REFORM
RESILIENT STATE

DXC.technology

Resilient public services in an age of cyber threats

Matthew Fetzer
Eleonora Harwich

October 2020

#reformcyber

Acknowledgements

External reviewers

The authors would like to thank William Barker and Mark Brett for helpful comments on an earlier draft of this paper.

Interviewees

The authors would like to express their gratitude to the seven individuals and organisations who were interviewed as part of the research for this paper and kindly agreed to be acknowledged:

William Barker, Associate Director Society for Innovation, Technology and Modernisation (SOCITM) and former Head of National Cyber Security Programme – Local, Ministry of Housing, Communities and Local Government (2015-19)

Mark Brett, Programme Director, National Local Authority Warning Advice Report Point

Prof Madeline Carr, Professor of Global Politics and Cyber Security, University College London

Ruth Edwards MP, Member of Parliament for Rushcliffe

Saira Ghafur, Lead for Digital Health, Institute of Global Health Innovation, Imperial College London

Mark Hughes, Senior Vice President and General Manager – Security, DXC Technology

Owen Pritchard, Cyber Security Programme Manager, Local Government Association

About

Reform is established as the leading Westminster think tank for public service reform. We are dedicated to achieving better and smarter public services. Our mission is to set out ideas that will improve public services for all and deliver value for money.

We work on core sectors such as health and social care, education, home affairs and justice, and work and pensions. Our work also covers issues that cut across these sectors, including public service design and delivery and digital public services.

We are determinedly independent and strictly non-party in our approach.

About *Reform* Ideas

***Reform* Ideas** – These are short research papers which enable a high-level exploration of a key public service challenge. The papers examine the policy context, identify key opportunities for reform and set a vision for the future.

Contents

Ideas

Idea 1: The National Cyber Security Centre should conduct an audit of existing Warning Advice Reporting Points, where public sector professionals can exchange information about cyber threats, to identify the best structures and practices that could be extended nationwide. This audit should include an assessment and subsequent provision of the necessary funding to finance these local-knowledge-sharing hubs.

Idea 2: The National Cyber Security Centre should increase the capacity of and mandate attendance to their current cyber security training courses to anyone working in the public sector handling sensitive information.

Idea 3: Government departments should, in conjunction with the National Cyber Security Centre, identify jobs that require a certain level of training in cyber security and change the job specification to reflect that. They should then prioritise opportunities for candidates who have those qualifications or create career pathways for those willing to complete that training. This would help improve the skills gap.

Idea 4: The National Cyber Security Strategy should explore the possibility of having a yearly random cyber security audit of local public sector organisations. These should be carried out by Government departments and statutory bodies in charge of cyber security policy. This will reveal adherence to standards at a local level, highlight reasons for non-compliance and improve knowledge of what works.

Idea 5: The National Cyber Security Centre should work on a kitemark of cyber secure products to help with procurement of new technology.

Introduction

Over the last decade cyber-attacks have become one of the biggest security threats to governments around the world, and the UK. As the world becomes more interconnected, digitised and open, this threat is likely to only increase.[1] Threats can have various origins like state-sponsored attacks or terrorism.[2] Attacks are also wide-ranging, from sophisticated operations on critical national infrastructure, to individual-level attacks aimed at getting access to a high-volume personal data, the latter rising in prevalence in recent years.[3]

During the COVID-19 pandemic, the surge in home working – including by the public sector workforce – has increased vulnerabilities.[4] According to a recent report from INTERPOL, this shift has occurred concurrently with an uptick in cybercrime targeting governments and critical health infrastructure, as opposed to individuals and small businesses.[5]

A robust cyber security strategy for the public sector is therefore essential. As highlighted by Mark Hughes, Senior Vice President and General Manager of Security at DXC Technology, this requires being able to deter cyber-attacks, ensure secure daily usage of technology, and appropriately respond to an incident if one should occur.

The Government has aimed to reduce the threat level whilst supporting the UK in being "at the vanguard of the digital revolution".[6] Cyber resilience – defined as the "ability to continuously deliver the intended outcome despite adverse cyber events"[7] – is key to achieving this. The Government needs to find ways of effectively navigating the tension of maintaining the delivery of vital public services whilst facing increasing threats.

The UK has been at the forefront of cyber security policy with its pioneering cyber security strategies and world-leading National Cyber Security Centre (NCSC). With the next National Cyber Security Strategy due to be published in 2021, it is an opportune moment to take stock and examine the progress so far in creating cyber-resilient public services and identify key areas for development.

[1] HM Government, *National Cyber Security Strategy 2016-2021*, 2016.
[2] Ibid.
[3] Ibid.
[4] National Cyber Security Centre, 'Advisory: COVID-19 Exploited by Malicious Cyber Actors', Press Release, 8 April 2020.
[5] INTERPOL, *COVID-19: Cybercrime Analysis Report - August*, 2020.
[6] HM Government, *National Cyber Security Strategy 2016-2021*.
[7] Fredrik Björck et al., 'Cyber Resilience - Fundamentals for a Definition', in *New Contributions in Information Systems and Technologies*, ed. Alvaro Rocha, Ana Maria Correia, Sandra Constanzo, Luis Paulo Reis (Switzerland: Springer, 2015), 312.

1. Cyber security landscape

The UK is world-leading when it comes to cyber security policy. Two successive cyber security strategies and programmes are the driving force for policy development in this area. When the first strategy was published in 2011, it was seen as a big shift as it recognised the role of public sector and industry bodies in protecting the UK from cyber threats.[8] Over the years as the threats continued to rise, government strengthened its approach and cyber security policy has become more centralised.[9]

1.1 How has the landscape evolved?

The UK is particularly vulnerable to cyber threats as it has one of the most open and digitised economies in the world.[10] For this reason, cyber security policy has risen in prominence in recent years, as outlined in Figure 1. This shift was kickstarted in 2010 when it was raised to one of the top four "tier one" risks in the National Security Strategy, and the Office of Cyber Security was established inside the Cabinet Office.[11] Under the oversight of this Office, between 2011 and 2016 the Government funded a National Cyber Security Programme (NCSP1) worth £860 million to deliver the 2011 National Cyber Security Strategy (NCSS).[12]

This programme and strategy aimed to provide resilience to public services and deliver online security for the country.[13] However, a National Audit Office (NAO) report in 2014 found that while National Cyber Security Programme 1 had made good progress, understanding of threats varied signficantly across public organisations and guidance on how to maintain security online was was not communicated to the wider public effectively.[14]

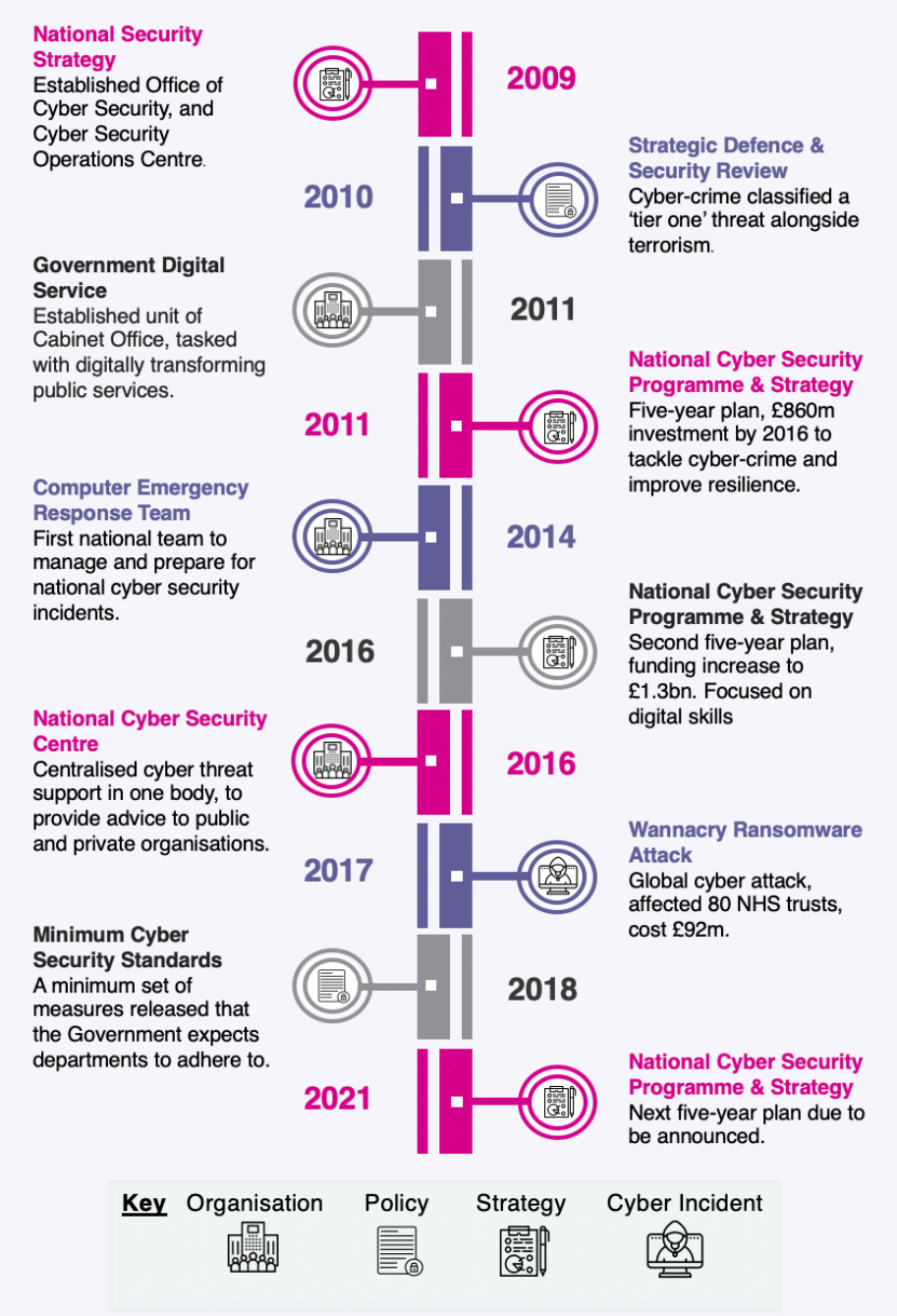
The second programme and strategy in 2016 therefore went further, consolidating cyber security policy across government. Instead of a lighter touch approach to security, the second strategy and programme aimed to expand government influence over the sector.[15] This included the establishment of the NCSC, an organisation meant to provide advice, address systemic vulnerabilities and undertake rapid response to incidents.[16]

A key reason for this was the Government's desire to improve "cyber hygiene" – defined as simple good behaviours that improve baseline security (see Glossary for further definition), across the population. While the first NCSS made Britain a pioneer in cyber security , there was a "market-based approach" to hygiene which did not produce

[8] National Audit Office, *The UK Cyber Security Strategy: Landscape Review*, 2013.
[9] HM Government, *National Cyber Security Strategy 2016-2021*.
[10] House of Commons Committee of Public Accounts, *Cyber Security in the UK, Ninety-Ninth Report of Session 2017 - 19*, HC 1745 (London: The Stationery Office, 2019).
[11] Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, 2011.
[12] Cabinet Office, *The UK Cyber Security Strategy 2011 - 2016 Annual Report*, 2016.
[13] Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*.
[14] National Audit Office, *Update on the National Cyber Security Programme*, 2014.
[15] HM Government, *National Cyber Security Strategy 2016-2021*.
[16] Ibid.

the "required pace and scale of change".[17] In practice, this meant that the focus was on more high-level protection, and assumed public and private organisations would adopt good behaviours because it was beneficial for them to do so – this was not the case.[18] As Ciaran Martin, Director of the NCSC, stated five to ten years ago everyone was told to have "level of defences equivalent to, frankly, the Government… of course, most people can not afford nor have the skills to do that."[19]

Figure 1: Cyber security policy timeline



Source: *Reform* research, August 2020. The timeline presented is intended to show key policy developments over the last decade. It not meant to be an exhaustive list.

[17] Ibid., 9.
[18] HM Government, *National Cyber Security Strategy 2016-2021*.
[19] Ciaran Martin, *Oral Evidence* (HC 1745, 2020).

1.2 Who is responsible for what?

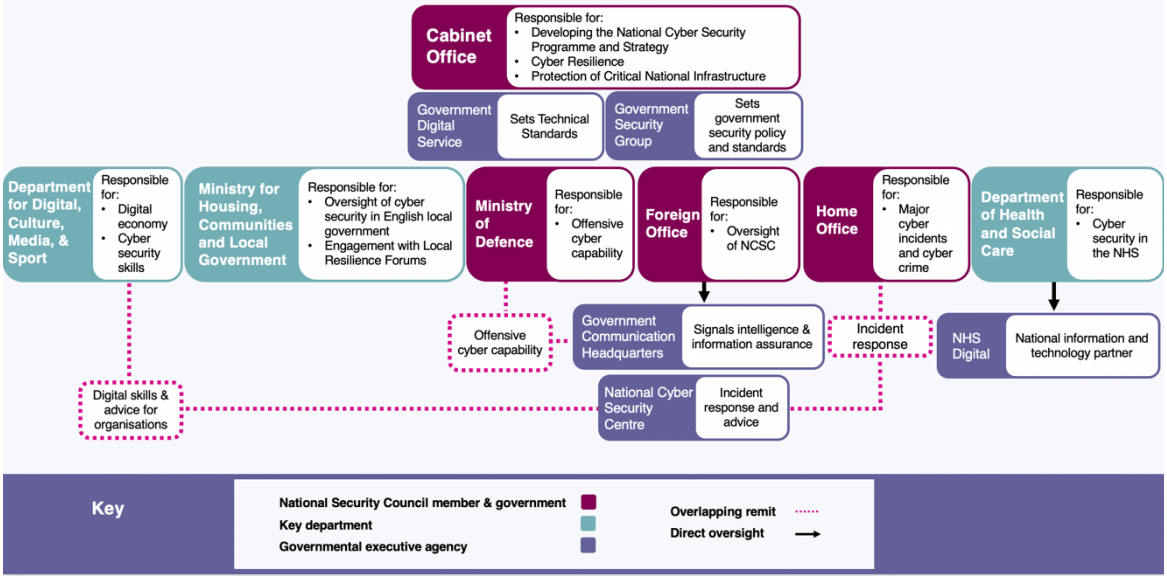
Delivering on cyber security policy in the UK is a fragmented landscape with many overlapping remits, as seen in Figure 2. Developing and publishing the NCSS and the National Cyber Security Programme is the responsibility of the Cabinet Office, and these set the overall cyber security policy across government departments.[20] Each department is responsible for making sure that they adhere to security standards.[21] In terms of cross-governmental issues, the Department for Digital, Culture Media and Sport (DCMS) leads in areas such as digital skills and sector growth.[22] The Home Office responds to major cyber incidents. At the same time, the NCSC is the body responsible for rapid incident response, and this is under the purview of the Foreign Office, as it is an arm of the Government Communication Headquarters (GCHQ). GCHQ is also partnered with the Ministry of Defence, through the National Offensive Cyber Programme.[23]

Collective oversight on cyber security matters is part of the remit of the National Security Council.[24] This is a Cabinet committee which oversees cross-government security, meeting weekly when Parliament is sitting. Further, both the Home Secretary and the Chancellor to the Duchy of Lancaster receive fortnightly briefings from the NCSC.[25] All departments above sit on the National Security Council, apart from the DCMS. This is paradoxical as this is the department in charge of digital skills, a key pillar of the NCSS. There was a Cabinet sub-committee for cyber security, but this only sat for a year and was disbanded in 2017.[26]

While fragmented, the Government believes that the current organisational structure is effective. The Chief Digital Officer for HM Revenue and Customs, Jacky Wright stated that the division and overlapping of responsibilities was a positive in developing cyber security policy because "it had built in checks and balances."[27] Whilst some remits may overlap, the current structure allows Departments to oversee how they implement these security policies themselves – meaning that these are more context-specific and directly applicable. For example, in areas like Critical National Infrastructure, allowing for departmental expertise to oversee their own security policy can, in theory, be advantageous according to the Joint Committee on the National Security Strategy.[28]

[20] Margot James and Oliver Dowden, *Digital Government: Written Evidence*, HC1455, 2019.
[21] Ibid.
[22] Ibid.
[23] Intelligence and Security Committee of Parliament, *Russia*, HC 632 (London: The Stationery Office, 2020).
[24] Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure, Third Report of Session 2017 - 19*, HL 222 HC 1708 (London: The Stationery Office, 2018).
[25] Ibid.
[26] Ibid.
[27] House of Commons Science and Technology Committee, *Digital Government, Eighteenth Report of Session 2017-19*, HC 1455 (London: The Stationery Office, 2019).
[28] Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure, Third Report of Session 2017 - 19*.

Figure 2: Cyber governance in the UK



Source: Margot James and Oliver Dowden 'Digital Government Written Evidence', April 2019; Intelligence and Security Committee of Parliament, 'Russia', July 2020; Joint Committee on the National Security Strategy, 'Cyber Security of the UK's Critical National Infrastructure' November 2018.

However, when it comes to dealing with incidents there is a concern that the current arrangement is "wholly inadequate to the scale of the task facing the government".[29] For example, the Wannacry ransomware attack of 2017 (see Figure 4) revealed that as a result of unclear guidelines to dealing with a cyber-attack "local organisations reported the attack to different organisations within and outside the health sector, including local police".[30]

New, more robust, plans were put in place for the NHS after this, but as highlighted in the 2019 St George's House Report on the cyber-related lessons from the Salisbury Novichok and Copeland "Zero-day" incidents, this issue is still prevalent within local authorities and many of their multi-agency resilience partners.[31] Subsequently this has been confirmed by the Ministry for Housing, Communities and Local Government pre-discovery report which found that "the process of how to recover, and who (and why) to communicate with, is unclear."[32]

Overall, multiple select committees and The Labour Party's former lead on cyber security believe that leaving cyber security to departments has meant a variation in standards.[33] A simplified governance structure, such as a cyber minister they believe,

[29] Ibid., 39.
[30] National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS*, HC 414 (London: The Stationery Office, 2018), 9.
[31] St George's House Consultation, *Local Leadership in a Cyber Society 3: Building Resilience Together - Lessons for the Future*, 2019.
[32] Ministry of Housing, Communities & Local Government, *Cyber Security in Local Government: Pre-Discovery*, 2020.
[33] Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure, Third Report of Session 2017 - 19*; Jo Platt, 'For Better Cyber Security, Change Starts at the Very Top', *New Statesman*, 3 May 2019; House of Commons Science and Technology Committee, *Digital Government, Eighteenth Report of Session 2017-19*.

would make standards more universal as it would increase direction and focus at the ministerial level.[34] Jo Platt MP argued that having a single cyber minister working with the NCSC would "provide the authority and weight of government behind their recommendations" to ensure resilience.[35] However, the Government disagrees stating that the Minister for the Cabinet Office is the one accountable to parliament for cyber security, and therefore the creation of a separate post is not required.[36]

Still, the Government has recognised the issues in standards, and implemented a more robust framework to measure them. In the National Security Capability Review of 2018 the Government recognised the need to do more to ensure performance is measured at the programme level,[37] hiring an official to oversee this in February 2018.[38] However, the NAO has low confidence in the success of this framework to help inform the next strategy. This is because it was introduced two years into the existing programme and is currently only measuring one-third of the 326 metrics it set out either due to low confidence in the metric, or that they will be used in the future.[39]

[34] Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure, Third Report of Session 2017 - 19*; Jo Platt, 'For Better Cyber Security, Change Starts at the Very Top', *New Statesman*, 3 May 2019; House of Commons Science and Technology Committee, *Digital Government, Eighteenth Report of Session 2017-19*.
[35] Platt, 'For Better Cyber Security, Change Starts at the Very Top'.
[36] HM Government, 'Digital Government: Government Response to the Committee's Eighteenth Report' (HC2673, 8 October 2019).
[37] HM Government, *National Security Capability Review*, 2018.
[38] National Audit Office, *Progress of the 2016-2021 National Cyber Security Programme*, 2019.
[39] Ibid.

2. Public-sector challenges with cyber security

The public sector has faced some challenges in developing greater cyber resilience. Legacy infrastructure is problematic because it can contain vulnerabilities if not maintained properly. A lack of cyber skills both at the "high-end", such as security architecture, and the "low-end", enforcing "cyber-hygiene" principles, inhibits progress on cyber resilience.[40] These concerns have been compounded by what some view as a lack of clear leadership in this space, seeing cyber security as an additional expenditure and not fundamental to the delivery of services. Finally, there is at times a gap between the national and local standards, with unclear procurement frameworks being a central issue.

2.1 Infrastructure

To maintain the security of public services there needs to be a robust IT infrastructure - defined as the hardware, software, network, operating system and data storage, required for an IT environment to function within an organisation.[41] As highlighted in Figure 3, several elements need to be considered to protect against cyberthreats. From the minimum requirement of implementing the latest software updates to investing in firewalls and gateways, which provide a basic level of protection online.

A key issue for secure infrastructure is the existence of legacy systems – defined as an old or outdated IT infrastructure.[42] The NCSS states these are vulnerable as they "often rely on older, unpatched versions" of software.[43] The strategy recognises that there are some instances in which the software being used is no longer supported by the vendor and states that central government make sure there are no "unmanaged risks from legacy systems and unsupported software".[44] Usually, when hardware is built there are certain vulnerabilities in the software, called "Zero-day" as they are present from when the item is manufactured, which will be regularly "patched" with software updates from the vendor.[45] The key issue with legacy then becomes one of maintenance.

Insufficient maintenance of existing infrastructure has proved a barrier to resilience. An NAO report from 2013 stated clearly that "well managed legacy ICT systems deliver continuity of service and suggest the lives of such systems can be safely extended".[46] Indeed, as Mark Hughes of DXC put it, technology can become legacy very quickly, the

[40] House of Commons House of Lords Joint Committee on the National Security Strategy, *Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017 - 19* (London: The Stationery Office, 2018).
[41] 'What Is IT Infrastructure', Web Page, Red Hat, n.d., accessed 7 August 2020.
[42] Sarah Timmis, Luke Heselwood, and Eleonora Harwich, *Sharing the Benefits: How to Use Data Effectively in the Public Sector* (Reform, 2018), 20.
[43] HM Government, *National Cyber Security Strategy 2016-2021*, 23.
[44] Ibid., 37.
[45] Norton, 'Zero-Day Vulnerability: What It Is, and How It Works', Web Page, Norton, n.d., accessed 27 March 2020.
[46] National Audit Office, *Managing the Risks of Legacy ICT to Public Service Delivery*, HC 539, 2013, 8.

question then becomes “how do you deal with the risks that legacy IT exposes you to?”.

Figure 3: Common threats and how to defend against them

Source: National Cyber Security Centre, ‘Common cyber-attacks: reducing the impact’, February 2016

Ruth Edwards MP echoed this, arguing that there is no need to “replace all legacy infrastructure as it would not deliver value for money”. Instead, councils and other bodies need to invest in upkeep. However, there needs to be a sound cost-benefit approach to decision-making as dependencies between legacy IT systems can create fragilities and risks. The complexities between these dependencies can also be used as ‘excuses’ for not moving away from legacy, as highlighted by a couple of interviews carried out for this paper. To ensure appropriate maintenance of legacy IT, the Cabinet

Office has set out clear guidelines around updating software, authentication, and encryption as part of the Minimum Cyber Security Standards in 2018.[47]

While various central government departments have been successful at this, NHS trusts and local government services have been reported as particularly vulnerable.[48] For instance the WannaCry attack (see Figure 4) was so effective because of a failure to update Windows XP, an operating system released in 2001.[49] Improvements have been made in the NHS after this attack.[50] However, in answers to written questions in July 2019 Jackie Doyle-Price MP, then a health minister, admitted that 2,300 NHS computers were still using Windows XP, and 1.05 million still using Windows 7 (initially released in 2009), out of a total of around 1.37 million.[51] Further, she wrote that all NHS organisations, apart from one which had already upgraded, have signed up to receive free centrally-funded Windows 10 licenses when Microsoft security support ran out for Windows 7 in January 2020.[52] As of July 2020, Windows 10 had only been installed on 846,000 devices across the NHS, despite NHS Digital clearly setting out the dangers of unsupported licenses, and that they required Extended Security Updates to be specifically purchased to combat them.[53]

Figure 4: The WannaCry Ransomware Attack 2017

On the 12 May 2017 a global ransomware attack occurred, locking users out of their computers unless they agreed to pay a fee in bitcoin.[54] It severely affected the NHS with around 80 of 236 NHS trusts being impacted, and almost 20,000 hospital appointments and operations cancelled.[55] Before the attack, the Department for Health and Social Care, and the Cabinet Office, had written to trusts calling for "robust plans" to migrate away from old software, as 18 per cent of NHS trusts were still using this.[56] NHS Digital, as part of its remit, broadcasted alerts and provided advice, including that trusts needed to patch their systems, just months prior to the attack.[57] However, there was no mechanism for checking this was done, and the response to this was mixed. "5 per cent of the NHS IT estate" was still using Windows XP at the time of WannaCry, making the organisation particularly vulnerable to an attack.[58]

[47] Cabinet Office, 'Minimum Cyber Security Standard', June 2018.
[48] UK Computing Research Committee, *Digital Government: Written Evidence*, DIG0002, 2018.
[49] National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS*.
[50] NHS Digital, *2019 - 20 Annual Report and Accounts*, HC 537 (London: The Stationery Office, 2020).
[51] Jackie Doyle-Price MP, 'NHS Computer Software: Question for Department of Health and Social Care' (UIN 275828, 22 July 2019); Jackie Doyle-Price MP, 'NHS Computer Software: Question for Department of Health and Social Care' (UIN 278598, 22 July 2019).
[52] Doyle-Price MP, 'NHS Computer Software: Question for Department of Health and Social Care', 22 July 2019.
[53] NHS Digital, 'Advanced Threat Protection from Microsoft', Web Page, NHS Digital, 7 July 2020; NHS Digital, *2019 - 20 Annual Report and Accounts*.
[54] National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS*.
[55] House of Commons Committee of Public Accounts, *Cyber-Atttack on the NHS, Thirty-Second Report of Session 2017 - 2019*, HC 787 (London: The Stationery Office, 2018).
[56] National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS*.
[57] Ibid.
[58] House of Commons Committee of Public Accounts, *Cyber-Atttack on the NHS, Thirty-Second Report of Session 2017 - 2019*.

2.2 Leadership and skills

To maintain cyber security principles, leaders in public sector organisations need to see cyber security as fundamental to delivery, and not just an additional operational expenditure. The National Cyber Security Strategy recognises that the UK cannot afford for security deficiencies to undermine the aims of digital transformation.[59] William Barker, former Head of National Cyber Security Programme at MHCLG, commented that the "education of senior leaders on cyber has been increasingly appreciated as an important function" of the strategy. MHCLG has attempted to address this through the Cyber Pathfinders scheme, bringing together senior leaders, policy makers and practitioners from local authorities.[60] This was a series of free regional seminars with over 3,000 places to provide cyber resilience training.[61]

However, at the organisational level, due to budget constraints, it can often be overlooked by leaders. Owen Pritchard, Cyber Security Programme Manager at the Local Government Association, stated that as a result of limited funds councils may decide to delay rollout of essential cyber security services. Cyber security suffers from being seen as an operational cost rather than a fundamental element of service delivery.

Public sector leaders need to realise the importance of training their staff in basic cyber hygiene procedures, in addition to rolling out vital security procedures. Cyber skills range from highly specialised top-tier skills to more basic technical skills aimed at maintaining cyber hygiene principles within an organisation.[62] Basic technical cyber skills are defined as "the ones that are needed to implement the five basic technical controls covered in the government-endorsed Cyber Essentials scheme" such as antivirus protection and keeping software up to date.[63] According to a cyber security skills survey by commissioned by DCMS, 27 per cent of public sector organisations outside of central government departments, have a basic technical cyber security skills gap.[64]

The high-level technical skills gap is also 27 per cent, however the issue here lies more in recruitment and retention of highly skilled individuals.[65] Recruitment of highly skilled cyber professionals into the public sector has been described as "challenging" both by Ciaran Martin, Director of the NCSC, and Rt Hon David Lidington MP, then Chancellor of the Duchy of Lancaster.[66] There have been positive steps taken to address this, such as the NCSC accrediting masters courses focusing on cyber security.[67] Further,

[59] National Audit Office, *Progress of the 2016-2021 National Cyber Security Programme*.
[60] Local Government Association, 'Cyber Pathfinder Training Scheme', Web Page, Local Government Association, n.d., accessed 7 February 2020.
[61] HM Government, *Initial National Cyber Security Skills Strategy*, 2018.
[62] House of Commons House of Lords Joint Committee on the National Security Strategy, *Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017 - 19*.
[63] Daniel Pedley et al., *Cyber Security Skills in the UK Labour Market 2020* (Department for Digital, Culture, Media & Sport, 2020).
[64] Ibid.
[65] Ibid.
[66] Ciaran Martin and Rt Hn David Lidington, *Cyber Security Skills and the UK's Critical National Infrastructure: Oral Evidence*, 2018.
[67] Tom Crick et al., 'A UK Case Study on Cyber security Education and Accreditation', *IEEE Frontiers in Education Conference*, 17 July 2019.

the recent move to establish a Government Wide Security Profession to upskill existing staff and recruit and train young people is to be welcomed.[68]

Despite this, external market conditions are a barrier when trying to recruit high-level professionals to the public sector.[69] There is widespread acknowledgment that there is a global shortage of these professionals across public and private sectors.[70] The public sector, especially at the local level with lower pay scales and lengthy recruitment processes, can be at a disadvantage from the outset when attempting to recruit in a competitive market.[71]

2.3 The local-national divide

There is a local-national divide in cyber resilience, particularly around knowledge sharing and communication. The effects of a cyber-attack can be devastating in local government. For instance, a high-profile ransomware attack in Copeland in 2017 caused some parts of the Council to go 10 weeks without IT functionality, the Council had no access to financial systems, and house sales had to be halted, putting some at risk of moving into temporary accommodation.[72]

As part of the DEFEND section of the 2016 National Cyber Security Strategy, a key objective was that all branches of government "will set and adhere to the most appropriate cyber security standards".[73] This led to the publication of the Minimum Cyber Security Standard in 2018, and various guidance, such as the "10 steps to Cyber Security".

Local authorities are entirely responsible for their own technology, with the NCSC supporting through Active Cyber Defence, and the guidance that is posted online.[74] Take-up of this mix of guidance and standards, however, has been varied at the local level. This potentially impacts not just on the operational capability of individual Local Authorities but also on their ability to work effectively with their partners such as the NHS, police and emergency services.

The National Cyber Security Programme funded a local leadership roundtable in 2019 which convened senior cyber security figures from central and local government. It identified a threefold challenge: define and implement a clearer policy for local IT security, determine the current situation, and champion high-quality standards.[75] The follow-up pre-discovery 2020 report from MHCLG utilised an additional survey of 173 English Councils. It confirmed these findings noting that "a potentially overwhelming amount of guidance paradoxically often leads to a lack of clarity and confusion".[76] In

[68] HM Government, *Initial National Cyber Security Skills Strategy*.
[69] National Audit Office, 'The Digital Skills Gap in Government', 2015.
[70] HM Government, *Initial National Cyber Security Skills Strategy*.
[71] Nick Walrond, 'Rethinking the Tech Skills Gap in Local Government', LocalGov, 13 January 2020.
[72] Local Government Association, 'Copeland Borough Council: Managing a Cyber Attack', Press Release, 9 October 2018.
[73] HM Government, *National Cyber Security Strategy 2016-2021*.
[74] James and Dowden, *Digital Government: Written Evidence*.
[75] St George's House Consultation, *Local Leadership in a Cyber Society 3: Building Resilience Together - Lessons for the Future*.
[76] Ministry of Housing, Communities & Local Government, *Cyber Security in Local Government: Pre-Discovery*.

practice, they found councils were unsure what was guidance and what was a standard they had to meet.

Likewise, multiple interviewees commented on the challenges in local and national government coordination. Mark Brett, the Programme Director at the National Local Authority Warning Advice Reporting Point, stated that the biggest problem is "there isn't a coordinating government body for local government cyber security". Owen Pritchard highlighted the tensions and difficulties that central government needs to navigate when advising local areas: it is hard to advise on "the digital and security needs of a community in Northumbria when no one in that department has been to Northumbria."

2.3 Procurement

Even though legacy infrastructure can be more effectively maintained, there is still a need to upgrade technology to maintain security. Public sector organisations find it difficult to assess the cost effectiveness of replacing legacy infrastructure; even when the business case is clear it can be difficult to secure funds to do so.

Since 2016 there has been a move to implement more robust standards across departments in procurement. All regulations in the Minimum Cyber Security Standard are required to be met by suppliers of third party services.[77] This could be done through holding a valid Cyber Essentials certificate, or assuring against the HMG Cyber Security Standard, as a minimum.[78] A Cyber Essentials certificate is a Government accreditation that an organisation will be protected against common cyber-attacks, and in this case it would "allow a supplier to demonstrate appropriate diligence" when it comes to the safety of their technology.[79] The enforcement of this is the responsibility of the department that is procuring the technology, with the Minimum Cyber Security Standard stating they "should" conduct their own assurance, meaning there is an expectation it will be done, but there can be rare exceptions.[80]

At the individual level, not all public organisations have the workforce capability to be able to do this. A survey commissioned by DCMS, excluding central government departments and instances where cyber security was outsourced, found that 18 per cent of cyber security professionals in the public sector were not confident in penetration testing, and 15 per cent in forensic analysis.[81] Penetration tests are a way of simulating a cyber-attack against your system (see Glossary for full definition).[82] According to the NCSC Cyber Assessment Framework for organisations in charge of important services, they are a key part of vulnerability management.[83]

Further, a lack of funding can prevent departments from moving away from legacy systems if they wanted to. Margot James MP, then a Minister at DCMS, speaking after Wannacry, stated that "substantial financial pressures" in the NHS, unfortunately

[77] Cabinet Office, 'Minimum Cyber Security Standard'.
[78] Ibid.
[79] Ibid.
[80] Ibid.
[81] Pedley et al., *Cyber Security Skills in the UK Labour Market 2020*.
[82] National Cyber Security Centre, 'Penetration Testing', Web Page, 8 August 2017.
[83] Ibid.

sometimes “militates against investments required to upgrade its security systems”.[84] Authors from the Imperial College London echoed this, writing in 2019 that limited budgets “mean health systems are faced with difficult choices in allocating resources and cyber security investment is often not a priority”.[85]

[84] James and Dowden, *Digital Government: Written Evidence*.
[85] Saira Ghafur et al., ‘The Challenges of Cyber security in Health Care: The UK National Health Service as a Case Study’, *The Lancet* 1, no. 1 (May 2019): 11.

3. Elements for the next strategy

The UK's first two cyber security strategies have been world leading. While departments and public bodies are responsible for their safeguards, the first publication recognised there needed to be a centrally driven strategy to manage exposure to risks.[86] The second advocated a "more interventionist" approach, according to Madeline Alessandri, former deputy National Security Advisor.[87] This included setting up bodies such as the NCSC to centralise policy, provide expert advice and respond to incidents.

The next strategy, due to be published in 2020, will be an opportunity for greater ambition and to build the public sector's cyber capabilities. It should reflect on the big changes which came about during the COVID-19 pandemic with an increased reliance on remote working, digital technologies, and multi-agency collaboration. A robust cyber security strategy will be essential for cyber resilience in the economy and public services over the next five years. The strategy should set out a more ambitious programme for skills and recruitment, advocate greater information sharing across organisations, implement robust performance frameworks, and close the local-national divide.

3.1 Building capability

In order to increase cyber resilience, there needs to be greater focus on the capability of the public sector workforce. There should be greater knowledge sharing to allow best practice to be replicated, and a renewed commitment to improve skills. Interviews carried out for this paper highlighted that an increase in knowledge sharing would be particularly beneficial at the local government level.

3.1.1 Knowledge sharing

Knowledge sharing is vital when it comes to cyber security, and can help both in preventing and responding to cyber incidents.[88] This includes both sharing real-time threat data but also increasing awareness of potential and unfolding threats within organisations, and across the public-private divide.[89] Cyber incidents develop so rapidly that there is a "greater need [than most] to support timely decision-making and automate responses to the greatest extent possible".[90]

The NCSC has been successful at increasing threat information sharing across sectors, with the use of the Cyber Information Sharing Partnership increasing 169 per

[86] National Audit Office, *Progress of the 2016-2021 National Cyber Security Programme*.
[87] Madeleine Alessandri, *Cyber Security in the UK Oral Evidence*, HC 1745, 2019.
[88] Adam Ziback and Andrew Simpson, 'Towards Better Understanding of Cyber Security Information Sharing', *IEEE*, June 2019.
[89] Ibid.
[90] Luc Dandurand and Oscar Serrano Serrano, 'Towards Improved Cyber Security Information Sharing', *5th International Conference on Cyber Conflict*, 2013.

cent between 2016 and 2018, but there is still work to be done.[91] This is a joint industry and government initiative which allows for real time exchange of threat information. Even so, according to Madeline Carr, the cyber security community in the UK still works in academic, public and private sector siloes. There needs to be a "greater revolving door between public and private" sectors, enabling cross-sector learning, which would help build resilience into the system as a whole.

Within the public sector itself, despites pockets of best practice for cross-organisational knowledge sharing, there is still a need for a more standardised approach. For Health and Social Care, the Cyber Associates Network is a free membership organisation where professionals can meet and discuss the cyber security landscape, share best practice, and give advice.[92] Warning, Advice, Reporting Points or (WARPs) are similar networks, where public sector professionals in a local area can exchange threat information and best practice.[93] These however are not standardised, meaning the quality differs and there is space for more knowledge sharing across different WARPs.[94] The Cyber Technical Advisory Group funded by the National Cyber Security Programme, which brings together WARPS and government agencies such as the Government Digital Service and NHSX, is a welcome addition in this space. [95]

> **Idea 1:** The National Cyber Security Centre should conduct an audit of existing Warning Advice Reporting Points, where public sector professionals can exchange information about cyber threats, to identify the best structures and practices that could be extended nationwide. This audit should include an assessment and subsequent provision of the necessary funding to finance these local-knowledge-sharing hubs.

3.1.2 Skills

As highlighted in the previous chapter, there are two key barriers to a cyber-skilled workforce in the public sector. First, there is a basic technical skills gap that leaves organisations, especially outside of central government, open to threats. Second, there is a challenge in overcoming the lack of supply of high-skilled cyber security professionals.

Basic technical skills need to be improved across the public sector to maintain resilience to threats. In a survey conducted by the NCSC, only 35 per cent of non-IT staff in schools had received cyber security training.[96] Encouragingly there is appetite for upskilling, with the same survey showing 92 per cent would welcome more cyber security awareness training for staff.[97] A key reason for the unavailability could be that

[91] National Audit Office, *Progress of the 2016-2021 National Cyber Security Programme*.
[92] NHS Digital, 'Cyber Associates Network', Web Page, n.d., accessed 19 August 2020.
[93] National Cyber Security Centre, 'What Is a WARP', Web Page, Information, 15 November 2018.
[94] Ministry of Housing, Communities & Local Government, *Cyber Security in Local Government: Pre-Discovery*.
[95] Local Government Association, 'Cyber Security - Resources', Web Page, n.d., accessed 7 October 2020.
[96] National Cyber Security Centre, *Cyber Security Schools Audit Report*, 2019.
[97] Ibid.

one quarter of cyber professionals in the public sector outside of central government do not feel comfortable providing training materials or sessions.[98]

One way this could be addressed is through educating leaders and empowering professionals to conduct training exercises. Centrally funded, multi-agency training models for senior leaders in the public sector, practitioners and policy makers, should be extended and mandated across the public sector. Courses such as Cyber Pathfinder would provide a framework for delivering this and should include a focus on hygiene training. Currently however, there is no mechanism in place to measure the success of this course on the cyber health of the organisation.[99]

> **Idea 2:** The National Cyber Security Centre should increase the capacity of and mandate attendance to their current cyber security training courses to anyone working in the public sector handling sensitive information.

In addition, there is a big challenge in recruiting highly skilled individuals to the public sector. Due to the current shortage of skills, cyber security professionals in the public sector can often enter the role without a technical background, as highlighted by several interviewees. One explanation could be the lack of a standardised qualification necessary to work in cyber security. Whilst the Certified Information Systems Security Professional (CISSP) is perhaps the most recognised accreditation, it requires 5 years minimum of work experience, and those obtaining the qualification generally have significantly higher salary expectations than those in the public sector.[100]

Steps have been taken to narrow this skills gap in the long term, such as with the CyberFirst and Cyber Discovery programmes, which are specifically designed to help inspire the next generation of cyber security professionals.[101] Additionally, the launch of the Government Security Profession (GSP) also aims to build the capabilities of security professionals and help those chart a career path forward.[102]

It is crucial to ensure a minimum level of technical knowledge for cyber security jobs in the public sector. However, it is also important, especially given the global skills shortage, to recognise that candidates can be trained to acquire them. Training in cyber security should not be viewed as static process, but rather a continuous one,

[98] Pedley et al., *Cyber Security Skills in the UK Labour Market 2020*.
[99] Ministry of Housing, Communities & Local Government, *Cyber Security in Local Government: Pre-Discovery*.
[100] Pedley et al., *Cyber Security Skills in the UK Labour Market 2020*.
[101] HM Government, 'Cyber Security of the UK's Critical National Infrastructure: Government Response' (HC 1658, 13 November 2018).
[102] Government Security Profession, 'About Us', Web Page, n.d., accessed 19 August 2020.

where cyber security professionals in the public sector update their knowledge on a regular basis.

Idea 3: Government departments should, in conjunction with the National Cyber Security Centre, identify jobs that require a certain level of training in cyber security and change the job specification to reflect that. They should then prioritise opportunities for candidates who have those qualifications or create career pathways for those willing to complete that training. This would help improve the skills gap.

3.2 Improving the local-national balance

The current strategy has aimed to be more interventionist than the previous one, and place bodies such as the NCSC at the centre of mandating cyber security protocols across the public sector.[103] However, as outlined the previous chapter, there are communication and organisational barriers that make public sector organisations at a local level less resilient to cyber threats

Multiple interviewees commented on the need for the next strategy to be centrally driven, but locally focused. William Barker stated that central bodies such as NCSC need to ramp up their support, and "local government needs to be encouraged to step up" and engender "new behaviours". The next NCSS is an opportunity for a long-term solution and can set robust performance frameworks to make sure the public sector is complying. As Mark Hughes of DXC put it, there needs to be a move from encouragement to a "thou shalt" approach.

Through more consistent communication on standards, procurement practices can be streamlined. Currently, procurement is delayed due to complicated cyber security standards that take a long time to decipher.[104] There have been recent moves to support this, including the Cyber Resilience programme from the LGA. This is a strategy where councils can apply for funding to strengthen resilience.[105] However, Mark Brett has warned that it needs to go beyond the LGA as it is not a long-term solution.

Part 1 of the Civil Contingencies Act (2004) sets out the roles and responsibilities for those tasked with dealing with an emergency response at the local level.[106] A key part of this act is "horizon-scanning" where responders should be aware of new threats and update plans accordingly.[107] As cyber threats are constantly evolving, a yearly random audit of all public sector organisations will help facilitate constant updates to resilience plans. Practice exercises, as mandated by this regulation,[108]

[103] HM Government, *National Cyber Security Strategy 2016-2021*.
[104] Ministry of Housing, Communities & Local Government, *Cyber Security in Local Government: Pre-Discovery*.
[105] Local Government Association, 'LGA - Cyber Resilience Funded Programme 2019/20', Web Page, n.d., accessed 19 August 2020.
[106] HM Government, 'Civil Contingencies Act 2004', Chapter 1.
[107] Cabinet Office, 'Introduction', in *Guidance: Emergency Preparedness*, 2012.
[108] Cabinet Office, 'Emergency Planning', in *Guidance: Emergency Preparedness*, 2011.

will therefore be more effective as they would be more likely to address new and emerging threats.

Idea 4: The National Cyber Security Strategy should explore the possibility of having an annual, random cyber security audit of local public sector organisations. These should be carried out by government departments and statutory bodies in charge of cyber security policy. This will reveal adherence to standards at a local level, highlight reasons for non-compliance, and improve knowledge of what works.

3.3 Spreading good tech

Spreading good technology throughout the public sector would be an effective way of achieving resilience in the system. Mandating stringent secure-by-design principles coupled with a commitment to usability and underpinned by an easy to understand marking system for cyber secure products would enable this to happen.

Technology employed by the public sector needs to be secure-by-design. This means building security into the technology so that it takes as much responsibility away from the end-user as possible.[109] As Madeline Carr stated in an interview for this paper "you can't ask everyone in the workplace to focus on cyber security".

However, secure-by-design cannot come at the cost of usability. Ruth Edwards MP stated that a key barrier is the appearance of "a trade-off between security and convenience" in public sector bodies. In reality, "usability doesn't depend on security" but "security often does depend on usability".[110] This is nothing new, in fact a paper from UCL in 1999 explored how a more user-centred design is integral to security.[111] It argued that many security measures are so complex that "it is…hardly surprising to find that many users try to circumvent such mechanisms".[112]

There are simple features to marry these two similar goals. According to a code of practice published by DCMS for manufacturers, implementing features such as no-default passwords could make a big practical difference in security. However, the NAO has stated that "the Department can only encourage manufacturers and retailers to comply as it has not yet supported this with regulation".[113]

A clearer kitemarking system would enable manufacturers to prove their products are secure-by-design and help public sector organisations to procure technology. Currently, there is no kitemark or system in place akin to that used for food safety, to show a consumer how cyber secure products are.[114] Although there are standards and frameworks through which to procure technology, the guidance has been shown to

[109] Department for Digital, Culture, Media & Sport, 'Secure by Design', Policy Paper, 7 March 2018.
[110] Emma W, 'Security and Usability: You CAN Have It All!', *NCSC Blog*, 24 August 2018.
[111] Anne Adams and Martina Angela Sasse, 'USERS ARE NOT THE ENEMY', *Communications of the ACM* 42, no. 12 (December 1999).
[112] Ibid., 4.
[113] National Audit Office, *Progress of the 2016-2021 National Cyber Security Programme*, 20.
[114] House of Commons Committee of Public Accounts, *Cyber Security in the UK, Ninety-Ninth Report of Session 2017 - 19*.

have mixed effects, and not all areas of the public sector know exactly where their vulnerabilities lie.

> **Idea 5:** The National Cyber Security Centre should work on a kitemark of cyber secure products to help with the procurement of new technology.

Conclusion

COVID-19 has accelerated the digitisation of public services in the UK, which while positive, poses an increased cyber risk. It has also accelerated the use of remote working tools and multi-agency working, which potentially exposes the public sector to more vulnerabilities. Without sound infrastructure, investment in maintaining or updating that infrastructure, and a cyber-aware workforce, there is a threat of large-scale damage both to the UK public sector and wider society.

The UK has been a leading nation in this policy area. The National Cyber Security Strategies, and in particular the creation of the NCSC, have represented best practice for countries around the world. Yet more needs to be done to mitigate the increasing threat.

The Government needs to take greater action to address the digital skills gap in the public sector workforce. Basic IT processing and understanding of vulnerabilities across the workforce is paramount to security. This can be achieved through more rigorous training schemes.

More effective maintenance of infrastructure across the sector is also needed. Legacy systems make organisations vulnerable if not maintained properly, and stricter enforcement methods, such as a yearly audit, would aid this.

Finally, spreading good technology would help to solve the local-national divide. Central government can facilitate this with clear manufacturing protocols and kite-marking cyber-secure products, which can increase security across the board'

The UK has set the 'gold standard' in terms of cyber security policy, the next iteration of the NCSS should address these issues to maintain the UK's position as a world leader.

Glossary

Authentication: a process of validating the identity of a register user before allowing access to the protected resource.

Cyber hygiene: practices and steps users of computers and other devices can take to improve security.

Cyber resilience: maintaining service delivery under cyber threats and attacks.

Cyber security: how individuals and organisations reduce the risk of cyber-attack.

Encryption: a process of scrambling readable text so that it becomes unreadable. When the text reaches the intended recipient, it is translated back into its original form.

Malware: a program or file that is harmful to a computer, there are a variety of types of malware such as viruses, worms, and Trojan horses.

Penetration tests: "[a] method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might."[115]

Phishing: a technique used by hackers to steal information. One common example is a fake email.

Ransomware: a type of malicious software which is designed to block access to a computer system before a certain amount of money is paid.

Software: a set of programs which tells a computer to undertake a task.

Virus: a type of malware that aims to corrupt, modify or erase information on a computer.

Zero-day Vulnerability: an unintended flaw in the security of the software which makes it vulnerable to an attack. It will be known to the vendor, but they will not have a patch in place to fix it, so they therefore have "zero days" to fix it.

[115] National Cyber Security Centre, 'Penetration Testing'.

Bibliography

Adams, Anne, and Martina Angela Sasse. 'USERS ARE NOT THE ENEMY'. *Communications of the ACM* 42, no. 12 (December 1999).

Alessandri, Madeleine. *Cyber Security in the UK Oral Evidence*. HC 1745, 2019.

Björck, Fredrik, Martin Henkel, Janis Stirna, and Jelena Zdravkovic. 'Cyber Resilience - Fundamentals for a Definition'. In *New Contributions in Information Systems and Technologies*, Ed. Alvaro Rocha, Ana Maria Correia, Sandra Constanzo, Luis Paulo Reis. Switzerland: Springer, 2015.

Cabinet Office. 'Emergency Planning'. In *Guidance: Emergency Preparedness*, 2011.

———. 'Introduction'. In *Guidance: Emergency Preparedness*, 2012.

———. 'Minimum Cyber Security Standard', June 2018.

———. *The UK Cyber Security Strategy 2011 - 2016 Annual Report*, 2016.

———. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, 2011.

Crick, Tom, James H. Davenport, Alastair Irons, and Tom Prickett. 'A UK Case Study on Cybersecurity Education and Accreditation'. *IEEE Frontiers in Education Conference*, 17 July 2019.

Dandurand, Luc, and Oscar Serrano Serrano. 'Towards Improved Cyber Security Information Sharing'. *5th International Conference on Cyber Conflict*, 2013.

Department for Digital, Culture, Media & Sport. 'Secure by Design'. Policy Paper, 7 March 2018.

Doyle-Price MP, Jackie. 'NHS Computer Software: Question for Department of Health and Social Care'. UIN 275828, 22 July 2019.

———. 'NHS Computer Software: Question for Department of Health and Social Care'. UIN 278598, 22 July 2019.

Ghafur, Saira, Emilia Grass, Nick R Jennings, and Ara Darzi. 'The Challenges of Cybersecurity in Health Care: The UK National Health Service as a Case Study'. *The Lancet* 1, no. 1 (May 2019).

Government Security Profession. 'About Us'. Web Page, n.d. Accessed 19 August 2020.

HM Government. Civil Contigencies Act 2004 (n.d.).

———. 'Cyber Security of the UK's Critical National Infrastructure: Government Response'. HC 1658, 13 November 2018.

———. 'Digital Government: Government Response to the Committee's Eighteenth Report'. HC2673, 8 October 2019.

———. *Initial National Cyber Security Skills Strategy*, 2018.

———. *National Cyber Security Strategy 2016-2021*, 2016.

———. *National Security Capability Review*, 2018.

House of Commons Committee of Public Accounts. *Cyber Security in the UK, Ninety-Ninth Report of Session 2017 - 19*. HC 1745. London: The Stationery Office, 2019.

———. *Cyber-Atttack on the NHS, Thirty-Second Report of Session 2017 - 2019*. HC 787. London: The Stationery Office, 2018.

House of Commons House of Lords Joint Committee on the National Security Strategy. *Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017 - 19*. London: The Stationery Office, 2018.

House of Commons Science and Technology Committee. *Digital Government, Eighteenth Report of Session 2017-19*. HC 1455. London: The Stationery Office, 2019.
Intelligence and Security Committee of Parliament. *Russia*. HC 632. London: The Stationery Office, 2020.
INTERPOL. *COVID-19: Cybercrime Analysis Report - August*, 2020.
James, Margot, and Oliver Dowden. *Digital Government: Written Evidence*. HC1455, 2019.
Joint Committee on the National Security Strategy. *Cyber Security of the UK's Critical National Infrastructure, Third Report of Session 2017 - 19*. HL 222 HC 1708. London: The Stationery Office, 2018.
Local Government Association. 'Copeland Borough Council: Managing a Cyber Attack'. Press Release, 9 October 2018.
———. 'Cyber Pathfinder Training Scheme'. Web Page. Local Government Association, n.d. Accessed 7 February 2020.
———. 'Cyber Security - Resources'. Web Page, n.d. Accessed 7 October 2020.
———. 'LGA - Cyber Resilience Funded Programme 2019/20'. Web Page, n.d. Accessed 19 August 2020.
Martin, Ciaran. *Oral Evidence*. HC 1745, 2020.
Martin, Ciaran, and Rt Hn David Lidington. *Cyber Security Skills and the UK's Critical National Infrastructure: Oral Evidence*, 2018.
Ministry of Housing, Communities & Local Government. *Cyber Security in Local Government: Pre-Discovery*, 2020.
National Audit Office. *Investigation: WannaCry Cyber Attack and the NHS*. HC 414. London: The Stationery Office, 2018.
———. *Managing the Risks of Legacy ICT to Public Service Delivery*. HC 539, 2013.
———. *Progress of the 2016-2021 National Cyber Security Programme*, 2019.
———. 'The Digital Skills Gap in Government', 2015.
———. *The UK Cyber Security Strategy: Landscape Review*, 2013.
———. *Update on the National Cyber Security Programme*, 2014.
National Cyber Security Centre. 'Advisory: COVID-19 Exploited by Malicious Cyber Actors'. Press Release, 8 April 2020.
———. *Cyber Security Schools Audit Report*, 2019.
———. 'Penetration Testing'. Web Page, 8 August 2017.
———. 'What Is a WARP'. Web Page. Information, 15 November 2018.
NHS Digital. *2019 - 20 Annual Report and Accounts*. HC 537. London: The Stationery Office, 2020.
———. 'Advanced Threat Protection from Microsoft'. Web Page. NHS Digital, 7 July 2020.
———. 'Cyber Associates Network'. Web Page, n.d. Accessed 19 August 2020.
Norton. 'Zero-Day Vulnerability: What It Is, and How It Works'. Web Page. Norton, n.d. Accessed 27 March 2020.
Pedley, Daniel, Tania Borges, Alex Bollen, Jayesh Navin Shah, Sam Donaldson, Sam Furnell, and David Crozier. *Cyber Security Skills in the UK Labour Market 2020*. Department for Digital, Culture, Media & Sport, 2020.
Platt, Jo. 'For Better Cyber Security, Change Starts at the Very Top'. *New Statesman*, 3 May 2019.
St George's House Consultation. *Local Leadership in a Cyber Society 3: Building Resilience Together - Lessons for the Future*, 2019.
Timmis, Sarah, Luke Heselwood, and Eleonora Harwich. *Sharing the Benefits: How to Use Data Effectively in the Public Sector*. Reform, 2018.

UK Computing Research Committee. *Digital Government: Written Evidence*. DIG0002, 2018.

W, Emma. 'Security and Usability: You CAN Have It All!' *NCSC Blog*, 24 August 2018.

Walrond, Nick. 'Rethinking the Tech Skills Gap in Local Government'. LocalGov, 13 January 2020.

Red Hat. 'What Is IT Infrastructure'. Web Page, n.d. Accessed 7 August 2020.

Ziback, Adam, and Andrew Simpson. 'Towards Better Understanding of Cyber Security Information Sharing'. *IEEE*, June 2019.

REFORM

@reformthinktank

info@reform.uk

www.reform.uk

ISBN: 978-1-910850-43-5