of risk that society is willing to tolerate for critical national infrastructure, and investigating the resilience that society expects and how to deliver it.

5. Connected health devices

This section reports on the Academy's roundtable discussion on connected health devices, which explored the nature of the vulnerabilities in connected health devices, the current regulatory context and possible regulatory and non-regulatory mechanisms for improving practice. The section explores connected health devices as a specific exemplar of the types of complex and interdependent systems that support the modern economy. It highlights where issues are consistent with the general messages developed earlier in the report, and where issues are specific to the health sector.

5.1 Digitalised systems in healthcare – the opportunities and challenges

Digital health, including the use of connected health devices in clinical and non-clinical settings, offers opportunities to create economic and social benefits by transforming health and social care best practice in the 21st century. A transformation is necessary because global healthcare costs are rising faster than the global economy as a result of demographic changes, advances in medical science and growing expectations of healthcare. There is also an increasing chronic disease burden, worsened by the conditions of modern life such as air pollution and an ageing population.

Tools such as IoT, smart phones and modern software enable connectivity and can support clinical decisions, and allow patients to be managed and treated remotely. Connected health devices, a key set of tools, range in scale and complexity from implantable devices such as cardiac pacemakers, drug administration devices and monitoring devices[182,183] to non-implantable devices such as infusion pumps, defibrillators, glucometers and blood pressure measurement devices[184]. Connected health devices also include large-scale hospital equipment such as MRI scanners and x-ray machines. Health devices may be connected into a network to carry out remote diagnostics of the equipment, for example, or for remote monitoring of patients.

Connected health devices are part of an international supply chain, and innovation in this area needs to keep in step with new demands on healthcare and the need for trusted health and care systems. Enhancing the prospects for digital health requires multidisciplinary expertise in, for example, health, engineering, data transfer and the associated regulations. Costs to the NHS because of poor quality hardware, software and systems should be minimised.

Connected health devices have a spectrum of possible impacts associated with the range of applications, from devices to enable assisted living and wellbeing monitors[185] used by individuals or insurance companies, for example to critical life-support systems. A process is needed to map the scale of impact from a cyberattack or inadvertent failure against the range of applications. One example of a non-critical application is the insurance sector's use of devices to adjust premiums according to the physical activity of the insured person, measured by wearable tracking devices[186]. The resources required for risk mitigation depend on the potential impact of a cyberattack or failure.

5.2 The nature of healthcare systems and their vulnerabilities

There are parallels between health devices and industrial control systems, and it is helpful to look at industrial control systems to understand why health devices might be vulnerable and where the vulnerabilities lie[187]. However, it should also be noted that the constraints under which systems are designed and operated are different, and so the impacts of a potential cyberattack or inadvertent failure are different.

There are similarities in generic architectures between industrial control systems and large-scale medical devices, such as machines delivering proton beam therapy or MRI scanners. Each system contains sensors and actuators, and there is a control process, such as the focusing of the beam, a controller, and a human-machine interface to the operator. Industrial control systems increasingly allow remote connectivity for remote control, diagnostics or maintenance. Many similar elements exist in smaller-scale health devices such as implantable devices, including a control system with sensors and actuators, and a controlled process.

As components and the links between them become digitalised, they also become targets for attack. Both individual components and the systems that are created from these components have vulnerabilities, with subsequent risks for individuals using the devices and the systems that they are connected to. Risks include loss of data and loss of control of system operation. As with other systems, the adoption of IoT has the potential to increase the degree of interconnectedness. Enterprise IT systems used by healthcare providers are also becoming more integrated with clinical engineering functions and suppliers.

Securing cyberphysical systems requires a different approach to enterprise IT systems[188]. In industrial control systems or health devices, 'edge devices' tend to be more vulnerable and likely to be attacked. There are also resource constraints such as low memory and processing capabilities, and low power that have not typically been present in enterprise IT systems, as well as many legacy issues. Many hospitals have very poor inventories of their embedded devices, and field devices may also be remotely located from resources.

5.3 Cyber safety and resilience – the legal and regulatory context

The regulation of health devices and systems has focused on patient safety, albeit not perfectly, but has not fully considered the possible impacts of poor cybersecurity on patient safety or privacy. As new technologies and systems are created, and the threat environment evolves, vulnerabilities in connected health devices need to be addressed. It is therefore necessary to revisit regulatory frameworks for health devices to assess whether there is sufficient consideration of cybersecurity, and how appropriate levels of safety and resilience can be achieved.

A CENTRAL CHALLENGE IS TO PRODUCE TRUSTWORTHY, REGULATED PRODUCTS THAT WORK TO MEDICAL STANDARDS AND HAVE GOOD CYBER SECURITY, BUT AT THE SPEED, EFFICIENCY AND PRICE OF CONSUMER PRODUCTS.

A consistent international approach to regulation of cybersecurity does not exist. For example, the EU and US regulatory regimes deal with this in very different ways. In Europe, the current Medical Device Directive 93/42[189] does not include cybersecurity. The new regulation, 2017/745[190], has a couple of references to cybersecurity, but it is still not an explicit driver for the regulation. It is also implicit in the various standards, for example ISO 14971[191] and IEC 62304[192]. In contrast, European privacy law is very robust[193], and medical data cannot cross international borders, which means telemedicine is not allowed across countries.

In contrast, the US FDA[194] provides guidance on addressing risks of cybersecurity threats for organisations[195]. Furthermore, medical device manufacturers as well as other firms involved in the distribution of devices must follow certain requirements and regulations once devices are on the market[196]. The FDA can bring to bear in-house expertise to judge whether products have sufficient cybersecurity, although there is a recognised tension between 'ideal' regulation, and industrial innovation and entry barriers. In Europe, there is a defined set of factors that must be satisfied in order to qualify for a CE mark but they do not include cybersecurity or cyber safety. In contrast, the FDA carries out a more subjective evaluation that takes cybersecurity into account. Furthermore, privacy law is less robust in the US, although it does have some sector-specific guidelines such as HIPAA[197].

Other regulatory differences exist between the US and Europe, notably in the telecoms sector. In the EU, licensed operators have to comply with telecoms standards, which are linked closely to EU privacy law. This approach is tighter than in the US, and reflects a more federated distribution model that includes both service providers and network operators. In contrast, the approach to connecting devices is looser in Europe. Global inconsistencies in regulation impact on telehealth and telecare, such as point-of-care testing[198], mobile wellness devices and wearables.

Incompatible regulation between different jurisdictions has important implications for the international supply chain. This is true for both cybersecurity and medical device regulation. Nevertheless, the EU and the US are de facto leaders in harmonised regulatory frameworks in healthcare, although practitioners report that the FDA either leads or is tighter in its requirements. Currently, Europe and the US represent the major share of the world market for health devices. Some countries accept medical certification from Europe or the US, while others such as China have their own regulation.

5.4 Improving cyber safety and resilience

Regulation and innovation

A central challenge is to produce trustworthy, regulated products that work to medical standards and have good cybersecurity, but at the speed, efficiency and price of consumer products. This requires differing cultures to come together: pharma/clinical research – 'do it once, take your time and get it right first time (or drop it)' – and IT 'create a minimally viable product, as fast as possible, and test it in the market to improve it'. There is some debate about which health or medical devices should go through a certification process. For wearable lifestyle devices, the gap between the two cultures is narrower and the regulation is more accommodating to innovation. However, there are examples of innovative medical devices in development that can fulfil regulations[199].

There are many non-validated health apps available that are not intended for use in a medical context and therefore are not regulated, but may still be adopted for use in a medical context by healthcare professionals or consumers[200]. These apps are not proven to be effective. It is not clear to consumers which products are regulated and which are not, although both Google and Apple are considering separate locations within their app stores for regulated applications.

Too much regulation may not be desirable because of its effect on innovation. In addition, the pace of change of technologies and the way in which people interact with technologies is very rapid and it is a challenge for regulations and standards to keep up. This can be reinforced by a slower moving culture within the regulators. A clear indication of the scope of use for which a device has been conceived is necessary, since users may use a device in a way that was not intended. This scope of use must also consider the types of threats that the device will face within a given context.

On the other hand, regulation could be considered as an enabler of innovation. It provides a defence in the case of litigation, demonstrates devices are trustworthy and helps to build trust. However, for small innovators submitting their device to the FDA in the US, it is a challenge to know whether they have done enough to satisfy the FDA experts as evaluation of cyber-risks is hard to do. A company may not want to cut corners to ensure they produce the cheapest possible product, but equally it will not want to be left behind if it acts more responsibly than others in the market.

Regulations around data protection and cybersecurity need to be adequately linked, with clear signposting

to innovators about how to navigate the regulations. Guidelines or a forum would help companies understand best practice.

The NHS has a strong existing framework for patient safety[201]. It will be important to identify its limitations in dealing with malicious threats and how the framework should be enhanced to take cyber safety and resilience into account.

Standards and cyber labels versus risk-based approaches

It is a challenge for hospitals to specify security requirements when procuring health devices. It may be clinicians undertaking procurement, who are not experts in cybersecurity.

Adding cybersecurity to existing standards would help to get improved cybersecurity practices into the field since hospitals would be able to demand cybersecurity standards. It is an accessible approach for manufacturers. Quality labels or 'cyber labels'[202], similar to EU energy efficiency labels on white goods and EU safety labels on car tyres, could also help procurers and end-users, whether staff or patients, to understand the product.

The consumer also requires clear information on the cybersecurity of products that they may be purchasing. A trusted source of information is necessary, which may provide online support or solutions. In the UK, there is potential for pharmacists to play a bigger role in providing support by giving advice to consumers, as they do in other countries. There may also increasingly be a role for insurers in the protection of consumers, particularly as new business models and end-user license agreements are developed.

While a compliance-based approach such as standards may help to improve cybersecurity, it is not a silver bullet. There could be adverse consequences such as box-ticking or unintended outcomes. Cyber labels could also lead to unintended outcomes. It may be possible to meet every medical standard and still be open to exploitation. There is a question about how kitemark schemes or cyber labels can be created that are technically robust and meaningful to users. There is a cost associated with applying them and a risk that they are meaningless if too simplistic. Moreover, it is possible that devices are used in a way that was not intended – for example, fitness trackers might be used to support a clinical diagnosis. Cyber labels should therefore consider and clearly specify the purpose and uses of the device for which they have been issued.

There may be advantages to clear, deterministic schemes that define the minimum requirements around patching.

A risk-based approach may be more appropriate in more complex situations. The necessary action is influenced by how much harm a product could do and the likelihood of that harm happening. For example, the risks for a monitoring device might be very different from an embedded device. Similarly, risks may be very different for devices used in a hospital setting in comparison to those used at home. A wide variety of people may need to access and use many implantable devices and they must be easy to configure regularly over their lifetime once implanted. For many medical devices, operational security is more important than data loss, particularly if the data is properly encrypted and anonymised, so that the device continues to work or at least fails safely. Other considerations include the length of time the devices will be in use and the lowest viable service that must be maintained at all times.

It would be a challenge to create a set of guidelines that fits the full breadth of medical devices. In the FDA's risk-based approach, which requires the balance of risks and benefits to be considered, the evaluation of cyber-risks may end up with the clinician without the requisite cybersecurity expertise. NCSC is considering developing principles-based ideas for IoT products similar to its bulk data-security principles[203] that would be applicable to connected health devices.

MANY IMPLANTABLE DEVICES NEED TO BE ACCESSED AND USED BY A WIDE VARIETY OF PEOPLE – FOR EXAMPLE, THEY MUST BE EASY TO CONFIGURE REGULARLY OVER THEIR LIFETIME ONCE IMPLANTED.

Strategies for defending against cyberattack

The US has developed seven strategies for defending industrial control systems[204]. These strategies could apply to health devices, given the similarities in architectures, although the extent of their applicability even to different types of industrial control system is still being explored. A key strategy is proper patch management, but there are questions about how it might best be done for health devices. As with other sectors, there may be tensions between achieving safety and security outcomes. For example, if a software update is available for a pacemaker, is it preferable to update the pacemaker or to live with the legacy pacemaker as originally implanted? Does the update work?

In a clinical engineering context, certain devices are patched or updated frequently. In other devices, the software may not be updated for several years unless there is a driving reason to do so. Government or the manufacturer may send alerts that explain how the update will obviate a risk, and such alerts will be acted on by device users. Software updates that provide additional features would have to be justified before the update is allowed. There is potential for patch management to be improved, if sufficient funding and resources were applied.

Human-centred approaches

The human aspects of security are a crucial consideration, and need to embrace both patient- and staff-centred approaches. There is an urgent need to address security culture and behaviours, together with the insider risk in healthcare. In addition, robust cyber-hygiene measures, the range of activities that allows an organisation to operate in a safe and secure way, should be developed by healthcare organisations.

A human-centred approach benefits the development of health devices and systems. Systems need to consider human behaviour and, in particular, human fallibility during the design process. If clinicians and carers input into the development process, it will help developers to understand better the diversity of users and how they will use the device in practice. Developer-centred security involves studying the culture of software development to understand the pressures on software developers, and the motivations and barriers for developers to consider cybersecurity during the development process[205].

Changing ways of thinking and practices in the NHS

As for other organisations, good cyber safety requires hospitals and other healthcare providers to have robust defences at every level. These should include cyber prevention, well-engineered and well-managed devices and systems that are used safely, good resilience and the ability to recover from adverse incidents. This is illustrated in Figure 1 in Section 4.5, which uses Reason's 'Swiss Cheese' model to explain accident causation that in turn impacts on cyber safety.

However, there is a combination of interlinked factors that contribute to the creation of systems with inadequate cyber safety[206]. Products supplied to healthcare providers have unknown quality and therefore procurement is unable to choose a good solution. There is a lack of evidence from research about what good and bad solutions are, and solutions are hard to evaluate. This leads to poor regulation and to purchasing systems that do not meet operational needs, particularly when needs such as safety and security are poorly articulated. Hospitals end up with incompatible systems that create new problems.

Education and knowledge exchange

Education and knowledge exchange will also be an important aspect of improving cyber practice around connected health devices. Training of clinical professions in areas such as data literacy and cybersecurity could help, as well as learning from other countries about the different regulatory approaches to training. New initiatives such as the Faculty of Clinical Informatics[207], the professional membership body for clinical informaticians in the UK, are emerging. There could also be a role for professional engineering institutions to spread best practice and facilitate cross-sectoral learning.

5.5 Conclusions: Applying general principles to the health sector

Table 1 (page 36), draws the observations from Section 5 together and shows how the general principles for improving cyber safety and resilience identified in Sections 1 to 4 of this report relate to the health sector. It addresses the nature of the vulnerabilities, regulation, governance, procurement and the supply chain, design of software, hardware and systems, strategies for defending systems, and education.

Table 1. Applying general principles to the health sector

	General findings and principles	Application to the health sector
Vulnerabilities	Vulnerabilities arise because of software and hardware with insufficient security functionality and poor design, and in legacy systems that were not designed with security in mind and are being connected to networks.	Vulnerabilities exist in implantable and non-implantable devices, for example, in low power, low footprint sensors, as well as in larger-scale legacy equipment that is becoming increasing connected via networks. Enterprise IT systems used by healthcare providers are becoming more integrated with clinical engineering functions and suppliers.
Regulation	Regulations must integrate safety, security and resilience and protect consumers.	While there has been a focus on patient safety in the health sector, there has been little consideration of the impact of poor cybersecurity on patient safety and privacy. Regulations around data protection and cybersecurity need to be adequately linked, with clear signposting to innovators about how to navigate the regulations.
	The UK must be outward-facing and sensitive to the various international regulatory contexts that vary by sector.	The fragmented nature of medical device regulation across different countries is a particular characteristic of the health sector, and brings its own challenges and risks for the international supply chain.
	Scope of regulations.	The health sector is perhaps unique in producing consumer-facing health and wellbeing apps with distinct regulatory requirements depending on whether or not they are considered to fall under medical device regulations.
Governance	Better governance is needed to address cybersecurity.	There is a need to urgently clarify roles and responsibilities within the NHS governance structure at both local and national level.
	Improved cyber hygiene is needed.	For the health sector, risks and impacts are unique. For example, the attack surface is large because of the number of people with access to a device. There is potential for life-threatening impacts if a device is compromised or fails in other ways. This makes good cyber hygiene all the more important.
Procurement and the supply chain	Organisations need to be more aware of the vulnerabilities that reside in components and other products provided by their supply chain.	The health sector needs to embed cyber safety into decision-making. Many other sectors are more advanced in terms of awareness, governance and resource. An increased awareness of supply chain risks is needed in procurement. Learning from other sectors that are further ahead in their approach to cyber safety would be of benefit, such as aviation or nuclear sectors.
	SME suppliers may not have capacity or incentives to address security and create components or products with sufficient security functionality.	A central challenge is to produce trustworthy, regulated products that work to medical standards and have good cybersecurity, but at the speed, efficiency and price of consumer products.
	Incentives such as kitemarks or cyber labels could be considered for certain products.	Cyber labels could help procurers and end-users, whether staff or patients, to understand the product better. The consumer of connected health devices also requires clear information on the cybersecurity of products that they are purchasing. A trusted source of information is necessary, which may provide online support or solutions. Pharmacists could play an important role here.

	General findings and principles	Application to the health sector
Design of software, hardware and systems	Using principles from human-factors engineering in the design and operation of software, hardware and systems is an important consideration.	The application of human-factors engineering is important for improving the security of connected health devices and more broadly their dependability.
Strategies for defending systems	Strategies for defending systems against cyberattack should focus on methods that can be implemented with current techniques, such as patching, and that counter common exploitable weaknesses.	There is little robust evidence or quantification of the current security risks in the NHS, for connected health devices or more broadly, upon which to base solutions. There is a need to start measuring the problem before appropriate solutions can be identified. The need for a central registry of device security testing and assurance results should be explored. There are questions about how patching might best be done for health devices. As with other sectors, there may be tensions between achieving safety and security outcomes. For example, if a software update is available for a pacemaker, is it preferable to update the pacemaker or to live with the legacy pacemaker as originally implanted?
Education	Better education and knowledge exchange is needed.	The move to create a membership body for clinical informaticians is analogous to initiatives to create a body of cybersecurity professionals. Training of clinical professions in areas such as data literacy and cybersecurity will help, as well as learning from other countries about the different regulatory approaches to training.

BETTER EDUCATION AND KNOWLEDGE EXCHANGE IS NEEDED

TRAINING OF CLINICAL PROFESSIONS IN AREAS SUCH AS DATA LITERACY AND CYBER SECURITY WILL HELP, AS WELL AS LEARNING FROM OTHER COUNTRIES ABOUT THE DIFFERENT REGULATORY APPROACHES TO TRAINING.

Glossary

CERT UK: the UK's national Computer Emergency Response Team, now part of NCSC.

CESG: part of GCHQ, it was the UK government's national technical authority for information assurance prior to the formation of NCSC.

Connected health device: a device used for fitness, wellbeing or healthcare purposes that is connected to the internet or another type of network, including the smallest implantable devices, devices for monitoring health or levels of activity, and large-scale medical equipment. The device may or may not fall under medical device regulations. .

COTS: commercial off-the-shelf components that are bought ready-made, avoiding the need for organisations to commission bespoke solutions.

CPNI: the Centre for the Protection of National Infrastructure is the government authority for protective security advice to the UK national infrastructure.

Critical infrastructure: critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.

Cyber hygiene: the range of activities undertaken to keep an organisation or function safe and secure, formed of policies and procedures, training and skills development, and technology. They are used in combination to ensure that risks are minimised.

Cyber label: a type of quality label that provides a way of making visible the level of cybersecurity, similar to EU energy efficiency labels on white goods and EU safety labels on car tyres.

Cyber resilience: the ability of digital systems to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events.

Cyber safety: the ability of systems to maintain adequate levels of safety during operation, including in the event of a cyberattack or accidental event, thus protecting life and property.

Cybersecurity: the practice of protecting systems, networks, and programs from cyberattacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Enterprise IT systems: hardware and software designed to meet the needs of an organisation, which has traditionally been separate from the hardware and software used to monitor and control physical devices and processes.

FDA: US food and drug administration, responsible for regulating medical devices.

Footprint: the size of the computer RAM memory used in an application.

Formal methods: formal descriptions of software or hardware can be used to guide development activities and to verify that the requirements for the system being developed have been completely and accurately specified. Once a formal specification has been developed, a process of verification can be used to prove the properties of the specification and the developed system.

Functional programming: a technique used by programmers to create well-structured software that is easy to write and debug. Its suitability will depend on the application.

Human-factors engineering: this discipline considers human strengths and limitations in the design of interactive systems that involve people, tools and technology, and work environments to ensure safety, effectiveness, and ease of use.

Internet of Things (IoT): an umbrella term that describes the distributed networks of physical objects that may (or may not) contain sensors and actuators and are connected to the internet or to other communications networks, allowing data about an object or its environment to be generated, shared and acted upon.

Middleware: software that serves to 'glue together' separate, often complex, existing, programs.

NCSC: the National Cyber Security Centre helps to protect critical services from cyberattacks, manage major incidents, and improve the underlying security of the UK internet through technological improvement and advice to citizens and organisations. It brings together expertise from CESG, the Centre for Cyber Assessment, CERT-UK, and CPNI.

Operational technology: the hardware and software that controls physical systems.

Patch: an update to a piece of software that is introduced to fix or improve the software.

Point-of-care testing: a method of testing that allows medical diagnostic testing to occur at the time and place of the patient.

Product liability laws: these laws apply to consumer goods and goods used in the workplace, and require that products must not cause injury or damage to private property.

Programmable logic controller: used in industrial control systems, it is a computer that has been adapted for the control of manufacturing processes, such as assembly lines or robotic devices.

Remote terminal unit: used in industrial control systems, it provides the interface between physical objects to distributed control system or SCADA (supervisory control and data acquisition) system.

Acknowledgements

The project was overseen by a working group:

Professor Nick Jennings CB FREng
(Chair) Professor of Artificial Intelligence and Vice-Provost (Research and Enterprise), Imperial College London

Professor Robin Bloomfield FREng
Founding Partner, Adelard LLP and Professor of System and Software Dependability, City, University of London

Professor Sir John V McCanny CBE FREng FRS
Regius Professor Emeritus, Electronics and Computer Engineering, Queen's University Belfast

Professor Martyn Thomas CBE FREng
IT Livery Company Professor of Information Technology, Gresham College

Professor M Angela Sasse FREng
Professor of Human-Centred Technology,
University College London

Dr Michael Short CBE FREng
Chief Scientific Advisor, Department for International Trade

Professor Jeremy Watson CBE FREng
Vice-Dean (Mission), Faculty of Engineering Sciences, University College London

with support from the following staff:

Dr Philippa Westbury
Senior Policy Advisor, Royal Academy of Engineering

The Academy would like to thank the following peer reviewers:

Professor Ross Anderson FREng FRS
Professor of Security Engineering, Computer Laboratory, University of Cambridge

Siddharth Varma
Senior Policy Advisor, National Infrastructure Commission

Professor the Lord Darzi of Denham OM PC KBE FRS FMedSci HonFREng
Director, Institute of Global Health Innovation, Imperial College London

Professor Chris Hankin
Co-Director, Institute for Security Science and Technology, Imperial College London

Professor Emil Lupu
Director, Academic Centre of Excellence in Cyber Security Research, Imperial College London

Professor Maire O'Neill
Director, Research Institute in Secure Hardware and Embedded Systems, Queen's University, Belfast

Sarabjit Purewal
Principal Specialist Inspector, HSE

Professor Harold Thimbleby FLSW
Professor of Computer Science, University of Swansea

This report was informed by a series of workshops on cyber safety and resilience, including a workshop on connected health devices. We would like to thank participants for their valuable contributions to the workshops.

We would like to thank Dr Lucy Mason, DSTL (formerly Home Office) and Professor Emil Lupu (Imperial College London) for their help in arranging the first workshop.

References and endnotes

1 HM Government, November 2017, *Industrial strategy: building a Britain fit for the future*, www.gov.uk/government/uploads/system/uploads/attachment_data/file/662508/industrial-strategy-white-paper.pdf

2 Cabinet Office, National security and intelligence, HM Treasury, and The Rt Hon Philip Hammond MP (November 2016), *National Cyber Security Strategy 2016 to 2021*, www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

3 Cabinet Office (September 2017), *National risk register of civil emergencies*, www.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

4 Centre for the Protection of National Infrastructure (CPNI) is the government authority for protective security advice to the UK national infrastructure, and it provides advice on physical security: www.cpni.gov.uk/physical-security

5 NCSC (December 2017), *Risk management collection*, www.ncsc.gov.uk/guidance/risk-management-collection

6 HSE (March 2017), *Cyber security for industrial automation and control systems (IACS)*, www.hse.gov.uk/foi/internalops/og/og-0086.pdf

7 Department for Business, Innovation and Skills, April 2014, *Cyber essentials scheme: an overview*

8 NIST Cybersecurity Framework, www.nist.gov/cyberframework

9 NIST, June 2016, Cybersecurity framework feedback: what we heard and next steps, www.nist.gov/sites/default/files/workshop-summary-2016.pdf

10 NIST (revised December 2017), *Framework for improving critical infrastructure cybersecurity*, version 1.1 draft 2, www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf
This version includes a clarification of the use of the Framework to manage cybersecurity within supply chains.

11 European Commission – Digital Single Market policies, The Directive on security of network and information systems (NIS Directive).

12 Royal Academy of Engineering and PETRAS (March 2018), *Internet of Things: realising the potential of a trusted smart world.*

13 NCSC (May 2017), Secure by default, www.ncsc.gov.uk/articles/secure-default. NCSC's secure by default guidance includes a set of principles aimed at product developers to ensure that security is built into a product from the beginning without compromising its usability and without requiring extensive configuration to work.

14 The recent uncovering of security flaws in Intel, ARM and AMD products has meant these companies have had to develop an industry-wide response for addressing the flaws, for example by providing software and firmware updates. Intel (January 2018), *Intel responds to security research findings*, newsroom.intel.com/news/intel-responds-to-security-research-findings/

15 NCSC (January 2018), *Supply chain security collection*, www.ncsc.gov.uk/guidance/supply-chain-security

16 NCSC (January 2018), *Supply chain security collection*, www.ncsc.gov.uk/guidance/supply-chain-security

17 One approach to creating secure systems might be a systems engineering 'v-diagram' approach, enabling the mitigation of security risks to be an integral part of the design of systems. Security must be ensured and assessed at each step, for each component and for its integration into the system.

18 Office for Nuclear Regulation (March 2017), *Security assessment panel for the civil nuclear industry*, www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

19 For example, Altran UK have developed tools for the design and construction of high-integrity systems and software, www.altran.com/uk/en/about-us/what-we-do/expertise-centres/intelligent-systems/

20 In this report, a connected health device is taken to mean any device used for fitness, wellbeing or healthcare purposes that is connected to the internet or another type of network, including the smallest implantable devices, devices for monitoring health or levels of activity, and large-scale medical equipment. The device may or may not fall under medical device regulations.

21 The Wannacry attack in May 2017 led to disruption in at least 34% of trusts in England although the Department of Health and Social Care and NHS England do not know the full extent of the disruption. National Audit Office (October 2017), *Investigation: WannaCry cyber attack and the NHS*, www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

22 The development of national standards for data security by Dame Fiona Caldicott, the National Data Guardian, are aimed at addressing potential risks of data breaches.

23 Wired (November 2015), Medical devices that are vulnerable to life-threatening hacks, www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks

24 Martin, G., Martin, P., Hankin, C., Darzi, A. and Kinross, A. (2017), *Cyber security and healthcare: how safe are we?* BMJ 2017; 358:j3179.

25 NCSC (January 2018), *Supply chain security collection*, www.ncsc.gov.uk/guidance/supply-chain-security

26 NHS Digital plus equivalent organisations in Wales, Scotland and Northern Ireland.

27 NHS Digital plus equivalent organisations in Wales, Scotland and Northern Ireland.

28 Royal Academy of Engineering and IET, November 2015, *Connecting data: driving productivity and innovation*, www.raeng.org.uk/publications/reports/connecting-data-driving-productivity

29 CEBR, February 2016, The value of big data and the internet of things to the UK economy, Report for SAS.

30 Royal Academy of Engineering and IET, November 2015, *Connecting data: driving productivity and innovation*.

31 World Economic Forum, *The global risks report 2016*, 11th Edition, www.weforum.org/reports/the-global-risks-report-2016

32 Cambridge Centre for Risk Studies, Lockheed Martin, January 2016, *Integrated infrastructure: cyber resiliency in society*.

33 UCL and Arup on behalf of the National Infrastructure Commission (November 2017), *Infrastructure and digital systems resilience – final report*, www.nic.org.uk/wp-content/uploads/CCCC17A21-Resilience-of-Digitally-Connected-Infrastructure-Systems-20171121.pdf

34 Royal Academy of Engineering on behalf of Engineering the Future (2011), *Infrastructure, engineering and climate change adaptation – ensuring services in an uncertain future*, www.raeng.org.uk/publications/reports/engineering-the-future

35 FT (August 2016), *Hackers expose holes in in road to smarter cars*, www.ft.com/content/0284ae3c-60cd-11e6-b38c-7b39cbb1138a

36 The Register (December 2017), *Brrr! It's a snow day and someone has pwned the chuffin' school heating*, www.theregister.co.uk/2017/12/12/building_heating_systems_still_hackable/

37 Royal Academy of Engineering and IET, November 2015, *Connecting data: driving productivity and innovation*.

38 Two attacks were reported at the time: Spectre and Meltdown. Meltdown affected only Intel processors, while Spectre affected Intel, ARM and AMD processors. Spectre is harder to mitigate against. meltdownattack.com/

39 Forbes (January 2018), *Intel processor bug leaves all current chips vulnerable and its fix saps performance*, www.forbes.com/sites/davealtavilla/2018/01/03/intel-processor-bug-leaves-all-current-chips-vulnerable-and-its-fix-saps-performance/#17667e0570af

40 Software defects were the cause of the Chinook helicopter accident in 2004. Software defects and a defective safety architecture caused unintended sudden acceleration in Toyota cars, resulting in a law suit in 2013. Presentation by Professor Martyn Thomas CBE FREng at the HSE Conference 2017 on *The Internet of Things: The challenge for health and safety professionals*, www.hse.gov.uk/events/independent-lecture.htm

41 The Times (May 2016), *Glitch in software used by GPs puts thousands on statin alert*, www.thetimes.co.uk/article/software-glitch-puts-thousands-of-heart-patients-on-statin-alert-tbjfdd590

42 See for example, Ofcom, April 2013, *Security and resilience vulnerabilities in the UK's telecoms networks - a review of the risks posed to the regulated telecoms industry by non-deliberate threat*, conducted by BAE Systems Detica on behalf of Ofcom, www.ofcom.org.uk/__data/assets/pdf_file/0027/69273/detica-report.pdf

43 One example of a cyberattack is the 'Stuxnet' attack on an Iranian nuclear plant, first discovered in 2010, where malicious code was targeted at the industrial control system, with the aim of causing damage to equipment and sabotaging operations.

44 In December 2015, floods in Lancaster caused an electricity black-out that in turn disrupted the operation of the internet and mobile phones, as well as other functions such as contactless payment, lifts and petrol pumps, with resulting impact on the community and the local economy. Royal Academy of Engineering, IET and Lancaster University (May 2016), *Living without electricity: One city's experience of coping with loss of power*, www.raeng.org.uk/publications/reports/living-without-electricity

45 FT (June 2017), BA faces £80m cost for IT failure that stranded 75,000 passengers, www.ft.com/content/98367932-51c8-11e7-a1f2-db19572361bb?yptr=yahoo

46 The Scottish Government, November 2015, *Safe, secure and prosperous: a cyber resilience strategy for Scotland*, www.gov.scot/Resource/0048/00489206.pdf

47 Royal Academy of Engineering, March 2011, *Global Navigation Space Systems: reliance and vulnerabilities*, www.raeng.org.uk/publications/reports/global-navigation-space-systems

48 UCL and Arup on behalf of the National Infrastructure Commission (November 2017), *Infrastructure and digital systems resilience – final report*, www.nic.org.uk/wp-content/uploads/CCCC17A21-Resilience-of-Digitally-Connected-Infrastructure-Systems-20171121.pdf

49 The UK government's official definition of CNI is: 'Those critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.' www.cpni.gov.uk/critical-national-infrastructure-0

50 The Internet of Things describes the distributed networks of physical objects that contain sensors and actuators and are connected to the internet or to other communications networks, allowing data about an object or its environment to be generated, shared and acted upon.

51 For example, industrial control systems were used in Crossrail's tunnel ventilation system, www.applied.co.uk/project/crossrail-tunnel-ventilation-system

52 Enisa (December 2016), *Communication network dependencies for ICS/SCADA Systems*.

53 HSE has published operational guidance on the cyber security of industrial control systems, for HSE inspectors and to inform industry: HSE, March 2017, *Cyber security for industrial automation and control systems (IACS)*, www.hse.gov.uk/foi/internalops/og/og-0086.pdf

54 A remote terminal unit provides the interface between physical objects to distributed control system or SCADA (supervisory control and data acquisition) system.

55 A programmable logic controller is a computer that has been adapted for the control of manufacturing processes, such as assembly lines, or robotic devices.

56 Department for Business, Energy and Industrial Strategy (2017), *Made Smarter* review, www.gov.uk/government/publications/made-smarter-review

57 Cambridge Centre for Risk Studies, Lockheed Martin, January 2016, *Integrated infrastructure: cyber resiliency in society*.

58 Langer, R., 2013, *To kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve*.

59 Business Advantage and Kapersky Lab (2017), *The state of industrial cybersecurity 2017 – global report*, go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

60 Royal Academy of Engineering and IET, November 2015, *Connecting data: driving productivity and innovation*.

61 Government Office for Science, December 2014, *The Internet of Things: making the most of the Second Digital Revolution*, A report by the UK Government Chief Scientific Adviser.

62 CEBR, February 2016, Report for SAS, *The value of big data and the internet of things to the UK economy*.

63 European Parliament, May 2015, Briefing on *Internet of Things: opportunities and challenges*, www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

64 Stankovic, J.A., 2014, *Research directions for the Internet of Things*, IEEE Internet of Things Journal (Vol. 1, Issue 1). The author envisions that the steady increasing density of sensing and the sophistication of the associated processing will lead to a significant qualitative change in how we work and live, with systems-of-systems that synergistically interact to form totally new and unpredictable services.

65 National Infrastructure Commission (December 2017), Data for the public good, www.nic.org.uk/wp-content/uploads/Data-for-the-Public-Good-NIC-Report.pdf

66 See for example World Economic Forum (June 2017), *The Internet of Things will power the Fourth Industrial Revolution. Here's how*, www.weforum.org/agenda/2017/06/internet-of-things-will-power-the-fourth-industrial-revolution

67 The Guardian, 25 October 2016, Can we secure the internet of things in time to prevent another cyber-attack? www.theguardian.com/technology/2016/oct/25/ddos-cyber-attack-dyn-internet-of-things

68 A footprint is the size of the computer RAM memory used in an application.

69 RISE, www.ukrise.org

70 Operational technology refers to the hardware and software that controls physical systems.

71 Table 3-1. Summary of IT System and ICS Differences , NIST Special Publication 800-82, Revision 1, May 2013, Guide to Industrial Control Systems (ICS) Security.

72 'Middleware' describes software that serves to 'glue together' separate, often complex, existing, programs.

73 In the *2015 Information Security Breaches Survey* commissioned by HM Government, 50% of organisations attributed the cause of their single worst breach to inadvertent human error.

74 IBM X-Force Research, *2016 Cyber Security Intelligence Index*. This reported that in 2015, 60% of all attacks were carried out by insiders, either ones with malicious intent or those who served as inadvertent actors.

75 IBM X-Force Research, 2017 *X-force threat intelligence index*, This reported that, of the five sectors investigated (financial services, information and communications, manufacturing, retail and healthcare), the healthcare and financial services sectors were particularly prone to attacks by inadvertent actors in 2016 (46% and 53% of attacks, respectively). This is likely to be as a result of phishing schemes and indicates that education of employees is vital.

76 A patch is an update to a piece of software that is introduced in order to fix or improve the software.

77 29% of ICS-CERT 2014 and 2015 incidents would potentially have been mitigated by proper configuration/patch management. 77 US Department of Homeland Security and the National Cybersecurity and Communications Integration Centre, December 2015, *Seven Strategies to Defend ICSs*. The Cyber Essentials scheme advocates as a key principle that organisations keep their devices and software up to date through patching: www.cyberessentials.ncsc.gov.uk/advice

78 Safety Critical Systems Club – The Data Safety Initiative Working Group (2017), *Data safety guidance version 2.0*, SCSC – 127B,

79 For example, these approaches allow enterprise architects to create 'sticky policies' for protected data, controlling access to data by incorporating attributes such as the user identity, device identity, location, time-limited attributes and read/write data access controls.

80 Prime Minister's Office and others, November 2015, *National security strategy and strategic defence and security review 2015*.

81 Ibid.

82 Cabinet Office, April 2016, *The UK Cyber Security Strategy 2011–2016 Annual Report*.

83 Cabinet Office, National security and intelligence, The Rt Hon Philip Hammond MP and HM Treasury, *National Cyber Security Strategy 2016 to 2021*, www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

84 The Cyber Schools Programme, launched in February 2017, aims to train nearly 6,000 young people in cybersecurity, www.gov.uk/guidance/cyber-schools-programme

85 See for example: DCMS, July 2016, Digital Economy Minister co-chairs first Cyber Growth Partnership meeting, www.gov.uk/government/news/digital-economy-minister-co-chairs-first-cyber-growth-partnership-meeting

86 UK-based companies such as ARM Ltd. are already market-leaders in developing cyber security technologies. See for example: www.businessweekly.co.uk/news/hi-tech/arm-group-builds-armour-shield-iot-cyber-raids

87 The Cyber Accelerator programme, launched in September 2016, provides startups with access to world-class experts to help them build cutting-edge technology. www.gov.uk/government/news/groundbreaking-partnership-between-government-and-tech-start-ups-to-develop-world-leading-cyber-security-technology

88 DCMS (July 2017), Major new cybersecurity innovation centre for London, www.gov.uk/government/news/major-new-cyber-security-innovation-centre-for-london

89 NCSC, Academic Centres of Excellence in Cyber Security Research, February 2017, www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research

90 NCSC, (February 2016), Research institutes, www.ncsc.gov.uk/information/research-institutes

91 RITICS: Research Institute in Trustworthy Industrial Control Systems, www.ritics.org

92 Cabinet Office, DCMS, NCSC and Caroline Nokes MP (November 2017), *Interim cybersecurity science and technology strategy: future-proofing cybersecurity*, www.gov.uk/government/publications/interim-cyber-security-science-and-technology-strategy

93 European Commission, (July 2016), The Directive on security of network and information systems (NIS Directive), https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

94 European Commission (2017), *Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505297631636&uri=COM:2017:476:FIN

95 DCMS and the Rt Hon Matt Hancock MP, (December 2016), Cybersecurity incentives and regulation review.

96 DCMS, (September 2017), www.gov.uk/government/collections/data-protection-bill-2017

97 DCMS and the Rt Hon Matt Hancock MP, (December 2016), Cybersecurity incentives and regulation review.

98 HM Government, (November 2017), *Industrial strategy: building a Britain fit for the future*, www.gov.uk/government/uploads/system/uploads/attachment_data/file/662508/industrial-strategy-white-paper.pdf

99 CESG, part of GCHQ, is the UK government's national technical authority for information assurance.

100 CERT UK is the UK's national Computer Emergency Response Team.

101 18 March 2016, New National Cyber Security Centre set to bring UK expertise together, www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together

102 NCSC, Cyber Essentials, www.cyberessentials.ncsc.gov.uk

103 NCSC (November 2017), A brief history of Cyber Essentials, www.cyberessentials.ncsc.gov.uk/2017/11/27/The-NCSC-and-Cyber-Essentials.html

104 NCSC (February 2017), Operational technologies, www.ncsc.gov.uk/guidance/operational-technologies

105 NCSC (August 2017), Risk management collection, www.ncsc.gov.uk/guidance/risk-management-collection

106 Centre for the Protection of National Infrastructure, (2015), *Security for industrial control systems*, www.ncsc.gov.uk/guidance/security-industrial-control-systems

107 ENISA, (December 2011), *Protecting industrial control systems: recommendations for Europe and member states*.

108 US Department of Homeland Security and the National Cybersecurity and Communications Integration Centre, (December 2015), *Seven Strategies to Defend ICSs*.

109 U.S. Department of Commerce and NIST, (May 2015), NIST Special Publication 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*.

110 NIST cybersecurity framework, launched February 2014, www.nist.gov/cyberframework

111 US Department of Energy and US Department of Homeland Security, (February 2014), Cybersecurity capability maturity model, Version 1.1, https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

112 DfT, CPNI and Centre for Connected and Autonomous Vehicles (August 2017), The Key Principles of Cybersecurity for Connected and Automated Vehicles, www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

113 ENISA (December 2016), Cybersecurity and resilience of smart cars – good practices and recommendations, www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

114 National Highway Traffic Safety Administration (October 2016), Cybersecurity best practices for modern vehicles. Report No. DOT HS 812 333.

115 Department for Transport (February 2016), Rail cybersecurity: guidance to industry, www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf

116 Rail Industry Cyber Security Assurance Group, Cyber Security Assurance Principles, Issue 7, November 2016.

117 Office for Nuclear Regulation (2017), Security Assessment Principles for the Civil Nuclear Industry, v1.0, www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

118 Bank of England, Financial sector continuity: cyber resilience, www.bankofengland.co.uk/financial-stability/financial-sector-continuity

119 European Commission (September 2017), *Resilience, deterrence and defence: building strong cybersecurity for the EU*, JOIN (2017) 450 final, ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF

120 Betanews, US senators reveal bipartisan effort to secure IoT devices, betanews.com/2017/08/03/us-senators-reveal-bipartisan-effort-to-secure-iot-devices/

121 115th Congress, 1st Session (Bill introduced January 2017), *To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes*, assets.documentcloud.org/documents/3911338/Internet-of-Things-Cybersecurity-Improvement-Act.pdf

122 Two such examples are: The Offshore Installations (Offshore Safety Directive) (Safety Case etc.) Regulations 2015, www.legislation.gov.uk/uksi/2015/398/contents/made, and Regulatory Article (RA) 1205: air system safety cases, www.gov.uk/government/publications/regulatory-article-ra-1205-air-system-safety-cases

123 The Health Foundation (December 2012), *Using safety cases in industry and healthcare*.

124 ALARP means 'as low as reasonably practicable'. See for example HSE website: ALARP is about 'making sure a risk has been reduced ALARP is about weighing the risk against the sacrifice needed to further reduce it', www.hse.gov.uk/risk/theory/alarpglance.htm

125 Royal Academy of Engineering and IET (November 2015), *Connecting data: driving productivity and innovation*, Section 5.3: Legislation around data and software.

126 Product liability laws apply to consumer goods and to goods used in the workplace, and require that products must not cause injury or damage to private property.

127 Royal Academy of Engineering, IET and Lancaster University (May 2016), *Living without electricity: One city's experience of coping with loss of power*, www.raeng.org.uk/publications/reports/living-without-electricity

128 Cabinet Office (March 2016), *National Risk Register for Civil Emergencies – 2015 edition*, www.gov.uk/government/publications/national-risk-register-for-civil-emergencies-2015-edition. This document distinguishes between 'risks of terrorist and other malicious attacks' and 'other risks' that may still have a high impact, such as major industrial accidents or widespread electricity failure.

129 Cabinet Office, May 2016, Summary of the 2015-16 sector resilience plans, www.gov.uk/government/publications/sector-resilience-plan-2015-to-2016

130 CPNI – policy context, www.cpni.gov.uk/cpni-context

131 UKRN (April 2015), Cross-sector resilience – phase 1 report, www.ukrn.org.uk/wp-content/uploads/2016/07/2015AprCSR-Phase1Report.pdf

132 House of Lords Science and Technology Select Committee (March 2015), First Report of Session 2014–15, *The Resilience of the Electricity System*, www.publications.parliament.uk/pa/ld201415/ldselect/ldsctech/121/121.pdf

133 National Grid, Black Start, www2.nationalgrid.com/uk/services/balancing-services/system-security/black-start/

134 Ofcom (April 2013), *Security and resilience vulnerabilities in the UK's telecoms networks - a review of the risks posed to the regulated telecoms industry by non-deliberate threat*, conducted by BAE Systems Detica on behalf of Ofcom.

135 UKRN (April 2015), Cross-sector resilience – phase 1 report.

136 Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, Brussels, 7.2.2013, COM(2013) 48 final

137 Ponemon Institute (June 2016), *2016 Cost of Data Breach Study: United Kingdom*.

138 Cambridge Centre for Risk Studies, Lockheed Martin, January 2016, *Integrated infrastructure: cyber resiliency in society*.

139 CPNI, June 2017, *Mitigating security risk in the national infrastructure supply chain: a good practice guide for employers*, www.cpni.gov.uk/advice/Personnel-security1/Security-in-the-Supply-Chain/

140 RSSB, Supplier assurance programmes, www.rssb.co.uk/improving-industry-performance/supplier-assurance-programme

141 Lloyd's Register Foundation and The Alan Turing Institute (September 2017), *Distributed ledger technologies: safety of engineering systems*, Insight Report No. 2017.4.

142 The size and competitiveness of the market means that Apple and Google have a strong incentive to create this security ecosystem, which includes a licencing regime that requires phone handset makers to provide updates, checking of software by static analysers, covert surveillance using anti-virus scanners, tracking of organisations that have shipped insecure apps, a strong security team, blogs, feedback from security researchers and a bounty programme.

143 Presentation by Professor Martyn Thomas CBE FREng at the HSE Conference 2017 on *The Internet of Things: The challenge for health and safety professionals*, www.hse.gov.uk/events/independent-lecture.htm

144 BSIMM is the 'Building Security In Maturity Model' that quantify the activities carried out by real software security initiatives to help the wider software security community plan, carry out, and measure initiatives of their own. www.bsimm.com/about.html

145 NCSC (January 2018), *Supply chain security collection*, www.ncsc.gov.uk/guidance/supply-chain-security

146 Insurance requires consideration of how to value and protect assets.

147 Department for Business, Innovation and Skills (2014), Cyber essentials scheme, www.gov.uk/government/publications/cyber-essentials-scheme-overview

148 CESG, Cabinet Office, CPNI and Department for Business, Innovation and Skills (2012, updated 2015) *Ten steps to cybersecurity*, www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

149 CESG, Cabinet Office, CPNI and Department for Business, Innovation and Skills (2014) *Common cyber attacks: reducing the impact*, www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

150 See for example: *HAT: Hub-of-all-things – Platform for multi-sided market powered by Internet of Things* where best common practice is defined contractually.

151 Building Information Modelling (BIM) Task Group, *PAS 1192-5:2015 - Specification for security-minded building information modelling, digital built environments and smart asset management*, https://thebimhub.com/2015/06/01/pas-1192-5-overview/

152 HSE, *Cybersecurity for industrial automation and control systems (IACS)*, Note 4 in Appendix 1 page 12 of the guidance gives an approach to risk assessment. Appendix 3 gives a generic example of risk assessment, www.hse.gov.uk/foi/internalops/og/og-0086.pdf

153 For example, Note 2 in Appendix 1 of HSE, *Cybersecurity for industrial automation and control systems (IACS)*. More detailed guidance can be found in IEC 62443-2-1 and 2-2. Guidance on general management systems can be found in IEC 61511 and HSE guidance HSG65, *Managing for Health and Safety*, www.hse.gov.uk/pubns/books/hsg65.htm

154 In May 2016, the Engineering Council published guidance for engineers and technicians on their role in dealing with security, www.engc.org.uk/security

155 (April 2016), *Shadbolt Review of Computer Sciences Degree Accreditation and Graduate Employability*

156 IET, Cybersecurity skills alliance, www.theiet.org/policy/key-topics/cyber-security/skills-alliance.cfm

157 For example, Cyber Security Challenge UK runs programmes that are aimed at schoolchildren and those in further and higher education, www.cybersecuritychallenge.org.uk/education

158 CyberFirst is a student scheme led by NCSC which aims to support and prepare undergraduates for a career in cybersecurity, www.gchq-careers.co.uk/early-careers/cyberfirst.html

159 Leverett, E., Clayton, R. and Anderson, R. (May 2017), *Standardisation and certification of the 'Internet of Things'*, www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf. This paper examines the need for regulators to embrace both safety and security, and describes the challenges in a European context.

160 Directive 2007/46/EC that is currently under review to make vehicle testing more independent and to increase surveillance of cars already in circulation. ec.europa.eu/growth/sectors/automotive/technical-harmonisation/eu_en

161 VCA, Type approval for cars, www.dft.gov.uk/vca/vehicletype/type-approval-for-ca.asp. VCA is the designated UK Vehicle Type Approval authority and provides testing and certification for vehicles, their systems and components.

162 Presentation by Professor Martyn Thomas CBE FREng at the HSE Conference 2017 on *The Internet of Things: The challenge for health and safety professionals*, www.hse.gov.uk/events/independent-lecture.htm

163 For example, there are conflicts between the EU Directives for telecoms and cars, and between the EU Directives for telecoms and medical devices. European Commission, Telecoms rules: ec.europa.eu/digital-single-market/en/telecoms-rules; European Commission, Medical devices – regulatory framework: ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en

164 For example, companies may produce wellness wearables rather than healthcare wearables to avoid the new EU Medical Devices Directive.

165 Leverett, E., Clayton, R. and Anderson, R. (May 2017), *Standardisation and certification of the 'Internet of Things'*, www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

166 ENISA (September 2017), *European Commission proposal on a Regulation of the European Parliament and of the Council on the future of ENISA: Proposal for a new Regulation for a stronger ENISA, the EU Cybersecurity Agency!*, www.enisa.europa.eu/news/enisa-news/european-commission-proposal-on-a-regulation-on-the-future-of-enisa

167 CEPS (July 2017), *Software Vulnerabilities Disclosure: The European landscape*, www.ceps.eu/publications/software-vulnerabilities-disclosure-european-landscape

168 The Health Foundation (December 2012), Using safety cases in industry and healthcare: A pragmatic review of the use of safety cases in safety-critical industries – lessons and prerequisites for their application in healthcare, www.health.org.uk/sites/health/files/UsingSafetyCasesInIndustryAndHealthcare.pdf

169 Royal Academy of Engineering and The Academy of Medical Devices (June 2013), *Establishing high-level evidence for the safety and efficacy of medical devices and systems*, www.raeng.org.uk/publications/reports/establishing_high_level_evidence

170 Bird and Bird, 20 July 2016, *Germany takes the next step to self-driving cars.*

171 HSE, *Health and Safety at Work etc Act 1974*, www.hse.gov.uk/legislation/hswa.htm

172 NCSC (August 2016), *Password guidance – simplifying your approach*, www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

173 NCSC (October 2017), *Avoiding phishing attacks*, www.ncsc.gov.uk/guidance/avoiding-phishing-attacks

174 For example, Hollnagel, E. (2014), *Safety-I and Safety-II: The past and future of safety management*, Farnham, UK: Ashgate, and Hollnagel, E. (2017), *Safety-II in practice: developing the resilience potentials*, Taylor & Francis.

175 Ashenden, D. and Lawrence, D. (2013), *Can we sell security like soap?: a new approach to behaviour change*, In Proceedings of the 2013 New Security Paradigms Workshop (pp. 87-94), ACM.

176 Kirlappos, I. and Sasse, M.A (2015), *Fixing security together: leveraging trust relationships to improve security in organizations*, Procs USEC 2015, https://iris.ucl.ac.uk/iris/publication/1011222/1

177 Reason, J. (2008), *The human contribution: unsafe acts, accidents and heroic recoveries.*

178 Formal descriptions of software or hardware can be used to guide development activities and to verify that the requirements for the system being developed have been completely and accurately specified. Once a formal specification has been developed, a process of verification can be used to prove the properties of the specification and the developed system.

179 Functional programming is a technique used by programmers to create well-structured software that is easy to write and de-bug. Its suitability will depend on the application.

180 Engineering design and development methods include configuration management – a systems engineering process - and release management – a discipline from software engineering.

181 iFACTS is a predictive tool for air traffic controllers that helps to increase capacity and improve safety. See for example: www.nats.aero/news/nats-scoops-prestigious-award-at-industry-showcase/

182 For example, Cardian, a spin-out from Imperial College, is developing a novel implantable device that improves the monitoring and treatment of cardiac failure patients, by providing completely automated, continuous wireless monitoring of blood pressure in the pulmonary artery.

183 For example, Drayson Health is developing GDm-health, a system for the management of diabetes in pregnant women that enable secure and remote communication between patient and care provider, reducing the number of clinic visits, draysontechnologies.com/gdm-health.html

184 For example, Leman Micro Devices is developing a sensor and software in a smart phone to measure blood pressure, heart rate, respiration rate, blood oxygen and non-contact body temperature, www.leman-micro.com

185 Wellbeing can be monitored using a range of devices including smart watches and mobile phones, with the relevant apps, as well as bespoke fitness trackers such as Fitbits or Misfits.

186 For example, the health insurance provider Vitality offers rewards for customers based on their level of activity as measured by a range of approved tracking devices: www.vitality.co.uk/rewards/partners/activity-tracking/

187 Presentation by Professor Chris Hankin at the Academy connected health devices workshop, July 2017.

188 Hardware and software designed to meet the needs of an organisation that has traditionally been separate from the hardware and software used to monitor and control physical devices and processes.

189 Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF

190 Regulation (Eu) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745&from=EN

191 ISO 14971 is the ISO standard for the application of risk management to medical devices.

192 IEC 62304 is the international standard (medical device software – software life cycle processes) that specifies life cycle requirements for the development of medical software and software within medical devices.

193 Data Protection Directive 95/46, ePrivacy Directive 2002/58, General Data Protection Regulation 2016/679.

194 FDA is the US Food and Drug Administration, www.fda.gov

195 FDA Cybersecurity of medical devices, www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

196 FDA Postmarket requirements (devices), www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/default.htm

197 Health Insurance Portability and Accountability Act (HIPAA). The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information.

198 Point-of-care testing allows medical diagnostic testing to occur at the time and place of the patient.

199 For example, Leman Micro Devices will incorporate medically-accurate health monitoring sensors into smartphones and will meet international medical device standards, www.leman-micro.com

200 *Health apps: regulation and quality control* (November 2014), Summary of a joint meeting hosted by the Academy of Medical Sciences and the Royal Academy of Engineering. www.raeng.org.uk/publications/reports/health-apps-regulation-and-quality-control

201 NHS Improvement, Patient safety, https://improvement.nhs.uk/improvement-hub/patient-safety/

202 A type of quality label that provides a way of making visible the level of cyber security.

203 NCSC (September 2016), Guidance on protecting bulk personal data, www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main

204 Homeland Security and NCCIC, *Seven Strategies to Defend ICSs*, https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

205 NCSC is funding research on developer-centred security.

206 Presentation by Professor Harold Thimbleby at the RAEng workshop on connected health devices, July 2017.

207 Faculty of Clinical Informatics, www.facultyofclinicalinformatics.org.uk

ROYAL ACADEMY OF ENGINEERING

Royal Academy of Engineering

As the UK's national academy for engineering, we bring together the most successful and talented engineers for a shared purpose: to advance and promote excellence in engineering.

We have four strategic challenges:

Make the UK the leading nation for engineering innovation

Supporting the development of successful engineering innovation and businesses in the UK in order to create wealth, employment and benefit for the nation.

Address the engineering skills crisis

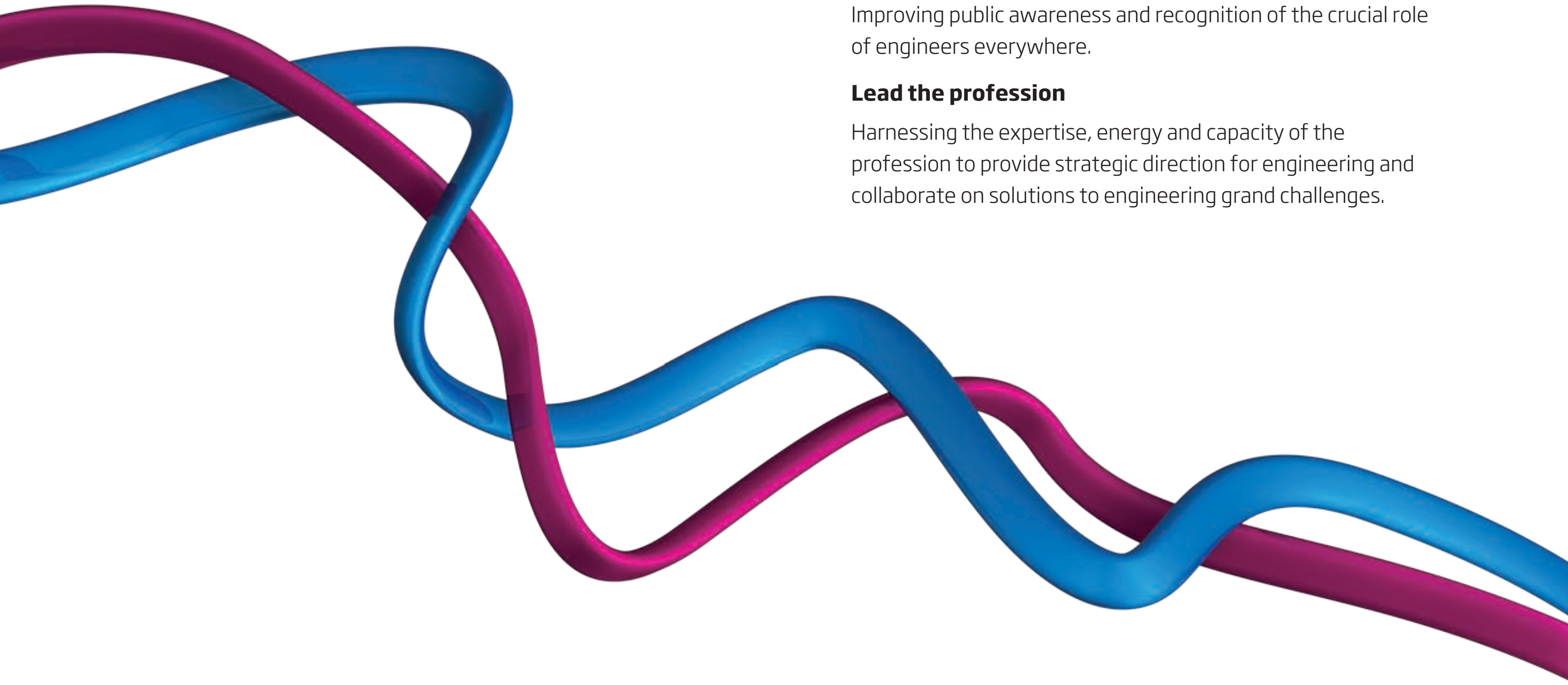
Meeting the UK's needs by inspiring a generation of young people from all backgrounds and equipping them with the high quality skills they need for a rewarding career in engineering.

Position engineering at the heart of society

Improving public awareness and recognition of the crucial role of engineers everywhere.

Lead the profession

Harnessing the expertise, energy and capacity of the profession to provide strategic direction for engineering and collaborate on solutions to engineering grand challenges.



Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG

Tel: +44 (0)20 7766 0600
www.raeng.org.uk

Registered charity number 293074

This brochure can be recycled.