Progress and research in cybersecurity

Supporting a resilient and trustworthy system for the UK

THE
ROYAL
SOCIETY

Progress and research in cybersecurity: Supporting a resilient and trustworthy system for the UK
Issued: July 2016 DES3800
ISBN: 978-1-78252-215-7

The text of this work is licensed under the terms of the Creative Commons Attribution License which permits unrestricted use, provided the original author and source are credited.

The license is available at:
creativecommons.org/licenses/by/4.0

Images are not covered by this license.

This report can be viewed online at
royalsociety.org/cybersecurity

Cover image
© mustafahacalaki.

Contents

Chapter four – Research 44

Chapter five – Translation 55

Appendices 60

Executive summary

Digital systems have transformed, and will continue to transform, our world. Supportive government policy, a strong research base and a history of industrial success make the UK particularly well-placed to realise the benefits of the emerging digital society. These benefits have already been substantial, but they remain at risk. Protecting the benefits and minimising the risks requires reliable and robust cybersecurity, underpinned by a strong research and translation system.

Trust is essential for growing and maintaining participation in the digital society. Organisations earn trust by acting in a trustworthy manner: building systems that are reliable and secure, treating people, their privacy and their data with respect, and providing credible and comprehensible information to help people understand how secure they are.

Resilience, the ability to function, adapt, grow, learn and transform under stress or in the face of shocks, will help organisations deliver systems that are reliable and secure. Resilient organisations can better protect their customers, provide more useful products and services, and earn people's trust.

Research and innovation in industry and academia will continue to make important contributions to creating this resilient and trusted digital environment. Research can illuminate how best to build, assess and improve digital systems, integrating insights from different disciplines, sectors and around the globe. It can also generate advances to help cybersecurity keep up with the continued evolution of cyber risks.

Translation of innovative ideas and approaches from research will create a strong supply of reliable, proven solutions to difficult to predict cybersecurity risks. This is best achieved by maximising the diversity and number of innovations that see the light of day as products.

Policy, practice and research will all need to adapt. The recommendations made in this report seek to set up a trustworthy, self-improving and resilient digital environment that can thrive in the face of unanticipated threats, and earn the trust people place in it.

Innovation and research will be particularly important to the UK's economy as it establishes a new relationship with the European Union. Cybersecurity delivers important economic benefits, both by underpinning the digital foundations of UK business and trade and also through innovation that feeds directly into growth. The findings of this report will be relevant regardless of how the UK's relationship to the EU changes.

HEADLINE RECOMMENDATIONS

- **Trust** Governments must commit to preserving the robustness of encryption, including end-to-end encryption, and promoting its widespread use. Encryption is a foundational security technology that is needed to build user trust, improve security standards and fully realise the benefits of digital systems.

- **Resilience** Government should commission an independent review of the UK's future cybersecurity needs, focused on the institutional structures needed to support resilient and trustworthy digital systems in the medium and longer term. A self-improving, resilient digital environment will need to be guided and governed by institutions that are transparent, expert and have a clear and widely-understood remit.

- **Research** A step change in cybersecurity research and practice should be pursued; it will require a new approach to research, focused on identifying ambitious high-level goals and enabling excellent researchers to pursue those ambitions. This would build on the UK's existing strengths in many aspects of cybersecurity research and ultimately help build a resilient and trusted digital sector based on excellent research and world-class expertise.

- **Translation** The UK should promote a free and unencumbered flow of cybersecurity ideas from research to practical use and support approaches that have public benefits beyond their short term financial return. The unanticipated nature of future cyber threats means that a diverse set of cybersecurity ideas and approaches will be needed to build resilience and adaptivity. Many of the most valuable ideas will have broad security benefits for the public, beyond any direct financial returns.

Detailed recommendations

CHAPTER TWO – TRUST

RECOMMENDATION 1

Governments must commit to preserving the robustness of encryption, including end-to-end encryption, and promoting its widespread use.

RECOMMENDATION 2

The Government should go further to establish and promote rigorous, evidence-based guidance on state of the art cybersecurity principles, standards and practices, accompanied by certification marks or benchmarks for digital products and services, focused on improving consumers' protection and understanding.

- The identification of rigorous, evidence-based benchmarking and evaluation standards for cybersecurity, how best to structure those standards, and how best to communicate them to users should be informed by existing and future research.

- Review processes for evaluating privacy preservation methods should be established, including anonymisation techniques (for releasing or providing access to data) and anonymous communications.

CHAPTER THREE – RESILIENCE

RECOMMENDATION 3

The Government should commission an independent review of the UK's future cybersecurity needs, focused on the institutional structures needed to support resilient and trustworthy digital systems in the medium and longer term.

- The Government has recently moved to consolidate a range of cybersecurity functions into a single new institution, the National Cyber Security Centre (NCSC). The review should work with those establishing the Centre and determining its programmes, to ensure that it has the capacity and incentives to deliver the requirements outlined in this report, and that there is continuing informed and open discussion about its role and ways of working. The independent review should be timed to take account of the experience of the new NCSC.

- The National Cyber Security Centre represents a helpful and important improvement in the UK's institutional arrangements for cybersecurity. However, the Centre will report in to the Government Communications Headquarters (GCHQ). Based on the trends and evidence available today this arrangement is unlikely to be ideal in the longer term, when digital systems will be embedded increasingly deeply across society and an increasingly large proportion of uses will be commercial and personal. The review should therefore also look 5 – 10 years into the future, to develop options for future governance arrangements that will better reflect the future distributions of benefits and harms across society.

RECOMMENDATION 4

The incentives for organisations to adhere to rigorous, evidence-based cybersecurity standards should be strengthened.

- Publicly listed companies and public bodies, including Government departments, should benchmark their adherence against cybersecurity standards, and regularly report on this.

- Changes to legal liability for cybersecurity failures should be considered.

- Publicly listed companies and public bodies may in future be required to report cybersecurity breaches to an appropriate coordinating body, under the EU General Data Protection Regulation, if the regulation is implemented in the UK. The identity and characteristics of any coordinating body should be in line with the requirements identified in Recommendation 3.

- The Government should build on existing initiatives to encourage organisations to report cybersecurity attacks and vulnerabilities to an appropriate coordinating body.

- Research is needed to ensure information sharing mechanisms for cybersecurity breaches and vulnerabilities remain effective and continue to improve.

- Research and innovation in cyber-physical system development should be further prioritised to mitigate the substantial risks these systems introduce. It is particularly urgent to increase the standards of cybersecurity practice for critical national infrastructure.

CHAPTER FOUR – RESEARCH

RECOMMENDATION 5

The Government and research funders should introduce new funding and management structures for an ambitious, challenge-led research funding organisation, focusing on cybersecurity in the first instance. This organisation would identify key challenges and provide flexible support for excellent researchers to tackle them, with a presumption of unencumbered access to the solutions.

RECOMMENDATION 6

Research Councils and other research funders must draw effectively on world-class expertise. Research funders should go further to: ensure peer review involves the best expertise available internationally; encourage multidisciplinary research in cybersecurity; encourage international research collaboration with competent parties; and reduce barriers to academic researchers engaging with industry and the public sector.

CHAPTER FIVE – TRANSLATION

RECOMMENDATION 7

The Government should promote the creation and uptake of real-world test facilities, including data sets that can be accessed and shared as a national resource to allow the robust evaluation of new cybersecurity research and products.

RECOMMENDATION 8

The Government should expand the engagement of SMEs and academic researchers with industrial partners through procurement mechanisms, including the Small Business Research Initiative.

RECOMMENDATION 9

The Government should establish one or more further dedicated support funds under specialised and professional management to support the financing of cybersecurity innovation, targeting cases where innovation would have spillover benefits but might not otherwise be funded.

RECOMMENDATION 10

Universities and their technology transfer offices should focus on the volume of commercialisation opportunities, recognising the difficulty of predicting the success of cybersecurity initiatives, and taking into account broader benefits beyond the expected financial return.

Chapter one
Cybersecurity and the digital society

Cybersecurity and the digital society

1.1 Digital technologies are transforming society and creating complexities in the process

Digital technologies have transformed how people socialise, shop, interact with government and do business. The Internet and World Wide Web have made vast amounts of information instantly available, and smartphones have put it at our fingertips everywhere we go. Our interaction with the physical world is now being transformed by the Internet of Things. As many as 15 billion devices[1] are already online; estimates for 2020 range from 26 billion[2] to 50 billion[3]. Data storage is increasingly shifting to the Cloud, increasing its availability and usefulness; but also increasing complexity.

Digital systems are complex[4] because of their large and distributed nature, their many subsystems and interconnections, and the mix of human, legal, regulatory and technological elements involved. The scale and interactions of these systems make their outcomes and risks very difficult to predict. The gains and losses that occur are often unanticipated, while predicted outcomes may fail to materialise.

This complexity and growth also create asymmetries between attackers and their targets, and incentives that drive underinvestment in cybersecurity[5]. Many of the systems underpinning today's networks were not designed with security in mind. As a result, current cybersecurity practice lags behind rigorous, evidence-based standards of engineering. This leaves digital systems vulnerable, both to emerging risks and to risks that are already well understood.

Digital systems are already central to our security, wellbeing and growth, but the threats are constantly growing and evolving. Cybersecurity tools, processes and institutions need to catch up and keep up.

[1] Macaulay, J., Buckalew, L., Chung, G. 2015 *The Internet of Things in Logistics. Troisdorf*, Germany: DHL and Cisco. (See http://www.dpdhl.com/content/dam/dpdhl/presse/pdf/2015/DHLTrendReport_Internet_of_things.pdf, accessed 24 April 2016).

[2] Gartner 2013 *Forecast: The Internet of Things, Worldwide*. (See http://www.gartner.com/newsroom/id/2636073, accessed 24 April 2016).

[3] Macaulay, J., Buckalew, L., Chung, G. 2015 *The Internet of Things in Logistics. Troisdorf*, Germany: DHL & Cisco. (See http://www.dpdhl.com/content/dam/dpdhl/presse/pdf/2015/DHLTrendReport_Internet_of_things.pdf, accessed 24 April 2016).

[4] Armstrong, R., Mayo, J., Siebenlist F., 2009 *Complexity Science Challenges in Cybersecurity*. (See http://sendsonline.org/wp-content/uploads/2011/02/DOE-Complexity-Whitepaper-2009.pdf, accessed 24 April 2016).

[5] Asghari, H., van Eeten, M. and Bauer, J.M., 2016. 13. Economics of cybersecurity. *Handbook on the Economics of the Internet*, p.262.

1.2 Digital systems' importance will continue to grow and to evolve in nature

Digital industries grew 32 per cent faster than the rest of the UK's economy between 2010 and 2014. Employment in the sector grew 2.8 times faster than in other sectors[6]. Internet banking is used by 56 per cent of adults in the UK, nearly doubling since 2007[7].

The UK is already among the world's most connected societies. In 2014 the digital economy represented 7 per cent of the UK's economy, 9 per cent of all businesses and 5 per cent of employment[8]. In 2015, 86 per cent of households were connected to the Internet, 76 per cent of people made an online purchase, and 74 per cent of people connected to the Internet from a mobile device[9]. Digital systems and products will become even more important as they continue to grow and evolve. Their adoption has grown rapidly over the last two decades and, in the absence of severe shocks, this growth will continue.

As adoption grows, the nature and effects of these digital systems will continue to change. The integration of digital and physical systems is connecting our infrastructure, automating our vehicles and interconnecting our domestic appliances[10]. Machine learning[11] technologies that augment or replace human decision-making are changing what we are shown online, how services are delivered to us, and how we interact with technology. These developments have large potential benefits, but also create new risks and challenges, including around agency and liability.

1.3 The UK is in a strong position to continue to benefit from the digital society

Supportive government policy, a strong research base and a history of industrial success make the UK particularly well-placed to realise the benefits. Government policy has committed the UK to unlocking the commercial and societal potential of open data[12], and government now publishes large amounts of data about crime, education, health, justice and other public services. Government service delivery and communications are also being transformed. In 2011, the UK Government created the Government Digital Service to improve its service delivery and information provision.

[6] Tech City UK & Nesta 2016 *Tech Nation 2016: Transforming UK Industries*. London: Tech City UK & Nesta (See http://www.techcityuk.com/wp-content/uploads/2016/02/Tech-Nation-2016_FINAL-ONLINE-1.pdf, accessed 26 April 2016).

[7] Office for National Statistics 2015 *Internet Access – Households and Individuals 2015*. (See http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06, accessed 26 April 2016).

[8] Rhodes, C., Rathbone D. 2016 *Digital economy: statistics and policy* (See http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7610, accessed 10 June 2016).

[9] Office for National Statistics 2015 *Internet Access – Households and Individuals 2015*. (See http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06, accessed 26 April 2016).

[10] Government Office for Science 2014 *Internet of things: making the most of the second digital revolution*. (See https://www.gov.uk/government/publications/internet-of-things-blackett-review, accessed 10 June 2016).

[11] Machine learning is an approach to computer programming, which creates algorithms that learn from data and self-improve.

[12] Cabinet Office 2012 *Open Data White Paper: Unleashing the Potential*. London: Cabinet Office. (See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78946/CM8353_acc.pdf, accessed 26 April 2016).

The UK has a strong track record of research success, illustrated by the pioneering work of Alan Turing FRS in mathematics and early computing[13] and code-breaking achievements during World War II. In the decades following, Tom Kilburn FRS led the development of a series of historically significant computers, including the first stored program computer (the Manchester Small-Scale Experimental Machine, or Baby)[14]. Sir Maurice Wilkes FRS FREng subsequently made stored program computing usable in practice for the first time through the development of EDSAC[15] at Cambridge. In the 1980s, Steve Furber FRS FREng and Sophie Wilson FRS FREng developed the original ARM processor architecture and instruction set[16], the foundations for one of the most successful pieces of modern computer hardware.

UK researchers have also shaped computer networking. Donald Davies FRS helped enable modern network communications through his ten years of pioneering work on packet switching at the National Physical Laboratory[17]. He went on to work on data security and encryption, including for the financial sector. In the late 1980s, Sir Tim Berners-Lee FRS FREng contributed a central piece of today's digital world by inventing the World Wide Web at CERN[18].

Many of these successes have also fed into industrial success. ARM processors are used in most mobile devices[19], while UK researchers have made major contributions to the encryption algorithms, key management schemes and hardware underpinning ATM networking and payment systems[20], as well as the authentication technologies that enable mobile telephony[21].

The UK must reinforce and build on these strong digital foundations.

[13] Newman, M 1955 *Alan Mathison Turing*. 1912-1954. Biographical Memoirs of Fellows of the Royal Society. London: Royal Society.

[14] Wilkes, M. and Kahn, H.J., 2003. *Tom Kilburn CBE FREng. 11 August 1921–17 January 2001*. Biographical Memoirs of Fellows of the Royal Society, 49, pp.283-297.

[15] The Electronic Delay Storage Automatic Calculator – the first practical computer to store data and instructions in memory, rather than having separate, more specialised mechanisms for program instructions.

[16] Garnsey, E., Lorenzoni, G. and Ferriani, S., 2008. *Speciation through entrepreneurial spin-off: The Acorn-ARM story*. Research Policy, 37(2), pp.210-224.

[17] Needham, R. 2002 *Donald Watts Davies, C.B.E. 7 June 1924 – 28 May 2000*. Biographical Memoirs of Fellows of the Royal Society (DOI: 10.1098/rsbm.2002.0006).

[18] Berners-Lee, T., Fischetti, M., 2000. *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor*. HarperInformation.

[19] Chu, J. quoted in Bent, K. 2012, *ARM Snags 95 Percent Of Smartphone Market, Eyes New Areas For Growth*. (See http://www.crn.com/news/components-peripherals/240003811/arm-snags-95-percent-of-smartphone-market-eyes-new-areas-for-growth.htm, accessed on 10 June 2016).

[20] Beker, H.J., 2000. *Mathematics at Work—A Perspective on the Development of Cryptography over the Last Twenty-Five Years*. Measurement and Control, 33(5), pp.132-137.

[21] Walker, M., Wright, T. 2001 *Security in GSM and UMTS: The Creation of Global Mobile Communication* (ed F. Hillebrand), Chichester, UK: John Wiley & Sons, Ltd. (DOI: 10.1002/0470845546.ch15).

1.4 Cybersecurity is central to the task, but faces a unique set of challenges

Despite the UK's strong starting position, the benefits from digital systems remain at risk. Vulnerabilities remain widespread, attacks are increasing, and breaches cause substantial harm to individuals and businesses. Digital systems will face more threats as they become more complex, and as the pay-offs to attackers increase. Research, policy and practice all have a role to play in protecting against these threats; each faces challenges that are distinctive to cybersecurity[22].

Cybersecurity is inherently multidisciplinary, needing to take account both of deeply technical and often mathematical insights, and of the social and behavioural sciences. Our understanding of the real-world behaviour of digital and human systems depends on a wide range of disciplines. Effective cybersecurity measures will need to integrate insights from them all.

Cybersecurity challenges are global, with networks, services and attacks rarely confined to a single jurisdiction. The best researchers are also located around the globe, and their ideas can quickly be applied anywhere. Data are also easily transmitted around the world, can be rapidly replicated and are extremely long-lived. Legal frameworks are not yet well-adapted to this situation, with public policy and law enforcement still working mostly at the national level. This makes it harder to respond to attacks, identify offenders and secure digital systems.

Cybersecurity spans private and public sector interests. Collaboration between governments, industry and academia helps take advantage of expertise and knowhow from all sectors, and develops solutions that are fit for purpose. However, collaboration can be challenging because motivations, interests, ways of working, and modes of communication vary.

The sensitive nature of the material protected by cybersecurity can affect how much information is shared about protective measures, vulnerabilities and breaches. This knowledge is an important collective resource for improving cybersecurity defences, but its use is often limited by lack of transparency. This lack of transparency is often based on justified concerns about the risks of releasing information, but sometimes risk-aversion or organisational culture drives greater secrecy than is warranted.

Cyber threats are hard to predict and constantly evolving. Attackers exploit the vulnerabilities created by complexity and our increasing reliance on digital systems. Simple malware has been extended into highly targeted exploits, such as ransomware and silent malware that remain undetectable until activated. To deal effectively with these evolving threats the digital sector must itself be diverse and responsive.

Technical and legal structures may mean that those who suffer most from attacks are not best placed to defend against them. Vulnerabilities affect a system's users, commercial partners and other stakeholders, and may cause more harm to them than to the organisation that is responsible for fixing the vulnerability.

Vulnerabilities may remain undetected for a long time[23]. Digital devices and systems can be difficult or expensive to update or retrofit, or might be used long beyond the security support period. Security by design can help minimise these vulnerabilities, and make them easier to fix once found, but is not yet common practice. This will be particularly important for Internet of Things devices, since customers often expect these devices to operate reliably *in situ* for a number of years[24].

[22] Anderson, R., 2008. *Security engineering (2nd ed)*. Wiley.

[23] For instance, the Shellshock vulnerability in Bash went undetected for 25 years before being identified and disclosed.

[24] Stankovic, J.A., 2014. *Research directions for the internet of things*. Internet of Things Journal, IEEE, 1(1), pp.3-9.

Finally, cybersecurity is characterised by persistent asymmetries[25]. Attackers are agile, difficult to detect and lose little if their attack fails. Their targets are slower to react, difficult to hide, and stand to lose a great deal to a single cybersecurity breach[26].

1.5 To capitalise on the UK's strengths, we need a trustworthy, resilient and self-improving digital environment

Policy, practice and research will need to adapt to deliver the cybersecurity system the UK needs. The recommendations made in this report seek to set up a self-improving, resilient digital environment that can thrive in the face of unanticipated threats, and earn the trust of the people who rely on it.

To establish trust, organisations must be trustworthy, and people must have access to credible and comprehensible information that helps them see that this is the case[30]. Building this awareness will help individuals choose more secure products, and will also help investors and regulators make better decisions.

Security can never be absolute, so organisations and individuals will need to consider how their choices affect the risks they face, and how to continue operating while facing those risks. To make sound decisions about countering risks, organisations will need better information, and the capacity to implement countermeasures. Resilience will be key to success.

The fast-changing nature of the risks and opportunities means that future policy and practice must be informed by excellent research. Maintaining the UK's position as a leading digital society will require collaboration, with information and expertise flowing across sectoral, disciplinary and national boundaries. Effective translation will be needed to ensure new ideas are rapidly translated into new products and services that benefit us all.

[25] Anderson, R. 2001 *Why Information Security is Hard – an economic perspective*. Louisiana, USA: Proceedings 17th Annual Computer Security Applications Conference (See https://www.acsac.org/2001/papers/110.pdf, accessed 26 April 2016).

[26] Estimates of the average cost of a security breach range widely. Recent estimates include $620,000[27], £1.46 to 3.14 million[28] and $3.8-4 million[29] per breach for large businesses.

[27] Kaspersky Labs 2015 *Global IT Security Risks Survey*, (See http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf, accessed 15 June 2016).

[28] PwC (research sponsored by BIS) 2015 *Information Security Breaches Survey 2015*, (See http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf, accessed 15 June 2016).

[29] Ponemon Institute (research sponsored by IBM) 2016, 2016 *Ponemon Cost of Data Breach Study*. (See http://www-03.ibm.com/security/data-breach/, accessed 26 April 2016).

[30] Lee, B.C., Ang, L. and Dubelaar, C., 2005. *Lemons on the Web: A signalling approach to the problem of trust in Internet commerce*. Journal of Economic Psychology, 26(5), pp.607-623.

1.6 This report

This report identifies the factors that are necessary to achieve a vibrant digital society which is supported by robust cybersecurity. The report seeks to build on and inform current debates about what actions and investments are needed for our future security, how security and surveillance can be balanced, and how the benefits of digital systems can best be realised.

The UK Government has committed to invest £1.9 billion in cybersecurity from 2016 to 2020, and will publish a new National Cyber Security Plan in 2016 to direct that investment[31]. A new National Cyber Security Centre is being established, and will play a key role in delivering that strategy[32]. In the USA, the administration has proposed cybersecurity spending of $19 billion in the 2017 fiscal year – a 35 per cent increase over 2016 – alongside a plan aimed at raising the level of cybersecurity across the country[33]. In 2017, the US Government plans to spend $728 million on cybersecurity and information assurance research[34] from the broader Networking and Information Technology Research and Development budget of $4.5 billion.

While governments have acknowledged the importance of cyber issues through greater spending, debates have continued about how authorities should use and govern digital systems. The UK Parliament has been debating the Investigatory Powers Bill 2016, which consolidates, extends and enshrines legislated powers to intercept and collect communications. Apple and the FBI have been engaged in a public dispute about the desirability, feasibility and risks of creating custom software to circumvent the access controls built into the iPhone. Both have been accompanied by vigorous debate about what powers authorities should have to access private communications, and the risks associated with those powers.

These developments make this report particularly timely. However, the digital environment is constantly evolving. This means the specific actions needed in the short term also change rapidly while, at the same time, policy questions often have deep and complex ethical dimensions. Trade-offs can often only be resolved through well-informed public debate and deliberation. The report seeks to inform those debates, but does not claim to be the final word on this fast-evolving topic. These debates will continue far into the future, and many others must contribute to them. Their outcomes will be improved if they take place in public, informed by the expertise available both in the UK and abroad. As a further step the Royal Society and British Academy are convening separate work on data governance (see section 2.4).

[31] Osborne, G. 2015 *Chancellor's speech to GCHQ on cyber security*. (See https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security, accessed on 10 June 2016).

[32] HM Government 2016 *National Cyber Security Centre prospectus*. (See https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus, accessed 10 June 2016).

[33] White House 2016 *Fact Sheet: Cybersecurity National Action Plan* (See https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, accessed 10 June 2016).

[34] The Networking and Information Technology Research and Development Program 2016 *The Networking and Information Technology Research and Development Program- supplement to the President's budget*. Washington, D.C.: NITRD (See https://www.nitrd.gov/pubs/2017supplement/FY2017NITRDSupplement.pdf, accessed 26 April 2016).

At the time of publication, the UK had voted to leave the European Union and the full implications of the referendum remained unclear. However, leaving the EU will further increase the importance of innovation and the value of research to the UK economy. Cybersecurity in particular can deliver important economic benefits, both by underpinning the digital foundations of UK business and trade and also through innovation that feeds directly into growth. The findings of this report will be relevant regardless of how the UK's relationship to the EU changes.

Ensuring the UK can enjoy the benefits of digital systems will require the existence of a resilient and self-improving environment, which can only be realised with the support of excellent research. A resilient and self-improving environment will also demand and stimulate the excellent research needed to meet the challenges we will face in the future.

The next four sections of this report outline the conditions necessary for a cybersecurity environment that is trustworthy and resilient, and supported by high-quality research together with effective measures for translation and innovation.

Chapter two
Trust

Trust

2.1 Trust and trustworthiness underpin growth and innovation

Trust is defined in a range of ways across computer science, philosophy and the social sciences. For the purpose of this report, trust is taken to mean an individual's or group's confidence in the integrity, safety and reliability of a system or organisation. So defined, greater trust opens up more opportunities for innovative products and services, and allows people to engage confidently with digital systems.

People already place their trust in a wide range of digital systems and organisations, including governments, banks, retailers, social networks, email and messaging services, hardware and software developers, and telecommunications providers. However, systems or organisations may turn out to be untrustworthy, and users have no fully reliable way to identify which ones they should trust.

High-profile hostile breaches occur regularly, and are rarely predicted in advance. In 2014/15, the US Office of Personnel Management was the subject of a data breach that resulted in the disclosure of 21.5 million federal employees' personal information[35,36]. In 2014, attacks on Sony Pictures Entertainment exposed sensitive information about employees, including confidential staff emails[37]. In 2013, credit card and other personal details of 40 million customers were stolen from the US retail chain Target[38], ultimately leading to the resignation of Target's CEO, and legal action being brought by both banks and customers.

Inadvertent or accidental disclosure of information also occurs. In 2015 an unencrypted memory stick containing over 3,000 National Health Service patients' personal and medical information was found in a car park behind a hospital[39]. In 2007, the names, dates of birth, National Insurance numbers and bank details of around 25 million people were lost in transit between HM Revenue & Customs and the National Audit Office[40,41].

Finally, information is sometimes used in ways that users do not realise they have agreed to, and might not have consented to if they had been fully informed when they signed up. Sometimes this happens because a service's business model changes after a user signs up. Business models based on advertising are particularly dependent on access to personal information. In 2011, LinkedIn updated its privacy policy to allow user photos and profiles to be used in advertising displayed on the site.

[35] Also includes applicants who had undergone background checks but had not taken up a post.

[36] Office of Personnel Management 2015 *Cybersecurity Incidents*. (See https://www.opm.gov/cybersecurity/cybersecurity-incidents/, accessed on 10 June 2016).

[37] Sony Pictures Entertainment 2014 *Breach Notification*. (See http://oag.ca.gov/ecrime/databreach/reports/sb24-47706, accessed 10 June 2016).

[38] US Senate Committee on Commerce, Science and Transportation 2014 *A "Kill Chain" Analysis of the 2013 Target Data Breach*. (See https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf, accessed on 10 June 2016).

[39] East Sussex Healthcare NHS Trust 2015 *30 September 2015 Board meeting papers* pp.150-160. (See http://www.esht.nhs.uk/EasysiteWeb/getresource.axd?AssetID=508651&type=full&servicetype=Attachment, accessed 10 June 2016).

[40] Poynter, K. 2008 *Review of information security at HM Revenue and Customs*. (See http://webarchive.nationalarchives.gov.uk/20100407011151/http://www.hm-treasury.gov.uk/d/poynter_review250608.pdf, accessed 10 June 2016).

[41] Darling, A. 2007 *Statement to the House of Commons by Chancellor of the Exchequer, Alistair Darling, MP, on HMRC*. (See http://webarchive.nationalarchives.gov.uk/20130129110402/http://www.hm-treasury.gov.uk/newsroom_and_speeches/speeches/statement/speech_statement_201107.cfm, accessed 10 June 2016).

Although individuals could opt out, and had been notified of the change, users responded negatively and LinkedIn removed user photos within a month of launching the new advertising format[42].

Whether misuse of data is hostile, accidental or merely unexpected, it can reduce trust. If digital products and services cannot become more reliable and secure, reduced trust could result in scenarios ranging from the minor dislocation of digital services through to widespread disillusionment.

A loss of trust in particular types of product or service might mean new systems or applications were no longer viable, and it might become harder for existing products and services to attract new users. This digital dislocation would put the benefits of some systems out of reach. Already some kinds of digital systems, while technically possible, have failed to take hold partly because of difficulties building trust. Electronic health records have not gained strong trust from the public: in the UK 79 per cent of survey participants were worried about their security, and 47 per cent believed electronic records would be less secure than existing records[43]. This trust deficit may limit the benefits from electronic records, for example if patients refuse to allow their data to be analysed in ways that could improve medical practices[44].

In a more extreme case, a widespread loss of trust could lead to the abandonment of some digital products and services. Individuals, businesses and society could lose the benefits of digital systems, while breaches of neglected systems would continue to cause harm.

To date, users have seemed to be relatively unresponsive to breaches of trust – digital systems continue to grow, and ever more sensitive information goes online. If this situation continues and there are no major improvements in security, people will face high risks. In this scenario digital systems would continue operating, but frequent and severe breaches would regularly harm individuals and organisations, reducing the net benefits.

Trust in some digital organisations is already weak, with UK survey respondents ranking ‘Internet companies’ the second-least trusted institution to handle their data (ahead of the press)[45]. To avoid these negative scenarios and realise the benefits, organisations will need to be able to demonstrate that they, and their products and services, are trustworthy.

Whether trust is well-placed depends on trustworthiness. A trustworthy organisation or service is one in which users have good reason to place their trust[46]. Trust granted to an untrustworthy organisation leaves users exposed to risks that could be avoided or reduced, and which they may not have factored in. When users cannot establish whether an organisation is trustworthy, they may not even be aware of the risks they are taking on.

There are two important aspects of trustworthiness: organisations must act in a competent way, and users must have access to information that convinces them the organisation is acting competently.

[42] Roslansky, R. (11 August 2011) *Privacy, Advertising, and Putting Members First*. Linkedin (See https://blog.linkedin.com/2011/08/11/social-ads-update, accessed 26 April 2016).

[43] Papoutsi, C., Reed, J. E., Marston, C., Lewis, R., Majeed, A., Bell, D. 2015 *Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study*. BMC Medical Informatics and Decision Making, 15(86) (DOI: 10.1186/s12911-015-0202-2).

[44] Broad, E., Sasse, T. 2016 *Two-way trust is needed to make the most of health data* (See: https://www.newscientist.com/article/2090017-two-way-trust-is-needed-to-make-the-most-of-health-data/, accessed 10 June 2016).

[45] Ipsos MORI (research sponsored by Royal Statistical Society) 2014 *Public attitudes to the use and sharing of their data*. (See http://www.statslife.org.uk/files/perceptions_of_data_privacy_charts_slides.pdf, accessed 26 April 2016).

[46] O’Neill, O. 2002 *A question of trust: the BBC Reith lectures*. Cambridge: Cambridge University Press.

2.2 Competent behaviour underpins trustworthiness

Trustworthiness depends on an organisation being competent in ways that are specific to its role and mission – competence means delivering the services a user expects, at the quality levels expected, as well as not behaving in ways that a user would not expect or condone. For organisations responsible for digital systems, competence means designing, implementing and operating their systems in ways that are reliable, secure and up to date. These include the digital systems themselves, the social and human systems that interact with them, and their connections to other systems.

Acting in competent ways is made more challenging by the complexity, scale and interdependence of the digital and social systems involved. The Heartbleed bug in OpenSSL left communications to and from between 24 and 55 per cent of all websites vulnerable to interception by hostile parties[47]; OpenSSL is open source software maintained largely by volunteers, but a huge number of commercial web services depend on it. Even if there is no technical vulnerability to exploit, social engineering attacks exploit flaws in the interface between technological and human systems and can cause substantial harm[48].

Competent security and reliability must be based on a rigorous and evidence-based standard of engineering – one that is continually rising based on strong scientific evidence. 'Best practice' should not refer to average practice, nor to a check-box approach, but to an ambitious, state of the art standard for security and reliability, informed by research.

Digital systems face a multitude of risks, from both malicious and accidental actions. A competent organisation must work actively and continually to reduce these risks, detect threats and breaches, and to respond effectively if they occur.

2.2.1 Robust encryption, authentication and access control

The competent operation of trustworthy digital systems relies on many different technologies. Fundamental security technologies include authentication, access control and encryption.

These techniques provide the technical assurance that enables people to entrust their personal and private information to digital systems. Authentication verifies the identity of a user – assuring the service that they are who they claim to be, and preventing unauthorised parties from imitating that user. Access controls determine the actions an authenticated user has the right to perform, ensuring that security-critical functions cannot be altered by a normal user.

Encryption is an important cryptographic technique that allows information to be securely transmitted and stored. Encryption is used to convert 'plaintext' information into 'ciphertext', which contains all the information of the plaintext message, but cannot be read without the proper key and mechanism to decrypt it (see box 2.1). If strong encryption is properly implemented, deciphering an encrypted message without the key is extremely difficult, if not impossible.

[47] Durumeric, Z., Kasten, J., Adrian, D., Halderman, A. J., Bailey, M., Li, F., Weaver, N., Amann, J., Beekman, J., Payer, M., Paxson, V. 2014 *The Matter of Heartbleed*. Proceedings of the 2014 Conference on Internet Measurement, pp.475-488 (DOI: 10.1145/2663716.2663755).

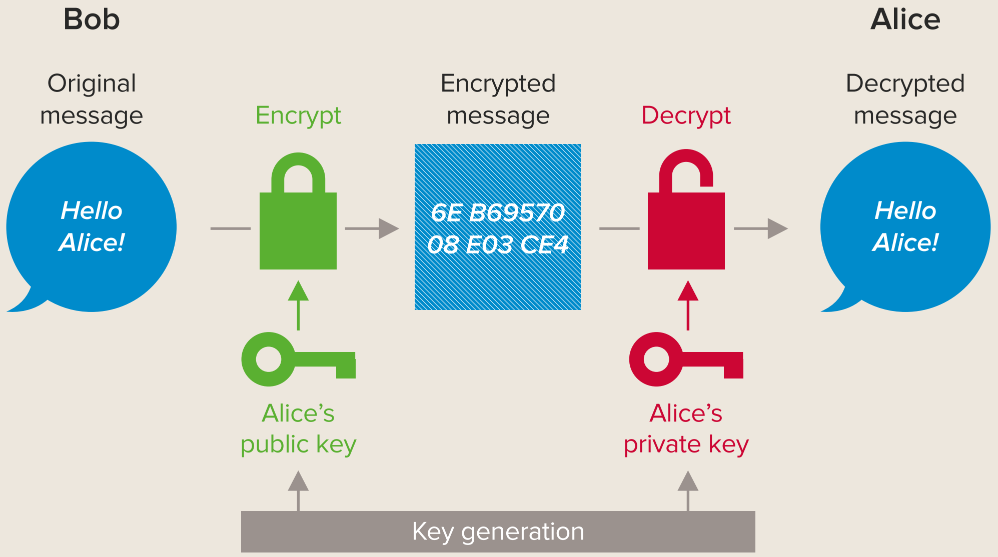
[48] APWG 2016 *Phishing Activity Trends Report Q1 2016*. (See http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf, accessed 10 June 2016).

BOX 2.1

Public key encryption

'Asymmetric' or 'public key' encryption allows two people to exchange a secret even though the communication with the shared secret might be overheard. A different key is used for encryption and decryption, with people making their public keys for encryption generally available, and keeping their private keys for decryption secret.

In an asymmetric message exchange, Bob asks Alice to send her open padlock (public key) to him through the post, keeping her private key to herself. When Bob receives it he uses Alice's public key to lock a box containing his message, and sends the locked box to Alice. Alice can then unlock the box with her private key and read the message from Bob. To reply, Alice must similarly get Bob's open padlock (public key) to lock the box before sending it back to him.



Material encrypted with Alice's public key can only be decrypted with Alice's private key.

Without robust encryption, services that store or transmit sensitive information could not carry out their missions securely. Robust encryption is necessary (though not sufficient) for trustworthiness – and trust – in the digital age.

Some third parties have an interest in gaining access to encrypted information. Malicious actors seek unauthorised access to valuable encrypted information, and clearly this must be prevented. On the other hand, intelligence and law enforcement agencies have legitimate reasons to seek access to encrypted material. Convicting criminals and preventing malicious acts – from child exploitation to terrorism – are valid activities for law enforcement agencies and the courts to carry out, and access to some encrypted materials might help them achieve these ends.

There has been vigorous public debate[49] in the UK, United States, the European Union and elsewhere about how to strike an appropriate balance between security and surveillance. This debate has particularly focused on how and whether authorities should be able to gain extraordinary access to encrypted material (although access to metadata and other unencrypted information has also been at issue).

[49] Perlroth, N. (7 July 2015) *Security Experts Oppose Government Access to Encrypted Communication*. The New York Times (See http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html, accessed 10 June 2016).

It is good that this debate is taking place, since it involves difficult trade-offs that will fundamentally affect all users of digital products and services. As in most important debates involving technology, sound scientific evidence will make an important contribution.

In this case, there is a clear consensus among security researchers that introducing "backdoors" or extraordinary access measures would also open doors through which malicious intruders could attack[50,51].

Extraordinary access requirements would give rise to a range of risks: malicious intruders may gain access to methods intended only for authorities, giving them access to all data to which those authorities have access; the increase in complexity increases the likelihood of errors and vulnerabilities in design and deployment; and products that must comply would be at a disadvantage compared to those available from other countries[52]. There are encryption solutions based in other countries that would not be subject to UK or US law, including in countries that have committed not to introduce backdoors[53]. It would be impossible to control access to encryption solutions from abroad, particularly where they are available as open source software.

These risks could open up new opportunities for attacks, jeopardising protection for the majority of people who rely on digital networks to store and transmit personal information, and who have a legitimate interest in maintaining the security of those networks. The severity and breadth of these risks will continue to grow as modern societies and economies rely more on digital systems.

The risk of opening doors for malicious intruders must be weighed against the risks from denying intelligence and law enforcement agencies access to encrypted material. These include the possibility that criminals go free because strong encryption obscures their actions and prevents their conviction, and that malicious acts which could have been detected and prevented are not.

While encryption makes some kinds of surveillance harder, not all sources of intelligence will 'go dark', and new sources of information are constantly coming online[54,55]. Many online businesses will be reluctant to adopt end-to-end encryption, since their business models depend on access to user data. Although encryption is becoming more common in messaging and telephony services, metadata – such as the identity of the sender, receiver, time and location of the

[50] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. & Weitzner, D. J. 2015 *Keys Under Doormats: mandating insecurity by requiring Government access to all data and communications. Journal of Cybersecurity, 1*(1) (DOI: 10.1093/cybsec/tyv009).

[51] Abelson, H., Anderson, R.N., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P.G., Rivest, R.L., Schiller, J.I. and Schneier, B., 1997. *The risks of key recovery, key escrow, and trusted third-party encryption*. (See http://hdl.handle.net/10022/AC:P:9130, accessed 10 June 2016).

[52] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. & Weitzner, D. J. 2015 *Keys Under Doormats: mandating insecurity by requiring Government access to all data and communications. Journal of Cybersecurity, 1(1)* (DOI: 10.1093/cybsec/tyv009).

[53] Schneier, B., Seidel, K., Vijayakumar, S. 2016 *Worldwide Survey of Encryption Products*. Cambridge, Massachusetts: Berkman Centre for Internet & Society at Harvard University (See https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf, accessed 26 April 2016).

[54] Swire, P. (9 July 2015) Senate Judiciary Committee Hearing. *Going Dark: encryption, technology, and the balance between public safety and privacy* (See https://www.judiciary.senate.gov/download/07-08-15-swire-testimony, accessed 26 April 2016).

[55] Bellovin, S.M., Blaze, M., Clark, S. and Landau, S., 2014. *Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet*. Northwestern Journal of Technology & Intellectual Property, 12(1).

message – is generally not encrypted, and can be highly valuable to authorities (and any organisation that aggregates data). Meanwhile, an increasingly networked world, including the rise of the Internet of Things, is rapidly creating new sources of information and opportunities for surveillance[56]. Physical evidence and surveillance will also remain firmly in scope for authorities.

Given that robust cryptography exists, and will continue to exist, we must decide what policy settings are most appropriate to govern its use. There are risks on both sides, and governments have a responsibility to act in ways that balance those risks, protecting and securing their citizens, society and the economy. Given the risks weakened encryption would create for all citizens, government should be a strong supporter of widespread, robust encryption.

RECOMMENDATION 1

Governments must commit to preserving the robustness of encryption, including end-to-end encryption, and promoting its widespread use.

2.2.2 Independent principles, standards and practices for better cybersecurity

While a competent organisation needs to address a wide range of risks, few organisations have the scale or breadth to understand and address every vulnerability and risk in modern digital systems.

Identifying technical risks requires deep and specific knowledge, and this expertise often lies outside an organisation's core business. Similarly, identifying risks in social systems requires sociological and behavioural expertise. Overlaid on digital and human systems are legal and regulatory systems, creating risks of their own. As a result, many organisations have little understanding of the likelihood and severity of the risks they face, or of the level of risk that users are, or should be, willing to accept. This makes it difficult for those organisations to identify and adhere to appropriate cybersecurity practice.

There are existing efforts to guide organisations on cybersecurity best practice: in 2014, the UK Government launched Cyber Essentials, a two-tier badging system to help businesses assess how effectively they have managed their cybersecurity risks[57]. This system can help businesses improve their basic cybersecurity arrangements, but is insufficient for an organisation providing more complex digital systems. The US National Institute of Standards and Technology's Cybersecurity Framework also provides guidance on good cybersecurity practice, but is targeted specifically at critical national infrastructure organisations.

[56] DeLong, J., Grasser, U., Hon. Gertner, N. (ret.), Goldsmith, J., Landau, S., Neuberger, A., Nye, J., O'Brien, D. R., Olsen, M., Renan, D., Sanchez, J., Schneier, B., Schwartztol, L., Zittrain, J. 2016 *Don't panic: making progress on the "Going Dark" Debate*. Cambridge, Massachusetts: Berkman Centre for Internet & Society at Harvard University (See https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf, accessed 26 April 2016).

[57] Department for Business, Innovation and Skills 2014 *Cyber Essentials Scheme Summary*. London: BIS. (See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf, accessed 27 April 2016).

Going beyond these existing schemes, guidance is needed that can be applied across a broad range of systems for digital products and services. Such guidance should cover principles, standards and practices for state of the art cybersecurity, should be built on robust evidence and research, and should be focused on protecting consumers. It should help organisations understand what rigorous, evidence-based systems engineering looks like, and should be continually improved as knowledge and understanding grow[58]. The expertise and evidence needed to inform this knowledge and understanding are distributed across business, academia and the public sector. To draw effectively on all these sectors and to earn the trust of organisations and customers, the guidance should be developed by a transparent and independent body with a clear remit to act in the public interest.

This guidance should cover both development processes and the testing and evaluation of the final products. It should promote security by being usable and encouraging security by design. Systems that are carefully engineered for robustness, security and usability will tend to be less vulnerable to security flaws[59] and, when vulnerabilities are found, a well-engineered system is more readily patched than one with fundamental design weaknesses. Usable security should also include automating security updates by default and ensuring that these updates do not interfere with the user's task.

The guidance should also make it as easy as possible for users to be safe and secure, by providing clear and verifiable assurance that the product adheres to sound principles, standards and practices, for instance through a verifiable kitemarking scheme. This scheme should reflect the need to stay up to date, and make use of feedback from users.

Developing quality and reliability guidance of this sort is more challenging than developing technical standards, such as those for network communications. This is partly because of the wide variety of products and methods of implementation, and partly because of the need for continual improvement. The processes to develop and improve sound principles, standards and practices for cybersecurity should be carefully considered, and informed by approaches that have worked for similar issues in the past. To drive change, they will need both to be usable for developers and to provide clear information that demonstrably improves customers' choices and users' security.

In the short term some of these principles, standards and practices will need to be based on expert advice, but over time they must be validated and improved based on rigorous scientific and experimental evidence. The UK can draw on existing efforts to build the evidence base for cybersecurity. Most notably the Research Institute in Science of Cyber Security was established in 2013 to develop evidence to allow organisations to make better decisions about cybersecurity[60] and to move from common, established practice to a more robust evidence-based approach to cybersecurity. This research should be built on and extended in developing new guidance for principles, standards and practices that characterise the state of the art in cybersecurity.

To supplement this evidence-based guidance, information sharing between organisations can help spread good solutions to security challenges. Similarly, reporting against excellent standards of practice can create incentives that drive improvement. Chapter 3 considers information sharing and reporting in more detail.

[58] Murdoch, S.J., Bond, M. and Anderson, R., 2012. *How certification systems fail: Lessons from the Ware report.* IEEE Security & Privacy, 10(6), pp.40-44.

[59] Molotch, H. 2013 *Everyday Security: Default to Decency*. IEEE Security & Privacy, 10(6), pp.84-87.

[60] The Research Institute is jointly funded by GCHQ and the Engineering and Physical Sciences Research Council. For more information see http://www.riscs.org.uk.

2.2.3 Anonymisation techniques

Protecting users' personal information and privacy is an important behaviour for a trustworthy organisation. This can be achieved using privacy preservation techniques including: anonymisation of data (preventing the user's identity from being inferred from data); anonymous communication (preventing the sender or recipient of a message from being identified); and private information retrieval (preventing the piece of information retrieved being known to the provider of the information)[61]. These techniques will be used to differing extents in different settings and across time, with anonymisation of data the most common technique in use today.

Anonymisation is made more challenging by the increasing volume of data available and by modern data-matching techniques, which have made it easier to de-anonymise data and reveal personal information[62]. Evolution in both the amount and nature of data available and the techniques used to extract information from it, mean that questions of privacy will be increasingly affected by the ways in which information about one individual may reveal information about another. Based on these trends, the US President's Council of Advisors on Science and Technology has concluded that simple de-identification used alone no longer provides a useful basis for policy[63]. New methods of anonymisation are being developed to address these challenges (see box 2.2)[64,65].

Anonymous communication technologies represent another important aspect of privacy preservation. Communication patterns can be one of the most revealing sets of data about an individual, and protecting this information is important for securing identity and privacy[66]. The growth of end-to-end encryption in messaging services, and in services like the Tor network[67], is increasing protection for this sensitive category of information.

The long life and large volumes of data now available mean that new methods of anonymisation will need to be robust, including anticipating future advances in de-anonymisation methods. Research also needs to consider the interactions between technological solutions and the social systems of governance and behaviours within which they sit. Independent processes to assess the robustness of anonymisation techniques would help demonstrate trustworthiness and build trust[68].

[61] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J-H., Métayer, L. D., Tirtea, R., Schiffner, S. 2014 *Privacy and Data Protection by Design – from policy to engineering*. Heraklion, Greece: European Union Agency for Network and Information Security. (See https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design, accessed 27 April 2016).

[62] Narayana, A. & Shmatikov, V. 2008 *Robust De-anonymization of Large Sparse Datasets*. Oakland, California, USA: 2008 IEEE Symposium on Security and Privacy. (See http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4531148, accessed 27 April 2016).

[63] President's Council of Advisors on Science and Technology 2014 *Big Data and Privacy: a technological perspective*. Washington, D. C.: PCAST (See https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf, accessed 27 April 2016).

[64] Erlingsson, Ú., 2014. *Learning statistics with privacy, aided by the flip of a coin*. (See https://security.googleblog.com/2014/10/learning-statistics-with-privacy-aided.html, accessed 10 June 2016).

[65] Blocki, J., Datta, A. and Bonneau, J., 2016. Differentially Private Password Frequency Lists. (See http://www.jbonneau.com/doc/BDB16-NDSS-pw_list_differential_privacy.pdf, accessed 10 June 2016).

BOX 2.2

Anonymising data: anonymisation techniques and differential privacy

There are two ways to anonymise data: by removing personally identifiable information from a database before data are processed, or by protecting identifiable data through controls on the queries that can be made to the database.

Simple de-identification is often applied to prevent the accidental identification of individuals, for example for patients' medical data, and relies on contractual and ethical controls to protect privacy. The personally identifiable information removed could be a birthdate, home address or other information that connects directly to a person. While some information may be uniquely identifying on its own, any non-trivial information can be identifying when aggregated with other databases. For example, location data from a mobile phone could at first glance appear impersonal, but a week's worth of location data from one smartphone could show where a person works and lives, narrowing down who that person might be.

Stronger anonymisation techniques provide assurance that an individual's identity will be protected even if an anonymised database is aggregated with other databases. Currently the most effective way to show that these criteria have been met is to apply an anonymisation technique which provides "differential privacy"[69]. Techniques which provide differential privacy can be applied either by releasing a dataset which has been modified to ensure all the individuals in the dataset are protected, or by allowing interaction with a database and adding a calculated amount of random noise to the answer of database queries. The latter option will, in general, preserve more of the original value of the database, regardless of the anonymisation technique used.

There are challenges in implementing and using techniques for differential privacy, but methods for data release that can be proven to preserve anonymity would be highly valuable in a wide range of settings.

[66] Murdoch, S.J., 2014. Quantifying and measuring anonymity. In Data Privacy Management and Autonomous Spontaneous Security (pp. 3-13). Berlin, Heidelberg: Springer.

[67] The Tor network preserves the privacy and anonymity of its users through encryption and obscured routing of data through the network.

[68] The annual Privacy Enhancing Technologies Symposium brings together privacy experts to discuss advances in privacy technologies (See https://www.petsymposium.org/, accessed 27 April 2016).

[69] Dwork, C. & Roth, A. 2014 *The Algorithmic Foundations of Differential Privacy*. Foundations and Trends in Theoretical Computer Science, 9(3-4), pp. 211-407 (DOI: 10.1561/0400000042).

2.3 Accessible information enables people to judge trustworthiness

People must have credible and comprehensible information to help them make well-founded judgements about where to place their trust.

The regularity and severity of breaches suggest people should be concerned about the competence, and therefore the trustworthiness, of many services and organisations – but which ones? Although there are many organisations that competently operate digital systems and products, they are hard to identify. There are also many organisations with the capacity to become more trustworthy but little incentive to do so, since people would not be able to tell anyway[70,71].

To judge competence, people need information that is credible, comprehensible and consistent. When users get that information, they need to decide whether to trust it – and sometimes vendors make claims that should not be trusted. This is hard for outsiders: they do not have enough information to make an informed judgement, because most systems' internal workings are hidden for reasons of user-friendliness, security or commercial confidentiality. To give their users good information on which to build trust, platforms like eBay and Uber use user-generated reputation scores to assure buyers and sellers that the other party can be trusted. Users of other digital systems need information about security that is similarly credible, comprehensible and consistent.

Giving people credible and comprehensible information would help trustworthy and secure organisations thrive and give others an incentive to improve. It might also make some new and more secure systems viable, by allowing organisations to make credible claims about greater security and assuring users that these systems are worthwhile.

However, providing credible information about reliability and security is difficult for digital systems, because they are opaque and complex by nature. Users cannot assess the inner workings of digital systems because they do not have access to them, either because of their commercial sensitivity, concerns about security or simply because the system would be less usable if users interacted with the inner workings directly. Even if users did have access to these internal workings, the interaction of digital systems with other systems means that users would also need to consider the security of all connected systems. The complexity involved makes this analysis unfeasible for any individual and for most organisations.

Nonetheless, people must constantly make judgements about whether to trust digital products or services. In some cases people cannot opt out, so they do not make an active judgement at all. In other cases, they must rely on incomplete or unreliable indicators. An encryption symbol in the user's browser address bar indicates their communication with the service is encrypted, but gives no assurance about what happens to the information after transmission. A government web domain or the logo of a well-known corporation might imply safety, but in fact these high-profile organisations are often targets for attacks. Many of these signals are also easily faked, for instance by phishing attacks that are increasingly deploying sophisticated imitations of genuine websites.

[70] Anderson, R. 2001 *Why Information Security is Hard – an economic perspective*. Louisiana, USA: Proceedings 17th Annual Computer Security Applications Conference (See https://www.acsac.org/2001/papers/110.pdf, accessed 26 April 2016).

[71] Akerlof, G. A. 1970 *The Market for "Lemons": quality uncertainty and the market mechanism.* The Quarterly Journal of Economics, 84(3) pp. 488-500.

This problem is more serious for individuals than for organisations. Large organisations have the resources to research and assess their options, hold their suppliers accountable, and manage the associated risks. Smaller organisations generally have less capacity, and individuals have very little. Individual consumers also face large potential harms from the loss or disclosure of personal information. To mitigate these risks, consumers need reliable signals of trustworthiness.

Kitemarks or other certification marks – potentially including dashboards, evaluation marks and benchmarking results – should be established to provide information that is clear, relevant, comprehensible and credible, to help consumers better judge trustworthiness. These kitemarks should reflect continuing improvement in the state of the art, for instance by indicating how up to date the certification is, or by incorporating the need to continually improve and update practice[72]. Kitemarks will also need to provide clear assurance of authenticity, to prevent the signal being undermined by fake certification marks. The development of effective kitemarks for the digital age will be challenging; this should be informed by evidence on the human factors that affect take-up and effectiveness, as well as by lessons from other trust mechanisms operating online (for instance, reputational and feedback systems).

The institution that develops these principles, standards and practices should be independent, transparent and expert (see section 3.2).

RECOMMENDATION 2

The Government should go further to establish and promote rigorous, evidence-based guidance on state of the art cybersecurity principles, standards and practices, accompanied by certification marks or benchmarks for digital products and services, focused on improving consumers' protection and understanding.

- The identification of rigorous, evidence-based benchmarking and evaluation standards for cybersecurity, how best to structure those standards, and how best to communicate them to users should be informed by existing and future research.
- Review processes for evaluating privacy preservation methods should be established, including anonymisation techniques (for releasing or providing access to data) and anonymous communications.

[72] For example, one criterion might be how long a product will receive security updates. This would encourage ongoing improvement in the security of deployed devices and systems.

2.4 Debates on ethics and governance are fragmented

An organisation that seeks to be trustworthy must behave competently and communicate that competence to its users. Competence is affected by governance arrangements and ethical frameworks. Robust governance arrangements are particularly important for resolving trade-offs between the legitimate interests of different individuals or groups, in which technical measures are little help.

Sometimes users have little choice about whether to place their trust in a system – for example, citizens are compelled to provide certain information to government, and employees must use their employer's systems at work. These kinds of digital systems often hold highly sensitive information and can be high-profile targets for attackers. If users do not trust these systems, they may try to subvert them (for instance by providing false information), limiting the benefits that can be realised. Ethics and data governance are even more important in these situations, where the stakes are high, individuals cannot protect themselves by legitimately opting out, and there is no competitive pressure on the provider to improve security.

There are substantial arrangements in place for the safe use of data in the UK, both generally and within specific sectors such as health or government. These largely have their roots in the early days of information technology, and do not cover all the aspects that will be important. In 2012, the European Commission began a process of reforming European data protection regulation, which will be enforced in EU member states from 2018[73]. However, there are broader challenges, including how best to implement the regulation.

In the future it is increasingly through engaging with machine learning and smart algorithms employed by businesses and governments, through people's use of connected and autonomous vehicles, of health devices, of assisted living or new forms of learning, that people will form their views and collectively negotiate what is acceptable in terms of use of data and what is not.

At the time of writing the report, the Royal Society and British Academy are convening another piece of work on data governance, including ethical aspects. The UK's experience with other emerging technologies is that we can create arrangements that enable a robust public consensus on the safe and valuable use of even the most potentially contentious technologies. The history of the engagement between science, government, regulators and public groups of all kinds on stem cell technologies shows this. In the case of stem cell technologies, high profile public debate began with the Warnock Commission, and continued through the establishment of the Human Fertilisation and Embryology Authority.

There is no exact historical parallel to the debate on data governance, but there are some important pointers to what we might do. The Royal Society, working with the British Academy, will begin by drawing together the existing somewhat fragmented debates, building connections between the major strands and identifying key questions and possible ways forward, with a view to making initial recommendations in late 2016.

[73] European Parliament and the Council of the European Union 2012 *Regulation (EU) 2016/679 of European Parliament and of the Council*. Brussels: EU. (See http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, accessed 28 April 2016).

Chapter three
Resilience

Resilience

3.1 Organisations will need to be resilient in the face of change

Digital technologies are constantly changing and improving, and organisations have to work hard to keep up. Cyber threats change and evolve just as quickly and so organisations must constantly work to maintain security and trust.

Digital systems operate in a risky environment, with attack or exploitation possible at any time. This environment is becoming more risky over time[74]. Threats are also often unpredictable, not only in who, where and when they strike, but also in how they work and what their effects are.

Organisations and systems that are resilient will be best placed to succeed in this environment. Resilience means having the capacity to function, adapt, grow, learn and transform under stress or in the face of shocks.

Cyber risks cannot be entirely eliminated, so organisations that are resilient must have a mind-set that constantly expects, looks for, and responds to incidents, vulnerabilities and risks. Resilience and risk mitigation can be costly, but many simple steps are inexpensive, and would require minimal organisational change. A competent organisation will have strategies and processes in place to address the remaining risks.

Security is a necessary element of resilience for any digital system. The right security allows an organisation to continue functioning during a cyber attack, respond appropriately, adapt quickly, and to grow and improve after the attack is over. These are the behaviours of an organisation that is competently protecting users' interests, and they will help to build users' trust despite threats or attacks.

An important element of resilience for digital systems is the ability to maintain critical operations while partially compromised. For example, the Tor network and other anonymous communication systems can maintain their security properties for most of their users even when elements of the network are malicious[75].

Since malware and vulnerabilities can remain undetected for a long time, a resilient organisation must take into account the risk that attackers can operate from inside their systems. Similarly, some of the most severe (and often unanticipated) risks faced by organisations come from insiders – either from insiders' own actions, or from manipulation of insiders by attackers. Anticipating and mitigating insider risk should be a priority, although some insider threat risk will always remain, since administrators need some degree of privileged access to systems and information.

To deal with this risk landscape, organisations will need to respond in two ways. They will need to continually improve their cyber practice, both maintaining and pushing forward the state of the art. They will also need to be able to adapt to unanticipated threats. They will only be able to respond effectively if they have sound advice and there is coordination across organisations and systems.

[74] PwC 2016 *The Global State of Information Security Survey 2016*. (See http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html, accessed 28 April 2016).

[75] Murdoch, S.J. and Watson, R.N., 2008. *Metrics for security and performance in low-latency anonymity systems*. In Privacy Enhancing Technologies (pp. 115-132). Berlin, Heidelberg: Springer.

3.2 Resilience will depend on trusted institutions to provide coordination and advice

Improvements in practice depend on greater information sharing, clearer standards for cybersecurity and sound advice for users and organisations. For these to be effective, users and organisations will need good reasons to trust the institutions responsible for facilitating information sharing, identifying the principles, standards and practices for state of the art cybersecurity and providing advice.

For guidance and advice on cybersecurity principles, standards and practices to be trusted, they must be authoritative and effective. They will need to be informed by world-class expertise, and by knowledge from across all sectors. Therefore, they must be developed transparently, with the security of users a clear first priority, and be based on rigorous scientific evidence.

For information sharing processes to be trusted, organisations will need to be able to provide information without concern that it could be misused. The processes for information sharing will therefore themselves need to be transparent and carefully designed.

In general, to earn the trust of users and organisations, institutions that coordinate information-sharing, set standards, and provide advice will need to be transparent and expert, and have a clear and widely understood remit and purpose.

Much of the history of computing and digital systems has been shaped by the military. For example, basic components of digital computing were developed through a programme for radar shields in the 1950s[76]. These and other advances made their way into commercial and civilian systems and, as the digital world grows, the balance of activity continues to shift towards civil society. The balance of risks is also shifting as the UK's economy and society become increasingly dependent on the security of digital systems. In the future, as this trend continues, the institutions that govern and guide the digital world will need to work with and reflect this more open environment.

There are a range of options for meeting these criteria, and there will be trade-offs in how such institutions are structured. An independent agency can have a clear remit to act in the interests of users, and can be transparent in how it does so. An agency within a national security organisation will have privileged access to classified information about threats, and to the expertise in the national security sector, but might face a tension between offensive and defensive cybersecurity missions: an offensive agency seeks to exploit some digital systems, while a defensive agency seeks to strengthen the defences of such systems. Multiple agencies can specialise in particular aspects of the broader cybersecurity task, while a single dedicated agency may benefit from being able to apply knowledge and lessons across areas.

In the USA, the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) are jointly responsible for setting information security standards, with the NSA historically providing the majority of input and expertise related to cryptographic standards. Following the release of the Snowden documents[77], there were concerns that the NSA may have influenced the development of NIST's cryptographic standards in ways that made the standards

[76] Edwards, P. 1996 *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge: MIT Press.

[77] Beginning in 2013, Edward Snowden, an ex-NSA contractor, leaked a large number of top secret intelligence documents to journalists, disclosing details of the surveillance capabilities and activities of UK, US and other intelligence services.

less secure[78,79]. An independent report into NIST's standards development processes concluded that it did not have sufficient resources and expertise to assess suggestions the NSA made for cryptographic standards[80]. As a result, NIST acknowledged there was a "possibility for tension between NIST's mission to promulgate the use of strong cryptography, and the law enforcement and national security missions of other agencies", and committed to safeguarding its independence by using open and transparent processes to develop standards and guidelines[81].

In Germany, the BSI (Federal Office for Information Security) is responsible for cybersecurity, but not intelligence or national security; this allows the BSI to engage more readily with companies and other organisations, enabling access to expertise from outside government.

In the UK, CESG[82] (the UK Government's National Technical Authority for Information Assurance) advises organisations on how to protect their information and information systems against threats, building on their original remit for the cybersecurity of government systems. CESG is located within the Government Communications Headquarters (GCHQ), which has a broader intelligence and national security mission. The classified nature of this mission means GCHQ must be secretive about many of its activities. This limits transparency, and also restricts how it can collaborate with outside experts.

In 2013, the Deputy Prime Minister commissioned the Royal United Services Institute to review the legality of the UK's surveillance programmes and the effectiveness of these regimes and their oversight. The report concluded that a series of reforms was needed, including new laws and processes to provide simplicity and greater clarity to the interception of private communications and related data by the security and intelligence services and the police[83]. This report focused on surveillance, but did not consider where information assurance should fit into the institutional structure.

In November 2015, the UK Government announced the creation of the National Cyber Security Centre (NCSC) which will bring together responsibilities for cybersecurity issues across society, providing a unified source of advice and support for the economy. It will work with industry, academia and international partners, but will report in to GCHQ.

By introducing the NCSC, government is seeking to move the UK's cybersecurity institutions to a more open and collaborative footing. This is a welcome direction of travel, but it will be challenging to ensure the NCSC can be sufficiently transparent, trustworthy and open to earn the trust of organisations and individuals. An early and open assessment of the UK's future institutional needs would help build that trust and ensure the new arrangements will support the best outcomes over the coming decades.

[78] Including as reported by Nicole Perlroth, Jeff Larson and Scott Shane in the New York Times on 5 September 2013 (See http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html, accessed 10 June 2016), and by James Ball, Julian Borger and Glenn Greenwald in the Guardian on 5 September 2013 (See https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, accessed 10 June 2016).

[79] The possible backdoor had also been identified earlier by researchers, in particular in a 2007 talk by researchers Dan Shumow and Niels Ferguson of Microsoft. (See http://rump2007.cr.yp.to/15-shumow.pdf, accessed 10 June 2016).

[80] NIST 2014 *NIST Cryptographic Standards and Guidelines Development Process: report and recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology*. (See http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf, accessed 28 April 2016).

[81] National Institute of Standards and Technology, Cryptographic Technology Group 2016 *NIST Cryptographic Standards and Guidelines Development Process. Gaithersburg, Maryland, USA: NIST* (See http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf, accessed 27 April 2016)

[82] Formerly the Communications Electronics Security Group.

[83] RUSI 2015 *A Democratic License to Operate*. London: RUSI (See https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf, accessed 27 April 2016).

As the digital environment grows and evolves into the future, the UK will need the right set of institutions to govern and guide its development. To deliver effectively, those institutions will need a clear remit and purpose, a strong presumption of transparency and world-class expertise. These future institutions will also need to take advantage of and be driven by excellent research, including any new challenge led research stream (see Recommendation 5).

It will be important for the UK's consumers and businesses that institutions for digital governance are well-suited to future needs, but in the digital era these institutions also have the potential to become a global asset. Indeed, the institutions will need to engage with the global businesses that are central to digital markets. High-quality, trusted institutions could attract businesses and systems operators to apply UK standards globally, use the UK's information sharing systems and to consider locating themselves in the UK. This could benefit users of digital systems everywhere, and would help the institutions themselves grow and improve. Conversely, competition from other countries offering these services could lead the highly mobile digital sector to re-orient towards other countries.

The precise institutional arrangements should be given careful consideration, and should build on existing institutions and on government's recent efforts to prepare for the future by establishing the NCSC. There will be trade-offs in deciding how these institutions should be structured, but it is clear that the future will see digital systems becoming ever more deeply integrated into society and individual lives. We must carefully consider how the institutional structures being introduced will be able to deliver in a substantially different future.

RECOMMENDATION 3

The Government should commission an independent review of the UK's future cybersecurity needs, focused on the institutional structures needed to support resilient and trustworthy digital systems in the medium and longer term.

- The Government has recently moved to consolidate a range of cybersecurity functions into a single new institution, the National Cyber Security Centre (NCSC). The review should work with those establishing the Centre and determining its programmes, to ensure that it has the capacity and incentives to deliver the requirements outlined in this report, and that there is continuing informed and open discussion about its role and ways of working. The independent review should be timed to take account of the experience of the new NCSC.

- The National Cyber Security Centre represents a helpful and important improvement in the UK's institutional arrangements for cybersecurity. However, the Centre will report in to the Government Communications Headquarters (GCHQ). Based on the trends and evidence available today this arrangement is unlikely to be ideal in the longer term, when digital systems will be embedded increasingly deeply across society and an increasingly large proportion of uses will be commercial and personal. The review should therefore also look 5-10 years into the future, to develop options for future governance arrangements that will better reflect the future distributions of benefits and harms across society.

3.3 Incentives for improving security should be aligned with wider incentives

Frequent breaches are often due to the same common security mistakes[84], while constant change also means that cybersecurity must be an area of continual improvement. Better-aligned incentives would encourage organisations to improve and invest in cybersecurity, encouraging prompt responses to breaches and vulnerabilities, and a culture of continuous improvement.

In order to preserve the agility and responsiveness of the digital sector, such incentives should be light touch and better-aligned with other incentives affecting the organisation's operations – primarily those arising from competition and corporate governance.

One reason that security lags behind threats is that the full costs of security failures are not borne by the organisation best placed to prevent them. Users or other organisations often bear much more of the cost of failure, while organisations making investments in cybersecurity can ignore these broader costs. This means some security investments do not occur, even though their full benefits would outweigh their costs[85].

Consumers' response to breaches and attacks is often muted, and this dilemma weakens incentives further. In 2015, TalkTalk suffered a major breach of sensitive user data, resulting from an exploitation of a well-understood security vulnerability in their public website[86,87]. TalkTalk lost 3% of their customers in the quarter the breach occurred, but this was followed by record low customer turnover in the following quarter[88].

Giving consumers more reliable information about cybersecurity measures (as recommended in Chapter 2) could strengthen incentives for cybersecurity by helping consumers make more discerning choices, but this will not be sufficient.

Organisations, both public and private, should regularly audit and report on their adherence to evidence-based cybersecurity good practice, in line with corporate governance requirements for other risks. This reporting should be based on the rigorous, evidence-based cybersecurity standards and certification marks proposed in Recommendation 2.

Reporting would improve practice in many organisations. Scrutinising and assessing security arrangements will reveal vulnerabilities, and will help organisations become more familiar with the evidence on what constitutes best practice.

Reporting in this way would also strengthen the incentives for continued improvement. Customers could use reported information to better judge trustworthiness. Investors and insurers would be better able to assess the risks – and mitigation measures – of companies. Regulators, governments and other stakeholders would similarly be better able to assess the risks borne by regulated bodies and public sector organisations.

[84] Open Web Application Security Project (OWASP) 2013 *Top 10 2013*. (See https://www.owasp.org/index.php/Top_10_2013-Top_10, accessed 26 April 2016) and OWASP 2004 Top Ten 2004. (See https://www.owasp.org/index.php/2004_Updates_OWASP_Top_Ten_Project, accessed 26 April 2016).

[85] Anderson, R. 2001 *Why Information Security is Hard – an economic perspective*. Louisiana, USA: Proceedings 17th Annual Computer Security Applications Conference (See https://www.acsac.org/2001/papers/110.pdf, accessed 26 April 2016).

[86] TalkTalk Group 2015 *Cyber Attack update – Friday November 6th 2015*. (See http://www.talktalkgroup.com/press/press-releases/2015/cyber-attack-update-november-06-2015.aspx, accessed 26 April 2016).

[87] The breach was reportedly achieved using an SQL injection attack, as reported by the BBC on 16 October 2015 (See http://www.bbc.co.uk/news/business-34635583, accessed 10 June 2016).

[88] TalkTalk Group Preliminary Results FY16, 2016 (See http://www.talktalkgroup.com/press/press-releases/2016/preliminary-results-fy16.aspx, accessed 10 June 2016).

Customers, investors and regulators each have an incentive to act on this information, and their actions would in turn improve the incentives for the providers and operators of digital systems. Users could take security into account when choosing which products to buy. Investors and insurers could better price the risk of breaches. Regulators and government could better build cybersecurity objectives into accountability frameworks and policy priorities.

These shifts would push organisations to improve security as a means to compete for customers, finance or better regulatory outcomes. The greater trust and investor confidence enjoyed by successful and secure organisations would set the pace for others, continually raising the bar of excellent practice. Not only would the incentives for better cybersecurity be stronger – the incentives for continual improvement would be too.

The design and implementation of reporting arrangements will be key to driving stronger security. At the moment, investors are often unresponsive to data breaches and consumers often do not appear to take security sufficiently into account in their decisions (or are locked into particular products and cannot switch rapidly). Careful research, design and evaluation of these policy measures will ensure they are effective.

3.4 Breach reporting can support adaptation to unpredicted threats

Steady and continual improvement in cybersecurity practice is necessary but even this cannot address all risks. The complexity of digital systems means that risks are often difficult to predict and, therefore, to prevent. Some of the most serious vulnerabilities have been entirely unanticipated but have affected vast numbers of people and organisations. For example, the Shellshock bug[89] went undetected for 25 years[90] but was widely exploited within a day of its disclosure[91,92].

To become resilient to unanticipated threats, organisations need the capacity to respond effectively at short notice, including by planning and being prepared for attacks, and through having access to timely and useful information about threats. Organisations that have been attacked can help others by rapidly sharing information about attacks and threats with organisations which are yet to be affected.

However, organisations do not have strong incentives to share information about breaches. The potential for reputational damage, loss of user and investor trust and legal liability might deter an organisation from sharing information on a breach. Some of those receiving the information might also be direct competitors, perhaps operating similar systems, who could gain a competitive advantage from the information. There are also scenarios in which sharing breach information too soon would increase the risks to which users are exposed. These factors make it harder to encourage organisations to release information on breaches than on defences[93].

[89] Shellshock was a vulnerability that, exploited in the right way, allowed attackers to execute arbitrary commands on affected systems. It particularly affected web and email servers, but many consumer machines would also have been vulnerable.

[90] As confirmed by Chet Ramey on the gmane.comp.shells.bash.bugs newsgroup on 12 October 2014 (See http://thread.gmane.org/gmane.comp.shells.bash.bugs/22418, accessed 10 June 2016).

[91] As reported by Nicole Perlroth in the New York Times on 26 September 2014 (See http://bits.blogs.nytimes.com/2014/09/26/companies-rush-to-fix-shellshock-software-bug-as-hackers-launch-thousands-of-attacks/, accessed on 10 June 2016).

[92] Delamore, B. and Ko, R.K. 2015 *A Global, Empirical Analysis of the Shellshock Vulnerability in Web Applications*. In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 1129-1135). IEEE.

[93] Campbell, K., Gordon, L. A., Loeb, M. P., Zhou, L. 2003 *The economic cost of publicly announced information security breaches: empirical evidence from the stock market*. Journal of Computer Security, 11(3), pp. 431-448 (DOI: 10.3233/JCS-2003-11308).

Although organisations have weak incentives to share some information, they have a strong interest in quickly receiving information shared by others, so they can fix vulnerabilities before they are exploited[94]. This results in a free-rider problem, in which organisations wish to receive information but not to share any themselves. To overcome this problem, existing initiatives rely on a share-to-receive model. These are yet to achieve wide uptake, although their importance is increasingly being realised in commercially sensitive sectors such as banking. In a different complex field, the aviation industry has implemented information-sharing arrangements that have delivered large benefits for the sector and its customers[95].

These barriers to voluntary breach reporting mean mandatory reporting may be necessary, in line with corporate governance requirements to report on risks and events that substantially affect the value or operations of the business. Mandatory reporting should take a risk-based approach to disclosure, with a presumption that peers will benefit from information sharing and that users should be informed if their personal information is disclosed, while recognising that some disclosures will need to be delayed to allow time to fix vulnerabilities.

There are various regimes around the world to encourage the reporting of breaches or other incidents. In the US, 47 states have breach disclosure laws that require organisations to notify individuals of security breaches of information that involve personally identifiable information[96].

In 2015, the EU developed a Directive on Network and Information Security that would result in critical national infrastructure organisations being required to report cybersecurity incidents to a national competent authority if they have 'significant impact'[97].

Going further, a new EU General Data Protection Regulation will be enforced from 2018[98]. The regulation will require breach reporting to an appropriate coordinating authority wherever there is a high risk of harm to an individual, and will impose fines up to 4 per cent of annual worldwide turnover for companies that fail to do so. If these arrangements are implemented in the UK, careful consideration should be given to the characteristics a trustworthy coordinating authority must have in order for these arrangements to be effective (see Recommendation 3).

Compulsory breach disclosure could be accompanied by a shift in legal liability toward the organisations that operate and design digital systems. While stronger legal liabilities for digital systems could strengthen incentives that drive improvement, they would need to be carefully designed. New liability arrangements would need both to fit with the UK's broader legal framework and demonstrably improve security.

[94] Gordon, L. A., Loeb, M. P., Lucyshyn, W. 2003 *Sharing Information on Computer System Security: an economic analysis*. Journal of Accounting and Public Policy 22(6), (DOI: 10.1016/j.jaccpubpol.2003.09.001).

[95] Barach, P. and Small, S.D., 2000. *Reporting and preventing medical mishaps: lessons from non-medical near miss reporting systems*. British Medical Journal, 320(7237), p.759.

[96] National Conference of State Legislators 2016 *Security Breach Notification Laws*. (See http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, accessed on 10 June 2016).

[97] European Commission 2013 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: EU.

[98] European Commission 2013 *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: Belgium. (See http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206342%202013%20INIT, accessed 10 June 2016).

To improve security, responsibilities should be assigned to parties that could effectively discharge them, and could afford to do so. Consumers typically have the least capacity to mitigate risks, while service providers can improve security through system design and implementation, and by taking careful account of real-world use of their products[99]. In most cases this means liability regimes should protect consumers, and prevent system operators from shifting liability to individuals where it is not reasonable to do so. All parties will also need to more clearly understand their responsibilities and potential liabilities if they are to take action to reduce risks[100].

3.5 Sharing information about vulnerabilities and attacks should increase resilience

Information on attacks and vulnerabilities (where there is no breach) can also help organisations improve their defences. Attackers are very good at sharing information; for cyber defences to become responsive and resilient, service providers will need coordinating mechanisms to enable them to share information quickly, clearly, in useful formats and to the right destination.

How and with whom this information is shared will vary depending on the circumstances, and information-sharing mechanisms will need to recognise this. Privacy-enhancing technologies can help overcome barriers by allowing organisations to share information while providing some protection for the organisation's identity (and those of its users). The best methods for sharing information should themselves be the subject of research.

There are existing initiatives to encourage information sharing and reporting. The UK's Cyber-security Information Sharing Partnership was set up in 2013 as a platform for businesses to share threat and vulnerability information, as well as information from third parties. It now has over 2,000 member organisations. Private platforms and organisations also have access to large amounts of data – IBM's X-Force initiative makes 700TB of threat data freely available to researchers and practitioners[101].

To build on these existing initiatives and make information sharing an expected activity for all organisations responsible for digital systems, coordinating institutions will themselves need to be trustworthy, transparent and expert. This will be important to assure organisations that any sensitive information reported will be treated and shared appropriately.

[99] Murdoch, S.J., Becker, I., Abu-Salma, R., Anderson, R., Bohm, N., Hutchings, A., Sasse, A. and Stringhini, G., 2015. *Are payment card contracts unfair?* (See http://sec.cs.ucl.ac.uk/users/smurdoch/papers/fc16cardcontracts.pdf, accessed 10 June 2016).

[100] Becker, I., Hutchings, A., Abu-Salma, R., Anderson, R., Bohm, N., Murdoch, S.J., Sasse, M.A. and Stringhini, G., 2016. *International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms*. Workshop on the Economics of Information Security. (See http://discovery.ucl.ac.uk/1492768/1/Bank_T_C__Comprehension_camera-ready.pdf, accessed 10 June 2016).

[101] Security Intelligence, IBM 2016 *IBM X-Force*. (See https://securityintelligence.com/topics/x-force/, accessed 27 April 2016).

3.6 Improving third party vulnerability reporting should increase resilience

Third-party reporting of vulnerabilities is an important way to make digital systems more robust, and reduce the risks to their users, not least because it allows problems to be fixed before they are exploited.

A set of informal norms have arisen for vulnerability reporting: researchers who identify vulnerabilities typically share them with the affected organisation or vendor, and later the information about the vulnerability is released alongside a fix from the vendor. However, there is much variation in the speed of response, notification of users and distribution of solutions.

There are various incentives that seek to encourage third party reporting (for instance bug bounties, reputational benefits and opportunities to publish findings), but more research would help show what works best. This research should also consider the need for human-to-machine and machine-to-machine sharing, as automated defences and responses become more viable. It should build on experience in other sectors – for instance in aviation, where a history of competitors collaborating on safety features and aircraft design, as well as effective systems for crew to report problems to a third party, have driven substantial improvements in the design of aircraft and their operation[102].

3.7 Cyber-physical systems must be a priority

Cheaper and smaller sensors, advanced robotics and smart materials are combining to increasingly embed digital systems in the physical and biological world. This means that cyber-physical systems are increasingly important, from autonomous vehicles and smart lighting to large-scale industrial control systems for water, electricity or manufacturing. Cyber-physical systems help us manipulate and navigate the physical environment more efficiently and effectively, and in new ways; but they also expose us to new risks. Resilience and security will be particularly important for these systems.

Industrial-scale systems have seen malicious attacks and worrying breaches already. In 2014, attackers gained access to a German steel mill's networks and used knowledge of its industrial control systems to cause millions of euros worth of physical damage to the blast furnace[103]. Discovered in 2010, Stuxnet malware was designed to gain control of the centrifuges of a uranium enrichment facility at Natanz, Iran, and to make them spin in ways that would lead to self-destruction while misleading operators for as long as possible to delay an effective response[104].

Household and individual technologies have not yet been widely targeted, but face similar risks. Researchers have already identified vulnerabilities in smart lightbulbs that allowed them to be turned on or off remotely[105]. Many medically implanted devices lack even modest security[106]. The technology enabling autonomous vehicles is developing rapidly,

[102] Barach, P. and Small, S.D., 2000. *Reporting and preventing medical mishaps: lessons from non-medical near miss reporting systems*. British Medical Journal, 320(7237), p.759.

[103] Langner, R., 2011. *Stuxnet: Dissecting a cyberwarfare weapon*. Security & Privacy, IEEE, 9(3), pp.49-51. (DOI: 10.1109/MSP.2011.67).

[104] Kushner, D. (26 February 2013) *The Real Story of Stuxnet*. IEEE Spectrum (See http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, accessed 26 April 2016).

[105] Goodin, G. (7 July 2014) *Crypto weakness in smart LED lightbulbs exposes Wi-Fi password*s. Ars Technica (See http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/, accessed 26 April 2016)

[106] Halperin, D., Heydt-Benjamin, T., Ransford, B., Clark, S. 2008 *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*. California, USA: 2008 IEEE Symposium on Security and Privacy. (See https://www.computer.org/csdl/proceedings/sp/2008/3168/00/3168a129-abs.html, accessed 27 April 2016)

but questions about how best to ensure the safety of human passengers and other road users are not yet resolved[107].

Cyber-physical risks would also have substantial follow on effects beyond their immediate physical impact. The economic cost of a hypothetical cyber attack leading to three weeks of rolling blackouts in London has been estimated at £12 billion in the first year alone[108].

Security practice for cyber-physical systems is at an early stage compared to that for purely digital systems[109]. Many industrial control devices and networks were not designed with security in mind[110]; in many cases, avoidable mistakes are being repeated, with the lessons learned securing digital systems not being applied in cyber-physical systems. Many control systems have also been in service – or are expected to be in service – for several decades. Greater connectivity to these systems increases their utility, but also their vulnerability to attack. Significant systems engineering research is necessary to develop new defences against such cyber-physical attacks.

Any gaps in the security or reliability of cyber-physical systems, including the Internet of Things, must be addressed as a particular priority. However, it is better to design infrastructure with security in mind than to retro-fit security later[111,112]. In some cases where systems are already in place, it may be more effective to redesign and refresh existing infrastructure and systems than to apply piecemeal approaches to update systems that are decades old. Further research will help to inform strong security engineering standards for these systems.

The UK Government's Centre for the Protection of National Infrastructure (CPNI), established in 2007, offers security advice to organisations and businesses in the public and private sectors that own or operate the national infrastructure and critical national infrastructure. It also coordinates information exchange between operators of critical national infrastructure and commissions research to make cyber-physical systems more resilient. The Research Institute in Trustworthy Industrial Control Systems[113], based at Imperial College London, focuses on infrastructure protection. Actions to rapidly improve the security of cyber-physical systems should build on such existing initiatives.

[107] Greenberg, A. 2015 *Hackers remotely kill a Jeep on the highway – with me in it*. WIRED. (See https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, accessed on 28 April 2016)

[108] Cambridge Centre for Risk Studies (supporting research carried out by Lockheed Martin) 2016 *Integrated Infrastructure: cyber resiliency in society*. Cambridge, UK: Cambridge Centre for Risk Studies. (See http://www.lockheedmartin.com/us/what-we-do/information-technology/cybersecurity/blackout.html#download-report, accessed 27 April 2016).

[109] Hawrylak, P., M., Haney, M., Papa, M., Hale, J. 2012 *Using Hybrid Attack Graphs to Model Cyber-Physical Attacks in the Smart Grid*. 5th International Symposium on Resilient Control Systems (See http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6309311, accessed 27 April 2016).

[110] Slay, J., Miller, M. 2008 *Lessons Learned from the Maroochy Water Breach*. In: Goetz, E., Shenoi, S. (Eds.), Critical Infrastructure Protection. Boston: Springer-Verlag.

[111] Government Office for Science 2014 *Internet of things: making the most of the second digital revolution*. (See https://www.gov.uk/government/publications/internet-of-things-blackett-review, accessed 10 June 2016).

[112] Molotch, H. 2013 *Everyday Security: Default to Decency*. IEEE Security & Privacy, 10(6), pp.84-87.

[113] RITICS is funded by the Cabinet Office and the Engineering and Physical Sciences Research Council.

RECOMMENDATION 4

The incentives for organisations to adhere to rigorous, evidence-based cybersecurity standards should be strengthened.

- Publicly listed companies and public bodies, including Government departments, should benchmark their adherence against cybersecurity standards, and regularly report on this.

- Changes to legal liability for cybersecurity failures should be considered.

- Publicly listed companies and public bodies may in future be required to report cybersecurity breaches to an appropriate coordinating body, under the EU General Data Protection Regulation, if the regulation is implemented in the UK. The identity and characteristics of any coordinating body should be in line with the requirements identified in Recommendation 3.

- The Government should build on existing initiatives to encourage organisations to report cybersecurity attacks and vulnerabilities to an appropriate coordinating body.

- Research is needed to ensure information sharing mechanisms for cybersecurity breaches and vulnerabilities remain effective and continue to improve.

- Research and innovation in cyber-physical system development should be further prioritised to mitigate the substantial risks these systems introduce. It is particularly urgent to increase the standards of cybersecurity practice for critical national infrastructure.

Chapter four
Research

Research

4.1 Cybersecurity research, policy and practice face distinctive challenges

Research needs the right support to be effective in improving cybersecurity policy and practice, and making digital systems more trustworthy and resilient. Cybersecurity's distinctive characteristics include its multidisciplinarity, global reach, and cross-sectoral interests. The research takes place across the academic, commercial and government sectors, such that research policies in all of these sectors will need to adapt.

To ensure future research funding decisions promote world-class work, all research funders must take advantage of international peer review and expertise. Since funding for academic cybersecurity research is concentrated among relatively few major funders, it is particularly important that those funders ensure their processes are rigorous.

Research can help level the playing field between attackers and their targets by improving the tools and techniques at the disposal of cybersecurity practitioners. These improvements can best be realised through ambitious challenge-led research.

Cybersecurity research must cover the full spectrum of inquiry. Discovery research will push fundamental cybersecurity knowledge forward, while clear links between research and practice are needed at the applied end of the spectrum.

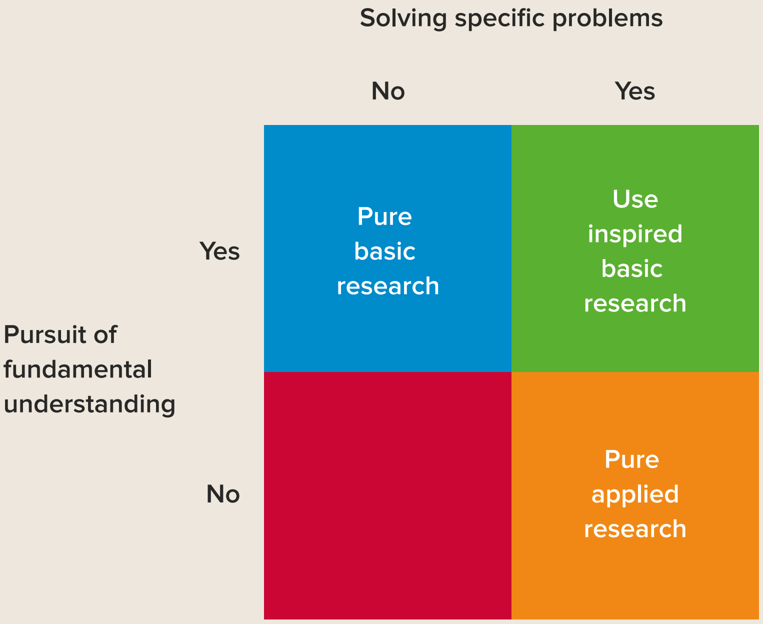
The UK Government has committed to providing £1.9 billion over five years for cybersecurity. Some of this funding will be allocated to research. This funding enables the UK to pursue an ambitious research agenda. To be successful, this agenda will need to have a strong challenge-led element and to enable collaboration across sectors, disciplines and countries. It will also need to support the digital environment's ability to use the products of research and, in turn, to feed back into the research agenda.

BOX 4.1

Spectrum of research

Discovery or basic research generates new knowledge while applied research aims to achieve specific goals or outcomes[114]. Translational or use-inspired research bridges discovery and applied research by expanding knowledge in a particular area to support more goal-orientated work (top right quadrant). The relationship between basic research and applied research is not linear and a cycle of ideas between the people involved in these different kinds of research needs to be iterative in order to push knowledge forward.

Policies should ensure that responsive-mode funding encourages risky, creative, innovative research that has the potential to deliver substantial returns, and that applied investigation benefits from a steady stream of ideas from discovery-oriented work[115]. Policies or funders that 'pick winners' and prescribe solutions are rarely successful.


Solving specific problems
No
Yes
Yes
No
Pursuit of fundamental understanding
Pure basic research
Use inspired basic research
Pure applied research

Pasteur's Quadrant, a concept that categorises research along two dimensions, representing the quest for understanding and the extent to which research is driven by specific problems. Research can be driven by one or both of these[116].

[114] Nurse, P. 2015 *Ensuring a successful UK research endeavour: A review of the research councils*. London, UK: Department for Business, Innovation & Skills. (See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478125/BIS-15-625-ensuring-a-successful-UK-research-endeavour.pdf, accessed 27 April 2016)

[115] Royal Society 2015 *Submission to the Nurse Review of the Research Councils*. London: Royal Society. (See https://royalsociety.org/~/media/policy/Publications/2015/royal-society-submission-to-nurse-review-2015-04-20.pdf, accessed 10 June 2016).

[116] Stokes, D, E. 1997 *Pasteur's Quadrant – Basic Science and Technological Innovation*. Washington D.C.: Brookings Institution Press.

4.2 Levelling the cybersecurity playing field is a grand challenge

Fundamental imbalances in cybersecurity[117] that make strong security elusive – research provides important ways to level the playing field. As discussed in earlier chapters, some of these imbalances can be addressed by reshaping the incentives for organisations; setting clear standards, reporting on cybersecurity efforts, and sharing information on breaches can all help cybersecurity practitioners' capabilities keep pace with attackers. In other cases, government can directly contribute to maintaining security, including by preserving important defensive tools such as robust encryption.

Some imbalances, however, are harder to address. Attackers need only find one vulnerability in a system; most targets remain vulnerable unless all vulnerabilities are fixed[118]. Attackers can be anonymous and hard to locate; target systems are often open to the public and their identities well-known. Attackers are difficult to neutralise and highly resilient; their targets often have relatively little redundancy built in, and find it hard to recover from an attack. Attacks evolve rapidly in response to defensive measures; defences are slower to react[119]. While rates of progress are hard to quantify, there is little reason to believe the gap is narrowing.

Significant progress is needed to match cybersecurity's capabilities with those of attackers. Reducing these imbalances requires a step change in the agility and effectiveness of cybersecurity defences.

Technical and social change mean it is timely to pursue ambitious new approaches to cybersecurity. The amount of data available to develop and test new approaches is greater than ever before. Connected devices are cheap and capable, with enough power to operate relatively advanced security systems, and wide enough distribution to benefit all. Finally, the value of the systems and data to be protected is high and growing.

Some examples of technologies that might contribute to this step change are listed in Box 4.2. These examples are only indicative, and researchers' expertise and judgement should guide decisions about which technologies should be pursued.

Achieving major progress will require substantial research and development; under current arrangements this will take a long time. Delays will reduce the benefits and allow attackers to get further ahead. However, the UK can learn from existing international approaches to achieving an ambitious rate of progress.

In the USA, the Defense Advanced Research Projects Agency (DARPA) funds disruptive research ideas that other parts of government and industry would not or could not develop, carrying them through to the proof-of-concept stage[120]. DARPA does not carry out its own research but funds research in academia and industry[121]. Key principles of DARPA include seconding external experts to deliver programmes (although responsibility for significant research budgets is necessary

[117] National Academy of Engineering, Grand Challenges for Engineering. 2016 *Secure Cyberspace*. (See http://www.engineeringchallenges.org/challenges/cyberspace.aspx, accessed 27 April 2016).

[118] Anderson, R. 2001 *Why Information Security is Hard – an economic perspective*. Louisiana, USA: Proceedings 17th Annual Computer Security Applications Conference (See https://www.acsac.org/2001/papers/110.pdf, accessed 27 April 2016).

[119] Rate of zero-day exploits increased by 115 per cent from 2014 to 2015 (See Symantec 2016 *Internet Security Threat Report*. California, USA: Symantec (https://www.symantec.com/security-center/threat-report, accessed 27 April 2016).

[120] Fuchs, E. R. H. 2009 *The road to a new energy system: cloning DARPA successfully*. Issues in Science and Technology, 26(1). (See http://issues.org/26-1/fuchs/, accessed 27 April 2016).

[121] Defence Advanced Research Projects Agency. 2012 *Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH)*. (See http://www.darpa.mil/program/clean-slate-design-of-resilient-adaptive-secure-hosts, accessed 27 April 2016).

BOX 4.2

New technologies for a step change in cybersecurity

These emerging advances in technology would help deliver a step change in cybersecurity[122].

- Extending encryption to allow computation to be performed directly on encrypted data, to enable full end-to-end data security.
- Quantum-safe cryptography including implementation-efficient algorithms that are resistant to advances in Quantum Computing, should this be necessary.
- Verified trustworthy systems, including through security by design.
- The application of formal methods to safety critical applications such as Critical National Infrastructure, industrial process control and medical applications.
- New data anonymisation methods for enhancing the protection of user identity, privacy and confidentiality.
- Strengthening the chain of custody of data or transactions using distributed ledger technologies such as blockchain.
- Technologies for intrusion, malware and distributed denial of service detection including new methods for the real-time application of network traffic analysis based on advanced machine learning algorithms.
- Malware-based defences to 'live with the threat', analogous to biological defences in living species.
- New technologies and models for Internet of Things network security, reflecting their highly distributed nature and the intrinsic need for security by design.
- New resource-constrained crypto and multi-factor authentication technologies for the Internet of Things and other low cost, low energy systems.
- New security architectures for hyperscale cloud infrastructures and highly virtualised computing and communications systems.
- Physical layer security for securing communications when cryptography is not possible due to limitations on computational capability, or to the network architectures involved.

to attract leading researchers); maintaining flat management structures to support flexible and rapid decision making; and articulating research challenges without defining specific solutions, to facilitate cross-disciplinary collaborations[123]. This individual-led approach can reduce risk aversion and open up more speculative possibilities that may have higher pay-offs than more traditional approaches.

This idea has been proposed previously in the UK. In 2006, a study commissioned by the UK Ministry of Defence recommended that some of its research funding should be modelled on DARPA and applied to a small number of targeted initiatives. In 2014, the UK Government announced that Innovate UK would investigate new ways of working with the Research Councils to learn from DARPA to identify and exploit disruptive technologies[124].

[122] This list is indicative only; the set of technologies that could contribute to the needed step change is likely to be broader than this list, and will continue to evolve rapidly.

[123] Fuchs, E. R. H. 2009 *The road to a new energy system: cloning DARPA successfully*. Issues in Science and Technology, 26(1). (See http://issues.org/26-1/fuchs/, accessed 10 June 2016).

[124] HM Treasury & BIS 2014 *Our Plan for Growth: science and innovation*. Policy Statement. London: HM Treasury & BIS. (See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/387780/PU1719_HMT_Science_.pdf, accessed 27 April 2016).

The challenges faced in cybersecurity make it a prime candidate for a DARPA-like, challenge-led approach. The UK should establish a funding stream and organisation, with each funded project having a clear ambition and purpose, and being led by an individual world-class project leader with an excellent track record.

Peer guidance should inform the overall programme direction, the selection of high level goals and the awarding of funding to project leaders, but the actual approach pursued in each individual project should be determined by the project leader.

These projects should be based on innovative and lightweight management structures, promoting agility and responsiveness. Collaborative work and secondments should be used to ensure projects have the expertise they need. Deliverables should be of whatever type will have greatest impact for the project in question, and may go well beyond prototypes or academic papers. The funder of the research should receive licences to use the results for their own purposes, while the research team involved should retain the ability to licence and develop their findings for other customers and users. The starting position for participating researchers should be an unencumbered approach to licensing.

This approach would be sufficiently different from current funding approaches that existing organisations are unlikely to be well-suited to administering the scheme. While existing approaches can identify high quality proposals or encourage collaboration with industry, they are less well suited to funding the self-directed pursuit of ambitious objectives that lie at or outside the margin of what is known to be possible. Existing approaches will remain important, and innovative approaches should run alongside more traditional approaches.

An appropriate institution to develop and deliver this funding stream should be identified during the review of the cybersecurity institutions the UK will need in future (Recommendation 3).

This approach would be particularly well-suited to cybersecurity research because of the potential for rapid progress and wide benefits in networked and scalable systems, and the importance of the issues at hand. It should also be considered for similar research areas, with the lessons learned in implementing this research strand being expanded beyond cybersecurity.

RECOMMENDATION 5

The Government and research funders should introduce new funding and management structures for an ambitious, challenge-led research funding organisation, focusing on cybersecurity in the first instance. This organisation would identify key challenges and provide flexible support for excellent researchers to tackle them, with a presumption of unencumbered access to the solutions.

4.3 Research and policy must bridge national, disciplinary and sectoral boundaries

4.3.1 Global expertise

Cyber threats and vulnerabilities are global in nature. Affected organisations are distributed around the world, and attacks often cross national borders. Research and innovation are also global – the best researchers may be located anywhere in the world, and their insights can have global applications.

To produce world-class research, the UK will need to take advantage of global expertise not only in doing research, but also in making research funding decisions. Peer review should draw on world-class expertise to allocate funding to the most promising research topics and researchers. While some research funders do make use of international peer review, this approach should be widely adopted to ensure all research funding decisions promote excellent, world-class research.

The global nature of cybersecurity means that UK research and practice can be strengthened through collaboration with talented researchers from outside the UK. Creating more opportunities to work with the best researchers in the world, wherever they are, will also make the UK a more attractive destination for excellent researchers.

4.3.2 Multidisciplinary approaches

Cybersecurity practice must take account of human, social, legal, regulatory and technological factors. The complexity of digital systems means that the connections between the social, human and technological elements of a system themselves create opportunities for exploitation. Research challenges are therefore multidisciplinary, including the social sciences and humanities as well as engineering and the physical, mathematical and computer sciences.

Usability, both for users and developers, is a key area that relies on insights from multiple disciplines. Users can only be secure if they have access to security tools that are easily deployed, and which do not introduce unnecessary friction into their use of digital systems. Similarly, developers must have usable security tools – security should be easy to implement in new systems.

4.3.3 Cross-sectoral partnership

Digital systems are used across military, government, business and social settings alike, and so all of these sectors are heavily invested in the successful practice of cybersecurity. Real-world problems, clearly articulated, can be a strong incentive for collaborative research[125].

These distinct sectors also have distinctive needs. For example, the National Audit Office has suggested that the UK Government has made good progress in improving its understanding of the most sophisticated threats to national security, but has a varied understanding of threats to wider public services[126].

There are existing initiatives to drive joint investment by industry and government – notably, CyberInvest, a dedicated industry and government scheme for funding the translation of research. However, collaboration should also include a range of different ways of working, including joint funding, staff transfers or secondments, and jointly managed ventures. To enable these kinds of collaborations, connections between academic researchers and other sectors will be important. Researchers must be alert to the sectors where their work is applied, and any barriers to researchers building and maintaining connections to these sectors should be minimised.

[125] Dowling, A. 2015 *The Dowling Review of Business-University Research Collaborations*. (See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440927/bis_15_352_The_dowling_review_of_business-university_rearch_collaborations_2.pdf, accessed 10 June 2016).

[126] Morse, A. 2014 *Update on the National Cyber Security Programme*. London: National Audit Office. (See http://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme.pdf, accessed 10 June 2016).

RECOMMENDATION 6

Research Councils and other research funders must draw effectively on world-class expertise. Research funders should go further to: ensure peer review involves the best expertise available internationally; encourage multidisciplinary research in cybersecurity; encourage international research collaboration with competent parties; and reduce barriers to academic researchers engaging with industry and the public sector.

4.4 The proposed changes will drive a more responsive cybersecurity research agenda

Over time, the cybersecurity research and innovation agenda will be shaped and strengthened by researchers, practitioners and customers, including through: stronger multidisciplinary, cross-sectoral and international collaborations; a stream of challenge-led research opportunities; and a self-improving, resilient system of cybersecurity. These changes will ensure the research system remains responsive, relevant and high-impact. To support and develop this self-improving system, the right research is needed in the short term too.

Two new cybersecurity research funding tracks have recently been established in the UK – the Academic Centres of Excellence Cyber Security Research (ACE-CSR)[127] programme, and three Research Institutes[128] in cybersecurity. The institutes are: the Research Institute in Science of Cyber Security[129], which is focused on building the evidence base for cybersecurity, and moving cybersecurity decision-making onto stronger foundations; the Research Institute in Automated Program Analysis and Verification[130], focused on provably correct and secure programs; and the Research Institute in Trustworthy Industrial Control Systems[131], focused on the security of industrial control systems.

Queen's University Belfast, one of the ACE-CSRs, also hosts the Centre for Secure Information Technologies, one of seven UK Innovation and Knowledge Centres. The Centre is funded jointly by the Engineering and Physical Sciences Research Council, Innovate UK and Invest Northern Ireland. It aims to be a global innovation hub for cybersecurity and runs a range of activities, from specialised education through to commercialisation of research.

[127] For more information see https://www.cesg.gov.uk/articles/academic-centres-excellence-cyber-security-research.

[128] For more information see https://www.cesg.gov.uk/articles/research-institutes.

[129] For more information see http://www.riscs.org.uk/.

[130] For more information see http://verificationinstitute.org/.

[131] For more information see https://www.epsrc.ac.uk/newsevents/news/cyberattackthreatscriticalinfrastructure/.

Each of these initiatives is making an important contribution to building the capacity for cybersecurity research and to improving cybersecurity practice in the UK. To build on these existing efforts, the Royal Society will convene discussions between academic researchers, industry and government to identify the priority research topics that should be pursued over the coming period, and which would help build a cybersecurity system that demands and relies on robust, world-leading research.

Some aspects are likely to be central in the short term, supporting a shift to a self-improving and resilient system which demands and relies on robust, world-class research:

- **Trust** Ensuring trust is not eroded, and giving individuals a sound basis on which to make judgements about trust will help enable new digital solutions.
- **Data and privacy** Attitudes to privacy and means of managing privacy risks are a growing area of research, but give rise to challenging dilemmas and contradictions. To build trust and understanding (and demand for trustworthy systems) it will be important to give people the controls they need – and want – to be secure online.
- **Encryption, authentication and anonymisation** Encryption, authentication and anonymisation are important underpinning technologies for security across digital networks. Ensuring they are robust and widely-deployed will help build the foundations of more secure systems.
- **Resilience** Greater ability to operate after and during breaches, to design systems that resist breaching and to measure the organisation's degree of resilience will all be necessary for success and security in the digital economy.
- **Information sharing** Learning from the experience of others will help organisations improve their security and respond more effectively to threats, but encouraging sharing is challenging.
- **Risk management and modelling** Cyber risks are distinctive in their scale, reach and complexity, making it difficult for organisations to factor those risks into their decision-making. Fuller understanding of how cyber risks manifest, how they can be controlled, and the damage they cause will help organisations become discerning users and creators of sound research evidence.
- **Regulation and policy** The complexity, responsiveness and reach of digital systems make regulating and governing the digital world highly challenging. Achieving success through policy interventions will depend on a sound understanding of which approaches work well in this environment, and where new frameworks or methods are needed.
- **Asymmetries and security deficits** The substantial deficits and asymmetries that characterise the current cybersecurity landscape will need to be reduced in order for defences to keep up with attacks.

Indicative examples of research topics under each of these areas are outlined in Box 4.3.

BOX 4.3

Cybersecurity research and innovation topics necessary to support implementation of this report's recommendations

Trust

- Measuring and reporting on competence, trustworthiness and trust.
- Providing verified assurance that recognises continuous improvement (eg kitemarks).
- Robust methods for systems to demonstrate reliability through strong evidence.

Data and privacy

- Characterising privacy online and understanding privacy behaviours, needs and harms.
- Managing potential conflicts between individual privacy and open data.
- Developing new legal and social approaches in response to global data flows.
- Managing privacy risks on social media using new kinds of data controls.

Encryption, authentication and anonymisation

- Enhancing robust encryption, including protecting metadata as well as the data itself.
- Increasing the robustness of authentication between users and with organisations.
- Robust methods of anonymising data.
- Robust methods of supporting anonymous communication.
- Easing the deployment of secure systems by non-specialists with usable software libraries.

Resilience

- Enabling wide adoption of security by design (technical, economic, legal and social).
- Developing systems which continue to operate even when parts have been compromised.
- Reducing time to fix discovered vulnerabilities (technical, legal and policy).
- Measuring organisational competence through continually evolving measures.
- Reducing the risk from social engineering.

BOX 4.3 (continued)

Information sharing

- Improved processes for reporting vulnerabilities, exploits and unsuccessful attempts.
- Encouraging and enabling safe sharing of sensitive data between untrusting parties.

Risk management and modelling

- Improving decision-making through metrics and methodologies to quantify cybersecurity risks.
- Strengthening risk management controls, including for insider threats, while promoting productivity.
- Increasing understanding of system level threats through new risk models, simulations and massive-scale modelling of aggregated risks.
- Managing risks when computer systems can operate on the physical environment.

Regulation and policy

- Informing and strengthening the regulation of data processing.
- Identifying vulnerabilities and testing risk management for CNI, including assessing CBEST (the Bank of England's cybersecurity testing framework, which takes a holistic approach and is based on replication of realistic threats) to assess its broader applicability.
- Ensuring government policies and regulators' tools best promote strong cybersecurity.
- Better aligning incentives to provide cybersecurity and reduce negative externalities.

Asymmetries and security deficits

- Improving security of deployed devices through retro-fitting.
- Measuring and predicting current and future security deficits and resulting breaches.
- Delivering effective support and guidance to organisations on technical and social attacks.

Chapter five
Translation

Translation

5.1 Innovative research-based cybersecurity requires diverse ideas and approaches

Research is a key generator of new ideas and approaches to cybersecurity threats and risks. These can deliver substantial benefits for organisations and users, but first they must be translated into products and services.

To effectively tackle hard to predict and multi-faceted problems like cybersecurity, organisations need ready access to the right tools to respond to unanticipated threats. They will need to draw on a diverse set of reliable, proven ideas and approaches.

Startups, early-stage companies and academic researchers are important sources of innovative and disruptive ideas[132]. Often these ideas originate in the worldwide research community, or early-stage companies collaborate with researchers to bring an idea to market.

However, digital systems are characterised by network economies (users prefer a product or platform that already has many existing users) and by economies of scale (products typically have high initial development costs, with very small costs for each extra customer served). Both factors make large companies an important part of the digital economy. This has advantages and disadvantages – notably, a lack of smaller companies is likely to mean less diversity in ideas and approaches.

The high start-up costs, difficulty building a customer base, and competition from established companies make it hard for small companies with new ideas to grow and establish themselves. In addition, the UK's early-stage companies are often acquired by larger companies, usually based outside the UK. These patterns may limit the number of proven ideas and approaches available in the marketplace.

As the diversity of ideas grows and better information becomes available, users, investors and regulators could be expected to become more discerning security buyers, reducing the need for support for some ideas. Government should monitor the need for support, and take account of changing market conditions, but some technologies with large spillover benefits may continue to require funding or other public support.

5.2 New approaches must be evaluated and demonstrated

Research and development need to produce credible defences against cyber threats, and this credibility needs to be demonstrated before these defences are implemented in real-world systems. To do this, researchers require access to data and test environments that mimic real-world threats and environments. These must reflect current threats and trends, and be maintained and regularly reviewed to avoid defences being based on out-of-date or unrepresentative data.

Similar systems exist in other countries and sectors, and could provide useful lessons. In the USA, for instance, the Department for Homeland Security provides researchers with access to the Protected Repository for the Defence of Infrastructure Against Cyber Threats (PREDICT), to which UK researchers were given access in 2015[133]. The Department for Homeland Security also provides access to

[132] Maughan, D., Balenson, D., Lindqvist, U. & Tudor, Z. 2013 *Crossing the "Valley of Death": transitioning cybersecurity research into practice*. IEEE Security & Privacy Magazine, 11(2), pp.14-23 (DOI: 10.1109/MSP.2013.31).

[133] IMPACT 2016 *Welcome to impact*. (See https://www.predict.org/Default.aspx?tabid=40&ctl=ViewFullNews&newsIndex=13&mid=871&selectmid=871, accessed 27 April 2016).

the Cyber Defence Technology Experimental Research (DETER) test facility. In the UK, the Cambridge Cloud Cybercrime Centre (established in 2015) is seeking to establish a large and diverse data set on cybercrime, and to create a sustainable and internationally competitive centre for academic research into cybercrime.

Data and test facilities will be an important part of the UK's national resource for cybersecurity research. To help researchers demonstrate that their solutions are fit for purpose, the UK should establish a national operational data and test facility mechanism, with key industry partners.

RECOMMENDATION 7

The Government should promote the creation and uptake of real-world test facilities, including data sets, that can be accessed and shared as a national resource to allow the robust evaluation of new cybersecurity research and products.

5.3 Funders can do more to support diversity and innovation

5.3.1 Government procurement

Given the importance of cybersecurity, the value of a diverse set of ideas and approaches in this field, and the challenges in getting these ideas to a wide market, there is a role for government and others in directly supporting greater diversity. Government can encourage diversity through policy measures, through its procurement arrangements, or through direct financing.

Government spending represents one third of the market for cybersecurity products and services[134], giving it the power to influence the shape and structure of the market. Government has recognised that its procurement policies can have a positive effect on market structure, introducing measures like the Centre for Defence Enterprise[135] and the Small Business Research Initiative (SBRI), which has recently been used to fund some cybersecurity procurement activities.

The SBRI is a useful innovation, providing valuable opportunities for early-stage and small to medium enterprises (SMEs). For the best results, government procurement, including through the SBRI, should encourage and allow bidders to take advantage of the full range of excellence and expertise available across SMEs, academia and industry.

RECOMMENDATION 8

The Government should expand the engagement of SMEs and academic researchers with industrial partners through procurement mechanisms, including the Small Business Research Initiative.

[134] Pierre Audoin Consultants (research sponsored by BIS) 2013 *Competitive analysis of the UK cyber security sector*. (See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf, accessed on 10 June 2016).

[135] For more information see https://www.gov.uk/government/organisations/centre-for-defence-enterprise.

5.3.2 Financing for early-stage companies

Government can also directly support small or early-stage cybersecurity businesses with financing aimed at increasing the diversity of ideas and approaches.

Financing schemes should support early-stage companies as they establish their customer base and prove the viability of innovative ideas and approaches. These schemes should seek to establish a sustainable and vibrant community of cybersecurity SMEs that are well-placed to anticipate and respond to emerging issues, and to generate better solutions for existing problems.

Early stage cybersecurity companies in the UK rely largely on individual or angel investors and only a small number of venture capital firms invest in cybersecurity. There is a scarcity of funding available, in part due to investors' limited expertise in cybersecurity. To address this, financing support should make use of expert advice and management, and it may be appropriate to establish specialised funds with particular remits.

Government financing should differentiate itself from commercial funding by focusing on ideas with large potential spillover benefits that might not otherwise be funded. These spillovers are common in cybersecurity, because the organisations which must implement security arrangements are often not the ones that suffer most in the event of a breach. For example, tools that prevent users' machines being used against others, open source software, and approaches that make the entire network or ecosystem more resilient are all likely to have large benefits that will not be reflected in financial returns.

To support this aim, in 2015 the Government announced CyberInvest, a dedicated industry and government scheme for funding the translation of research. To date, 18 companies have committed to investing £6.5 million over the next 5 years[136]. In 2015, the Government also announced a £165 million Defence and Cyber Innovation Fund to use the government's procurement power to help cybersecurity and defence start-ups secure a first big customer[137]. While these activities are providing valuable support for ideas that aim to become commercially successful, it is important that public funding is also used to support innovative ideas that have broader non-financial benefits.

RECOMMENDATION 9

The Government should establish one or more further dedicated support funds under specialised and professional management to support the financing of cybersecurity innovation, targeting cases where innovation would have spillover benefits but might not otherwise be funded.

[136] For more information see https://www.gchq.gov.uk/press-release/£65-million-cyberinvest-scheme-boost-world-class-uk-cyber-security-research.

[137] Osborne, G. 2015 *Chancellor's speech to GCHQ on cyber security*. (See https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security, accessed on 10 June 2016).

5.3.3 University technology transfer policies

Finally, academic research is an important source of new ideas and approaches. University commercialisation policies affect the flow of these new ideas into commercial opportunities. Universities and their technology transfer offices (TTOs) can help promote a diverse set of ideas in cybersecurity by encouraging a free flow of ideas and people from academia into commercial settings.

The nature of cybersecurity products means it is important for these transfers to be rapid and generally unfiltered by attempts to assess viability, since that is inevitably hard to pre-judge.

Cybersecurity research ideas, once translated into products, can be rapidly scaled and deliver large benefits. However, it is difficult to predict which cybersecurity ideas will be successful, because of: the technical complexity of the products; the complexity of patterns of demand; and complex market dynamics, due to the economies of scale, network effects and complex supply chains involved.

In this situation, TTOs should prioritise knowledge exchange over short-term income generation, as recommended by the Dowling Review[138]. Further work is needed to ensure contracts and intellectual property agreements do not unnecessarily limit the flow of ideas from universities into implementation.

An effective TTO can accelerate knowledge exchange and technology transfer, but there is some confusion about whether TTOs' goal should be to generate income for universities, or to create benefit for the wider community. As noted in the Dowling Review, TTOs measure of success should be effectiveness in supporting translational activities over the long term, not short-term revenue generation. For cybersecurity in particular, there are large potential public gains, resulting from the spillover benefits associated with many security investments[139]. This means that the public is better served by greater translation, rather than a focus on financial returns.

DARPA's research funding and licensing arrangements provide one model for intellectual property management that does not limit the spread or implementation of ideas; the US government retains the right to licence back the results from the programme of research for its own use only, but products and inventions are otherwise largely unrestricted in how they can be commercialised and licensed to others. This model could be adapted to the university setting, together with its objectives of maximising the spread and of ideas, and the incentive to innovate.

RECOMMENDATION 10

Universities and their technology transfer offices should focus on the volume of commercialisation opportunities, recognising the difficulty of predicting the success of cybersecurity initiatives, and taking into account broader benefits beyond the expected financial return.

[138] Dowling, A. 2015 *The Dowling Review of Business-University Research Collaborations*. (See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440927/bis_15_352_The_dowling_review_of_business-university_rearch_collaborations_2.pdf, accessed on 10 June 2016).

[139] Bauer, J.M. and Van Eeten, M.J., 2009. *Cybersecurity: Stakeholder incentives, externalities, and policy options*. Telecommunications Policy, 33(10), pp.706-719. (DOI: 10.1016/j.telpol.2009.09.001).

Appendices

Appendices

Appendix 1: About this report

This report considers the emerging cybersecurity research challenges in the next five to ten years and what policy frameworks are necessary to address these challenges.

Methodology

An expert Steering Group was set up to oversee this project and help analyse the evidence gathered (see Appendix 2). An open call for evidence was held during December 2013 and January 2014. A series of one day workshops were held in January to May 2014 to explore specific themes identified in the evidence call. These activities were complemented by desk research, seminars, meetings and other consultations (see Appendix 3).

Acronyms	
ACE-CSR	Academic Centre of Excellence in Cyber Security Research
ARM	Formerly: Advanced RISC Machine
BSI	British Standards Institute
CBEST	An intelligence-led testing framework to test resilience to cyber attack of financial firms, infrastructure providers and regulators.
CERN	The European Organization for Nuclear Research
CESG	Formerly: Communications Electronics Security Group
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure
DARPA	Defense Advanced Research Projects Agency
DETER	Defence Technology Experimental Research
EDSAC	Electronic Delay Storage Automatic Calculator
GCHQ	Government Communications Headquarters
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PREDICT	Protected Repository for the Defence of Infrastructure Against Cyber Threats
SBRI	Small Business Research Initiative
TTO	Technology Transfer Office

Appendix 2: Steering Group, Project Team and Review Panel

Steering Group members

The members of the Steering Group involved in this report are listed below. Members acted in an individual and not a representative capacity, and declared any potential conflicts of interest. Members contributed on the basis of their own expertise and good judgement.

Co-chairs	
Professor Andrew Hopper CBE FREng FRS	Professor of Computer Technology, Head of Department, Computer Laboratory, University of Cambridge
Professor John McCanny CBE FREng FRS	Director of the Institute of Electronics, Communications and Information Technology, Queen's University Belfast
Members	
Professor Ross Anderson FREng FRS	Professor of Security Engineering, Computer Laboratory, University of Cambridge
Professor Philip Bond	Visiting Professor, Department of Engineering Mathematics and Computer Science, Bristol University
Mr Martin Borrett	IBM Distinguished Engineer, CTO IBM Security Europe
Professor Sadie Creese	Professor of Cybersecurity, Department of Computer Science, University of Oxford
Dr Steven Murdoch	Principal Research Fellow, Department of Computer Science, University College London
Professor Angela Sasse FREng	Director, UK Research Institute in Science of Cyber Security (RISCS), Department of Computer Science, University College London
Mr Alex van Someren	Managing Partner, Early Stage Funds, Amadeus Capital Partners
Dr Claire Vishik	Security, Privacy Standards and Policy Manager, Intel Corporation UK

Royal Society Staff

Staff from across the Royal Society contributed to the production of this report. The Royal Society acknowledges the contributions of project team members in managing this project, carrying out research and analysis, and drafting the report:

The Royal Society Science Policy Centre staff	
Elinor Buxton (until February 2014)	Policy Adviser
Dr Claire Craig (from February 2016)	Director of Science Policy
Belinda Gordon (May-November 2015)	Senior Policy Adviser
Dr Nick Green (until February 2016)	Head of Projects
Alice Jamieson (until May 2016)	Policy Adviser
Ben Koppelman (until February 2016)	Senior Policy Adviser
Aaron Maras (from January 2016)	Senior Policy Adviser
Tony McBride (until December 2015)	Director of Science Policy
Siobhan McMahon, Lauren Ratcliffe, Laura Schofield, Marcus Shepheard and David Williams (various periods)	Policy Interns and Project Assistants

Review Panel

This report has been reviewed by an independent panel of experts, before being approved by the Council of the Royal Society. The Review Panel members were not asked to endorse the conclusions or recommendations of the report, but to act as independent referees of its technical content and presentation. Panel members acted in a personal and not a representative capacity and were asked to declare any potential conflicts of interest. The Royal Society gratefully acknowledges the contribution of the reviewers.

Chair	
Professor Sir John Pethica FREng FRS (until November 2015)	Former Vice President and Physical Secretary, Royal Society
Professor Alexander Halliday FRS (from November 2015)	Vice President and Physical Secretary, Royal Society
Review panel	
Professor Dieter Gollmann	Head of Department, Security in Distributed Applications, Technical University of Hamburg-Harburg
Professor Andrew Hopper CBE FREng FRS (until July 2015)	Professor of Computer Technology, Head of Department, Computer Laboratory, University of Cambridge
Dr Richard Horne	Cyber Security Partner, PwC UK
Paul Kearney	Chief Security Researcher at BT
Dr Neil Manson	Senior Lecturer in Philosophy, Lancaster University
Professor Vincent Poor ForMemRS FREng FRSE	Professor of Electrical Engineering, Princeton University
Dr Martin Sadler OBE	Vice President and Director, Security and Cloud Lab, HP
Professor Tieniu Tan FREng	Professor of Computer Vision and Pattern Recognition, Deputy Secretary General of the Chinese Academy of Sciences
Professor Sir Mark Welland FREng FRS	Professor of Nanotechnology, University of Cambridge

The Royal Society would also like to thank the following individuals for providing comments on previous drafts:

Expert readers	
Adjunct Associate Professor Mary Aiken	Geary Institute, University College Dublin
Professor Sir John Beddington CMG HonFREng FRS	Senior Adviser, Oxford Martin School
Bird & Bird LLP	
Professor Brian Collins FREng	Chair of Engineering Policy, University College London
Professor Jon Crowcroft FREng FRS	Marconi Professor of Communications Systems, University of Cambridge
Professor Dame Wendy Hall DBE FREng FRS	Professor of Computer Science, University of Southampton
Professor Nick Jennings CB FREng	Vice-Provost (Research), Imperial College London
Professor Sir Peter Knight FRS	Senior Research Investigator, Imperial College London
Dr Herb Lin	Chief Scientist, Computer Science and Telecommunications Board, NAS
Dr Mike Lynch OBE DL FREng FRS	Founder, Invoke Capital
Dr Steve Marsh	Formerly Information Assurance Advisory Council and Cabinet Office
Elisabetta Zaccaria	Founder, cyberY

Appendix 3: Evidence gathering

Evidence was gathered during the project in the following ways:

- A formal call for evidence at the start of the project
- Events on specific themes that arose during the project
- Meetings with key stakeholders

Call for evidence

An open call for evidence was issued in November 2013, following the Steering Group’s first meeting, which resulted in 28 responses. All respondents are listed below:

Respondents

Bird & Bird LLP

Mark Brown, EY

Dr Richard Chisnall, Facilitate Industry and Research in Europe Project

Professor Peter Cochrane OBE FREng

Dr Robert Ghanea-Hercock, BT plc

Mike Hawkes, MHInvent

Professor Michael Huth, Imperial College London

David Jones, Westgate Cyber Security

Dr Mike Lynch OBE DL FREng FRS, Invoke Capital

Dr Jamie MacIntosh, University College London

Professor Danny McCaughan OBE FREng, McCaughan Associates

Professor Leo Motus, Estonian Academy of Sciences

Dr Igor Muttik, McAfee Labs

Fraser Nicol, EY

Professor Awais Rashid, Lancaster University

Ian Ritchie CBE FRSE FREng, Vice President, Royal Society of Edinburgh

Professor Mark Ryan, University of Birmingham

Adam Shostack

Professor Peter Sommer

Hilary Sutcliffe, Matter

Dr Martyn Thomas CBE FREng

Dr Nithin Thomas, SQR Systems Limited

UK Computing Research Committee

University of Southampton

Joe Weiss, Applied Control Solutions

Professor Sir Alan Wilson FRS, University College London

Elisabetta Zaccaria, cyberY

Appendix 4: Acknowledgements

This project would also not have been possible without contributions from a range of individuals, including those who met with us, contributed through seminars or participated in other consultations. In particular we wish to thank:

Acknowledgements

Richard Anning, Institute of Chartered Accountants in England and Wales

Adjunct Associate Professor Mary Aiken, Geary Institute, University College Dublin

Dr Nick Appleyard, Innovate UK

Stuart Aston, Microsoft

Dr David Bailey CTO, Cyber BAE Systems Applied Intelligence

John Baird, EPSRC

Adam Beautement, Research Institute in the Science of Cyber Security

Professor Isaac Ben-Israel

Dr Alastair Beresford, University of Cambridge

Hugh Boyes, IET

Jon Bradford, Springboard/Techstars London

Professor Pamela Briggs, Northumbria University

Professor Ian Brown, Oxford Internet Institute

Mark Brown, EY

Jon Browning, Office for Cyber Security and Information Assurance, Cabinet Office

Ben Buchanan, King's College London

Dr Andrew Bud, University College London/ iProov Limited

Dr Mike Burrows FRS, Google Inc

Robert Carolina, Royal Holloway, University of London

Emma Carr, Big Brother Watch

Tristan Caulfield, Research Institute in the Science of Cyber Security

Centre for the Protection of National Infrastructure

Chris Chew, Head of Policy, Export Control Organisation

David Chinn, McKinsey

Dr Richard Clayton, University of Cambridge

Dr Neil Cohen, Centre for Applied Science and Technology, Home Office

Dr Lizzie Coles-Kemp, Royal Holloway University of London

Professor Brian Collins CB FREng, University College London

Professor Jason Crampton, Royal Holloway, University of London

James Crawford, CERT-UK

Mr Mark Crosbie, Facebook

Professor Jon Crowcroft FREng FRS, University of Cambridge

Catherine Crowe, Home Office

Defence Science and Technology Laboratory

Dr Rowan Cruft, University of Stirling

Cory Doctorow, Electronic Frontier Federation

Dr Donna Dodson, National Institute of Standards and Technology

Sam Dowling, Home Office

Professor Bill Dutton, Oxford Internet Institute

Professor Paul Ekblom, Central Saint Martins

Jeremy Epstein, National Science Foundation, USA

Dave Evans, Bank of England

Hamid Falaki, Digital Catapult

Dr Andrew Fielder, Research Institute in the Science of Cyber Security

Cédric Fournet, Microsoft Research

Paddy Francis, Airbus Defence and Space

Paul Galwas, Digital Catapult

Dr Flavio Garcia, University of Birmingham

Professor Philippa Gardner, Director of the Research Institute in Automated Program Analysis and Verification, Imperial College London

Dr Godfrey Gaston, Titan IC Systems

Dr Robert Ghanea-Hercock, BT Technology

Kirstin Gillon, Institute of Chartered Accountants in England and Wales

Andy Gordon, Microsoft Research

Acknowledgements (continued)

Evgeny Grigorenko, Kaspersky Lab

Dr Thomas Gross, Newcastle University

Dr Zeynep Gurguc, Research Institute in the Science of Cyber Security

Neil Hampson, PwC

Professor Chris Hankin, Imperial College London

Dr William Harvey, Office for Cyber Security and Information Assurance, Cabinet Office

Hermann Hauser FRS, Amadeus Capital Partners

Matthew Hogg, Cyber Risk and Insurance Forum

Richard Horne, PwC

Alex Hulkes, EPSRC

Fredrik Hult, Bank of England

Professor Christos Ioannidis, University of Bath

Sir Roland Jackson, Executive Chair, Sciencewise, BIS

Dr Nigel Jefferies, Huawei Technologies

Professor Nick Jennings CB FREng, Imperial College London

Dr Marina Jirotka, University of Oxford

Katerina Joannou, Institute of Chartered Accountants in England and Wales

Professor Adam Joinson, University of the West of England

Nick Kingsbury, Accumuli plc

Dr Mark Lacy, Lancaster University

Ben Laurie, Google

Eliot Lear, Cisco

Eireann Leverett, University of Cambridge

Professor Michael Levi, Cardiff University

Professor Mark Levine, University of Exeter

Dr Makayla Lewis Researcher, Research Institute in the Science of Cyber Security

Dr Herb Lin, National Academies of Science

Professor Paul Luff, King's College London

Dr Emil Lupu, Imperial College London

Dr Mike Lynch OBE DL FREng FRS, Invoke Capital

Dr Steve Marsh, IAAC

Dr Andrew Martin, University of Oxford

Paul Martin, Plextek

Dr Douglas Maughan, Director, Cybersecurity Division Homeland Security, USA

Kris McConkey, PwC

Professor Janet McDonnell, Central Saint Martins

Jamie Miller, Office for Cyber Security and Information Assurance, Cabinet Office

Dr Granville Moore, University College London

Dr Karenza Moore, Lancaster University

Dr Charles Morisset, Research Institute in the Science of Cyber Security

Miranda Mowbray, HP Labs

Dr Steve Moyle, Secerno Limited

Andy Nicholson, Head, Centre for Defence Enterprise

Fraser Nicol, EY

Sara Ogilvie, Liberty

Austen Okonweze, BIS

Edin Omanovic, Privacy International

Professor Maire O'Neill, Queen's University Belfast

Dr Tom Ormerod, University of Surrey

Emily Orton, Darktrace

Dr Manos Panaousis, Research Institute in the Science of Cyber Security

Dr Davide Papini, Research Institute in the Science of Cyber Security

Dr Simon Parkin, Research Institute in the Science of Cyber Security

David Petrie, Institute of Chartered Accountants in England and Wales

Dr Emma Philpott, Wyche Innovation Centre

Acknowledgements (continued)

Dr Ian Pratt, University of Cambridge/Bromium

Russell Price, Cyber Risk Forum

Professor David Pym, University College London

Sean Ralph, Defence Science and Technology Laboratory

John Reid, RepKnight

Professor Awais Rashid, Lancaster University

Dr Simon Rice, Information Commissioner's Office

Andrew Rogoyski, CGI Group

Javier Ruiz, Open Rights Group

Professor Mark Ryan, University of Birmingham

Professor Vladimiro Sassone, University of Southampton

Jamie Saunders, National Crime Agency

Professor Sakir Sezer, Queen's University Belfast

Professor Nigel Smart, University of Bristol

Professor Peter Sommer, Digital Forensic Services

Professor Tom Sorell, University of Warwick

Professor Sarah Spiekermann, Vienna University for Management of Economics and Business

Professor Bernd Stahl, Centre for Computing and Social Responsibility, DeMontfort University

Dr Frank Stajano, University of Cambridge

Dr Gianluca Stringhini, University College London

Matt Stroud, Digital Catapult

Professor Joseph Swierzbinski, University of Aberdeen

Dr Martyn Thomas FREng, Royal Academy of Engineering

Dr Nithin Thomas, SQR Systems

Paul Thorlby, QinetiQ

Scott Tousley, Department of Homeland Security, USA

Andrew Tyrer, Innovate UK

Professor David Upton, Oxford University

Ezekial Vidra, Google Inc.

Jonny Voon, Innovate UK

Mark Waghorne, KPMG

Dr Robert Watson, University of Cambridge

Ollie Whitehouse, NCC Group

Arabella Whiting, Consultant, BAE Systems Applied Intelligence

Dr Edgar Whitley, London School of Economics and Political Sciences

Andrew Whittaker, CERT-UK

Professor Monica Whitty, University of Leicester

Professor Richard Wortley, University College London

Elisabetta Zaccaria, CyberY

The Royal Society is a self-governing Fellowship of many of the world's most distinguished scientists drawn from all areas of science, engineering, and medicine. The Society's fundamental purpose, as it has been since its foundation in 1660, is to recognise, promote, and support excellence in science and to encourage the development and use of science for the benefit of humanity.

The Society's strategic priorities emphasise its commitment to the highest quality science, to curiosity-driven research, and to the development and use of science for the benefit of society.
These priorities are:

- Promoting science and its benefits
- Recognising excellence in science
- Supporting outstanding science
- Providing scientific advice for policy
- Fostering international and global cooperation
- Education and public engagement

For further information
The Royal Society
Science Policy Centre
6 – 9 Carlton House Terrace
London SW1Y 5AG

T +44 20 7451 2500
E science.policy@royalsociety.org
W royalsociety.org

Registered Charity No 207043

ISBN: 978-1-78252-215-7
Issued: July 2016 DES3800