WPI ECONOMICS

Developing Digital Resilience in the United Kingdom

Extending digital resilience beyond cyber security

November 2023

A WPI Economics report for Splunk

splunk>

Contents

About WPI Economics

WPI Economics is a consultancy that provides economics that people understand, policy consulting and data insight. We work with a range of organisations – from FTSE 100 companies, to SMEs and charities and Central and Local Government – to help them influence and deliver better outcomes through improved public policy design and delivery. Our focus is on important social and economic policy debates, such as net zero, levelling up and poverty, productivity and mental health. We are driven by a desire to make a difference, both through the work we undertake and by taking our responsibilities as a business seriously. We are an accredited Living Wage employer.

wpieconomics.com info@wpieconomics.com @wpi_economics

About Splunk

Splunk Inc. (NASDAQ: SPLK) helps build a safer and more resilient digital world. Organisations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions, and accelerate digital transformation.

Acknowledgements

We would like to acknowledge the significant input of all the individuals and organisations that contributed to this report as we gathered information and tested the ideas presented here. In particular we would like to thank Rayna Stamboliyska, Board Member of Renaissance Numérique and the wider WPI team, who pulled a lot of research together across multiple languages, and the government data experts and other national stakeholders who gave their time to assist in the development of our benchmark and our country research.

Introduction to the project

This report focuses on the United Kingdom and is part of a wider research project on digital resilience in Europe and its importance in enabling governments to respond to the opportunities of newer technologies in delivering core services, as well as to mitigate against an increasingly complex set of threats.

We have assessed three key European governments (France, the UK and Germany) on their approaches to digital resilience, analysing their performance to identify best practice, and areas for development.

We have also considered the wider context of government digital resilience, and what best practice looks like according to the multinational institutions monitoring resilience and cyber security, pulling out key insights and policy recommendations.

Creating a framework

Based on these principles of best practice, we defined a framework for analysing the focus countries, considering them against three key processes of digital resilience:

- **Prevention** - identifying key risks and detecting threats before they become major incidents;
- **Smoothing** - faster recovery to minimise impacts of outages and breaches; and
- **Enabling** - leveraging visibility to improve services and organisational resilience

We used this to develop a model drawing on Splunk's definitions of digital resilience, but which aligns with relevant international organisation views as well, including the OECD, EU and various cybersecurity indices.

Overarching observations

All countries we explored showed renewed interest in bolstering digital resilience post pandemic, having seen the events of 2020-2022 as a wakeup call. Overall, a core risk is that governments define digital resilience too narrowly, and as a result, miss out on the opportunities offered by new technology and/or cannot defend their systems sufficiently against a broader set of risks.

We found that:

- The approaches remain quite cyber security focused, despite a growing recognition of the importance of a whole systems approach, which considers organisational resilience on equal footing with cyber security.
- New thinking is having to grow out of historically quite conservative approaches, usually led by defence forces, which had tended to centre on cyber security rather than the breadth of considerations relevant to the future of digital resilience.
- Finally, all the countries we explored face challenges of legacy systems, teams, and tools, which are considered in more detail in the overarching report.

The following report will consider findings specific to the UK within this context, and the implications for the UK's future digital resilience policies.

Snapshot on the United Kingdom

Country Snapshot

United Kingdom

Prevention	Visibility	▲	• UK strategies focus on cyber security and the **prevention** of cyber threats specifically • Stress on **visibility** of systems and understanding of digital assets, and on **automated** asset detection and monitoring • The **visibility** element is strong due to mandates for the sharing of information about vulnerabilities between departments • However, **preventive** strategies mainly focus on cyber security and do not directly address the visibility of threats and risks to digital resilience which do not result from cyber-attacks
	Automation	●	
Smoothing	Collaboration	●	• **Smoothing** elements informed by UK cyber security strategy • Focused on minimising disruption from cyber-attacks, rather than holistic emphasis on responding to disruptions • Strong aims for **collaboration** in the UK's cyber security strategy texts, however, there are challenges around implementation • The **unity** of platforms and technologies across and even within government departments is limited by the prevalence of legacy systems • The importance of **simplification** and harmonisation of systems for wider digital resilience is not explicitly addressed
	Unity	▼	
	Simplicity	▼	
Enabling	Service Management	●	• Principles for **service management** and delivery of digital services are referenced in the Government Functional Standard on Digital, but resilience is not a primary focus • Where specific resilience guidance does exist on **enabling**, it continues to be mainly through the prism of cyber security • Reviews are also to be informed by **observation** and monitoring of systems. However, this guidance does not extend to digital resilience and potential benefits of a learning feedback loop are being missed • There is awareness of the challenges and opportunities presented by the pace of technological change, however no framework for continuous improvement and **innovation**
	Observability	▲	
	Innovation	●	

KEY

▲ **Fairly developed** - element is addressed in policy and/or is under implementation

● **Neutral** - either touched upon in policy or acknowledged as an area for future intervention

▼ **Not developed** - neither addressed through policy nor identified as an area for future development

Digital resilience in the United Kingdom

National approach to digital resilience

In the UK, key aspects of digital resilience are incorporated into national cyber security frameworks. Of these, the most important is the Cabinet Office's *Government Cyber Security Strategy (GCSS)*, which covers resilience to cyber security threats, for government departments and public sector organisations.[1] Additionally, *Cyber Assessment Frameworks (CAF)*, authored and maintained by the National Cyber Security Centre, provide a series of self-assessment templates, primarily for public sector organisations but also for private sector organisations with an interest in measuring their resilience to cyber security challenges.[2]

More broadly, there is general consensus that government guidance on general organisational resilience in the public sector has improved with the introduction of the Cabinet Office's *Government Resilience Framework*. However, digital resilience as a concept is still underdeveloped, with a greater emphasis on cyber security more narrowly, which creates a risk for future technology adoption and threat management.

There are some materials touching on digital resilience within the Government's Functional Standards. Specifically, Government Functional Standard 005: Digital.[3] In these, resilience emerges as a secondary theme, with management and direction of digital services the main focus. There is an opportunity for the Government to adopt a focus on a holistic concept of digital resilience – currently a "missing middle" in UK resilience planning – with existing resilience frameworks either too general, or too specific to cyber security.

Within the public sector, NHS England is currently providing a good example of a digital resilience framework through its "What Good Looks Like" framework.[4] While this touches on many areas of digital resilience, it is not fully comprehensive. This framework could provide an example for a more general, cross-governmental digital resilience framework, and also for in-house digital resilience frameworks for individual public sector organisations.

Digital resilience assessment framework

We benchmarked our three focus countries against the three processes of digital resilience identified in our framework (see Developing Digital Resilience main report) - prevention, smoothing and enabling - which were assessed against key elements of each process.

The **prevention** process, defined as a government's ability to detect and prevent threats and outages, is assessed by considering government's approach to automation and visibility. Note that prevention must not be limited to stopping cyber security incidents and must ensure that digital systems are sufficiently well understood for all outages to be prevented, as far as possible.

- The level of **visibility** across a digital system, including across systems, interdependencies and data sources, is essential to preventing both outages and threats. Assessing this element includes considerations of whether governments can foresee threats and potential disruptions and respond in advance based on sight across data sources and silos. This will include visibility of vulnerabilities to cyber-attack, but also visibility of system vulnerabilities that may lead to outages or performance issues as usage requirements change, or under iterative development.
- The level of **automation** is also instructive as to how strong the prevention process is within a digital system. Automated processes can create alerts and flag threats with automated systems to handle them. Assessing prevention capabilities includes considerations for which systems have been put in place to address alerts when they come up. Once again, these automated systems should n be narrowly tailored for cyber but should also flag other threats to system performance and reliability.

The **smoothing** process of digital resilience is defined as government's ability to recover and remediate more quickly from outages, or respond more quickly to threats, in order to minimise their impacts. It is assessed by considering the government's approach to collaboration, unity and simplicity within their digital systems.

- **Collaboration** between teams is necessary to be digitally resilient – teams need to be able to communicate challenges quickly and effectively, to share data to resolve problems across teams, and to be able to access each other's work and data to make improvements to systems or conduct data analyses. This element can be assessed based on whether teams share information and work together to resolve problems quickly, and whether this is facilitated by existing systems.
- To this end, some level of **unity** across systems, platforms and tools is required to enable cooperation across teams. If tools and platforms are unaligned, signals can be easily missed, and it is more challenging to have one version of the truth, making collaboration and visibility more challenging. This element is assessed based on how aligned systems are in terms of platforms and tools.
- Given the growing risk that comes with complexity, **simplicity** and clarity are essential for strength in smoothing. One version of the truth aligned across teams, tools and platforms allows for swifter action and stronger collaboration. This also applies to simplicity of procedures within the system, and clear communication of those procedures: in order to recover swiftly from outages, it is essential that procedures are clear. We therefore assess whether procedures and roles within the system are simple and easy to understand.

The final process of digital resilience is its enabling function, whereby the government is leveraging its visibility over its systems and processes in order to improve services, systems, threat detection and recovery processes. Note that continuous improvement should not be limited to cyber security but should instead cover all processes and technologies required to run resilient digital systems. The enabling function is assessed by its service management, observability and innovation elements.

- The **observability** element is essential to make sense of the visibility into an organisation's systems, processes and data. We define observability as the process of continuous analysis of the systems, services and processes data provided by good visibility, with the aim of making improvements across all other areas of digital resilience – particularly contributing to improved service management and innovation. This is assessed by whether insights are being derived from the visibility across the system, and whether this insight is being used to make improvements to service delivery or internal processes.
- **Service management** is needed to continuously improve the services provided to citizens, and is both a result of strong resilience, and contributes to it through this continuous improvement. A digitally resilient organisation has sight of and can remediate service quality issues through strong visibility into its processes and service data. This is assessed by considering the extent to which service quality and issues are monitored and tracked, and whether they are continuously improved upon.
- In a digitally resilient organisation, **innovation** can stem from the insights derived from good observability and visibility practices and be leveraged to improve outcomes, particularly with respect to learning lessons from previous breaches or outages. A digitally resilient system will have some process of continuous improvement based on these lessons learned from each incident and will build in this continuous improvement through a process of innovation. This refers both to technological and organisational (process) innovation. This is assessed by whether continuous learning is evidenced within the system, and whether this learning is used to improve threat detection or the digital experiences of citizens.

UK Assessment Results

Prevention

The UK's preventative frameworks and policies are partially developed. The GCSS, and the CAFs against which public organisations are assessed, both specify several measures for enhanced prevention of cyber security incidents.[5,6] In large part – and in alignment with this framework – these documents focus on **visibility** of systems and understanding of digital assets, and also on **automated** asset detection and monitoring.

These measures, while intended for prevention of cyber security incidents, will no doubt help to improve digital resilience more widely. In conducted interviews, some evidence has emerged that governments are beginning to focus on digital resilience more broadly. However, there is limited published evidence of work specifically on prevention within digital resilience, and no published government policy documents. This is a gap which will need to be filled to ensure that the Government is better able to address future threats and harness potential opportunities.

Under the visibility aspect of prevention, the GCSS requires that government has "comprehensive visibility and understanding of its digital assets", in order to "identify and manage vulnerabilities and cyber security risks they present". The GCSS further requires comprehensive visibility of the data being handled, and an assessment of risks presented. It is recommended that government organisations meet these objectives by "take[ing] advantage of available asset management tools which make it significantly easier for an organisation to know what it owns and operates, how they are configured, and where they are vulnerable". It is further required that information about vulnerabilities be shared between government departments, in order to create a "central view of critical vulnerabilities", through the use of a new cross-government vulnerability reporting service.[7]

Government strategies and frameworks – principally the GCSS and the CAF – specify a number of requirements around monitoring and detecting cyber security threats. These fit broadly into two categories:

- proactive assessment of risk profiles and developments in attack capabilities;
    - The National Cyber Security Centre's CAF specifies that organisations "maintain a current understanding of exposure … to publicly known vulnerabilities". Additionally, the CAF requires that organisations use "threat intelligence feeds … based on your business needs and sector".[8]
    - As specified above, the GCSS requires government departments and public bodies to proactively understand their digital systems and the vulnerabilities within them.[9]
- monitoring and detection of live cyber events, within systems.
    - The CAF specifies that organisations complete automated searches for abnormal activity on their networks. Objective 14 of the GCSS requires that government "networks, systems, applications and end points are monitored to provide proportionate internal detection capability".[10,11]

While these objectives are focussed on cyber security – with visibility interpreted in terms of assessing vulnerabilities and attack surface area, and not of assessing other risks and design weaknesses in digital systems – some of the monitoring and visibility requirements permit natural extension to other aspects of digital resilience. For example, if organisations are monitoring system performance to detect malicious cyber activity, then this provides a pool of data which could be used for a more holistic appraisal of the resilience of their systems.

Government strategies do require the **automation** of some aspects of prevention. The GCSS requires that government organisations have an "active and automated" method for asset discovery and management.[12] It further specifies that government bodies generate threat information "from the monitoring of their system in a systematised manner - automated wherever possible." The strategy also requires that the central mechanisms for threat information sharing between government departments and public bodies be automated wherever possible. These automated procedures,

while primarily focussed on anticipating and detecting cyber threats, provide a good basis for wider automated system monitoring and information sharing that if implemented will improve digital resilience.

For many public bodies, automated cyber capacity will in large part be provided by capabilities under the Active Cyber Defence programme.[13] Active Cyber Defence is a programme, run by the National Cyber Security Centre, which develops automated capabilities and utilities – to be shared across government – to detect and disrupt threats, and to provide self-service checks and alerts. These tools are complementary to system owners' investment in cyber security but will enhance automated capabilities for many public sector organisations. These automated capabilities, however, are more narrowly focussed on cyber security and are less transferable to wider digital resilience.

Smoothing

UK Government guidance on the policy and processes required for recovery from outages is largely informed by cyber security strategy. Within the domain of cyber security, detailed guidance exists for unity and coherence of platforms, **simplicity** of processes, and **collaboration** – both between organisations and departments and within.[14]

As with other areas, there is limited generalisation from a cyber security perspective to a more holistic emphasis on responding to shocks and outages. However, the practices and processes that are in place to allow for quick response to outages caused by cyber security incidents will no doubt prove useful when responding to all service outages.

Government strategy highlights the importance of **collaboration** in recovering from outages, with the GCSS stating that the ambition of government should be to "defend as one", with cyber security data, expertise and capabilities shared across government.[15] The strategy says that this will be facilitated by the establishment of a new Government Cyber Coordination Centre (GCCC), building on successful private sector models such as the Financial Sector Cyber Collaboration Centre (FSCCC).[16]

Central incident response functions will manage security incidents, with processes in place to ensure that "impacted parties are working collaboratively to minimise the impact", with the GCCC playing a "critical role". Alongside the GCCC, government will develop a cross-government vulnerability reporting service.

Our research indicates that cross-government collaboration frameworks are primarily focused on the specific threat of cyber-attack. There is less focus on collaboration in smoothing service outages that do not result from cyber-attacks.

A level of **unity** across systems, platforms and tools is required to enable cooperation across teams. Within the UK context, unity of platforms and technologies across government, and even within departments, is limited by the prevalence of legacy systems. The GCSS notes that "maturity, capability, investment and security understanding across government organisations remains inconsistent and the size and complexity of the government's digital estate, including the presence of legacy IT, makes the challenge significantly more complicated." [17]

There is, within the strategy, an ambition that government "manage, upgrade, or remove legacy technology across the government estate." However, there is no requirement for different government departments or teams to adopt the same technologies or platforms. For those services that are in use widely, common best-practice configurations are to be developed centrally and shared. Additionally, the adoption of common platforms and policies for different data classifications (e.g., OFFICIAL, OFFICIAL SENSITIVE, SECRET) should lead to some commonality between different government systems.

However, unity of platforms and technologies across government is largely intended for the purpose of reducing exposure to cyber-attack and making recovery from cyber-attack easier and quicker. While there will be some application to wider digital resilience – approaches that make recovery from cyber-attacks easier will also likely make it easier to recover from other outages – these policies do not directly address recovery from outages unrelated to cyber-attack. The Government Functional Standard on Digital suggests that government organisations ensure that digital services are "planned and managed as part of a unified and consistent system", and that dependencies between systems are understood - this needs to be further implemented.[18]

Simplicity and coherence of systems is undermined by the size and complexity of the Government's IT estate, which includes a significant amount of legacy technology and systems.

The CAF requires that information be available to different response actors. CAF Objective D requires that "operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential function". The CAF also requires that "continuity and disaster recovery plans" be easily available, practical, and implementable. It states that these plans must be tested by different methods to ensure their practicality and effectiveness.[19]

As with unity of platforms, simplicity is primarily considered in the context of cyber-attack. However, it seems likely that steps to improve smoothing in this context would also lead to easier and better recovery from all outages, including those that do not result from cyber-attack.

Enabling

The final process of digital resilience is its enabling function, whereby organisations leverage their visibility over their systems and processes in order to improve services, systems, threat detection and recovery processes. Within a UK context, there are significant gaps in government's frameworks and guidance for leveraging insights to improve services and to increase their resilience.

Where specific resilience guidance does exist, it is mainly through the prism of cyber security. Both the GCSS and the NCSC's CAF include significant guidance on learning from cyber incidents and from "near misses".[20,21] Additionally, significant guidance is in place for improving processes and services according to regular reviews of sectoral best-practices, and of organisations' own systems and their performance. And, in all cases, reviews are to be informed by observation and monitoring of systems.

However, this guidance does not extend to processes and policies for improving resilience of digital services more generally. This omission may lead to various government services being less resilient to non-cyber outages than would be the case under a more holistic strategy for continuous improvement.

From a **service management** perspective, assessment frameworks require some monitoring of the performance of services and of their accuracy. The CAF requires that organisations have a full understanding of normal system behaviour. However, this is for the purpose of threat detection, and not to manage the performance of services[22]. The Government Functional Standard on Digital goes further, specifying that service owners use qualitative and quantitative data to inform their understanding of their services, and to prioritise development and improvements. Performance metrics should be defined and collected by service owners, covering useability and efficiency of services, along with whether they are meeting defined service levels.[23]

The CAF further requires that organisations maintain recovery plans, for use in case of service outages, and that these are routinely tested for practicality and effectiveness. Incident response plans should be up-to-date and grounded in a thorough risk assessment.[24] While these recovery plans are primarily intended for use after cyber-attacks, they would likely be of use in tackling outages that are not a result of cyber-attack.

The GCSS requires **observability** of systems, such that government organisations have "proportionate monitoring capabilities", including the ability to retain and interrogate logs. These capabilities should be as holistic as possible, including monitoring domains, endpoints, cloud-based services, and privileged accounts.[25] Similarly, the CAF outlines observability requirements across several different areas, including identity and user access, device management, privileged user management, and access management. Requirements also exist for oversight of the security of data in storage and in transit.[26]

The CAF further specifies that normal system behaviours should be monitored and understood to such an extent that detection is possible by looking out for system abnormalities. While observability guidelines were clearly devised with cyber security in mind, practices such as logging, monitoring accounts, domains and endpoints, and monitoring end-user behaviour, all have clear application to observability more broadly.

Turning to **innovation**, in the cyber security context, the GCSS requires continuous learning and improvement, both from incidents and near misses, but also from routine testing and assurance exercises. It specifies that government learns from "every cyber security event": everything from serious incidents to near misses. This is to be underpinned by the "creation of a culture where cyber security colleagues feel confident sharing such information across government, without fear of embarrassment or blame."[27] Similarly, the CAF requires that an organisation "uses lessons learned from incidents to improve your security measures." Additionally, it states that continuous improvement will be driven by "real world testing and exercising", including the use of red teaming.[28] Under the CAF, it is required that policies be regularly updated to ensure relevance. It is made clear that this process is additional to reviews that must be carried out after cyber incidents and near misses. While the same continuous improvement framework is not in place for service outages that do not result from a cyber security incident, policies could be adapted that extend this approach to digital resilience more broadly.[29]

The Government's strategy also acknowledges both the challenges and opportunities presented by the pace of technological change. Artificial intelligence and quantum computing are identified as technologies that are of particular importance to cyber security.

Case study 1 – NHS England: "What Good Looks Like"

The COVID-19 pandemic, and the strains that it imposed on the NHS across the UK, required a transformational response. As explored in the Developing Digital Resilience report, during the pandemic NHS England achieved "a level of digital transformation that might have otherwise taken several years".[30]

As the pandemic has abated in the UK, NHS England has taken steps to ensure that care providers build on the progress made during the pandemic. As part of this, the "What Good Looks Like" (WGLL) framework has been developed, setting out "clear guidance for health and care leaders to digitise, connect, and transform services safely and securely".[31]

As part of the WGLL framework, each NHS Integrated Care System (ICS) is required to "routinely review system-wide security, sustainability, and resilience." Standards are set out in the Digital Technology Assessment Criteria for health and social care (DTAC).[32] This set of assessment criteria covers data protection standards, technical security, but also standards around interoperability and accessibility. Within technical security, there is an emphasis on cyber security, but also more general assessment criteria around logging and reporting, and load testing. In general, these assessment criteria require an ICS to have good *visibility* of its digital systems.

There are further cyber security requirements, additional to DTAC. For example, an ICS is required to implement a system-wide process for responding to safety recommendations and alerts from central bodies, including (but not limited to) NHS Digital. The NHS England WGLL framework additionally requires that an ICS ensures compliance with national contract provisions around technology-enabled delivery. In effect, these require an ICS to monitor the usage and performance of their systems, relative to these national standards. Once again, these requirements will lead ICSs to improve the *observability* of their systems, and their *service management* systems.

There are also digital transformation objectives surrounding "simplification of infrastructure", with a drive away from legacy systems - the ultimate aim being to retire legacy systems. Additionally, objectives are in place for more consistent use of national tools and services, to ensure that different teams in different places are using the same platform, and that custom tools and platforms within an ICS are configured to work together in the simplest way possible. By tackling unnecessary complexity, these objectives will lead to improved digital resilience.

The WGLL framework goes further than digital resilience. For example, the framework (and DTAC) covers clinical appropriateness of platforms, training for staff to use relevant platforms, and appropriate consultative design of citizen-facing platforms.[33] Additionally, WGLL specifies that ICSs should use data collected by systems to create intelligence platforms, to "improve outcomes and address health inequalities". The WGLL framework is included in A Plan for Digital Health and Social Care, a Department of Health and Social Care plan for digitisation of services.[34]

Case study 2 – Building Digital Resilience in Local Government

Local authorities are responsible for many different kinds of functions which includes everything from planning functions and infrastructure creation to delivering social welfare and many more. It is imperative that they capitalise on " technological and economic opportunities to both improve the quality of life and avoid digital and social exclusion".[35]

With this background, it is a positive development that local authorities in the UK have been shifting to digital provision of services in an accelerated manner, especially after the launch of the Local Digital Declaration in 2018, which pushed for "user-friendly, cost effective services, which are based on flexible, secure technology that can be reused across the sector".[36]

There is, however, a growing risk of cyber-attacks with an uptick in incidents across the country, including high profile attacks on Hackney and Redcar and Cleveland councils.[37] The Department for Levelling Up, Housing and Communities (DLUHC), through its Local Digital team, launched the Future Councils program in 2022. It is a pilot program that forges partnerships between Local Digital and six councils to "deliver replicable pathways to digital and cyber security reform that other councils can follow".[38]

The activities of the pilot program include:[39]

- Baselining current digital and cyber maturity, and develop a plan with DLUHC to make and evidence improvements
- Working towards adopting and meeting the Cyber Assessment Framework for Local Government
- Identifying at least one key service area to transform through migrating away from legacy technology
- Identifying organisational and cultural barriers to reform and create a plan to fix those

Potential impact of the program, especially once it is rolled out to all local authorities:

- Increased **service management** due to baselining exercise and development of evidence based improvement plan
- Greater **visibility** of potential risks as well as higher **observability** through adoption of the Cyber Assessment Framework for Local Government
- Creation of an **enabling** environment by mitigating barriers to reform and promoting organisational resilience
- **Innovation** in new technology and processes by moving away from legacy systems

Conclusion and recommendations

Government frameworks and guidelines on resilience are mainly focussed on the domain of cyber security: this limited definition of digital resilience presents a risk both to the future adoption of new enabling technologies and to the defence against a more complex set of threats. If the UK truly wants to be "AI ready" then a much stronger foundation of digital resilience is required to build upon.

The existing documents provide good guidance on best practices in resilience to cyber-attack, which could be built on to create a more sophisticated approach to digital resilience. For example, the simplicity and unity of systems necessary to restore services quickly after a cyber incident will also make it easier to recover from outages more generally.

The Government Functional Standard on Digital provides specific guidance on the delivery and management of digital services within government. This document is not explicitly about resilience, but many of the resilience measures assessed here overlap with best-practice guidelines within this standard. However, there is still a need for focussed guidance on management of threats to digital resilience outside of cyber.

NHS England's digital framework "What Good Looks Like" provides an interesting case study of a strategy that considers digital resilience holistically, without focussing on cyber security to the exclusion of other resilience considerations. This document could provide inspiration for an emerging government strategy and framework.

Our key recommendations:

There is a strong case for the creation of an **International Cooperation Taskforce**, given the process of standardisation of approach at the EU level, and calls from business for standardisation of regulations and expectations of digital resilience at the international level. The UK should ensure it has a voice at the table advocating for harmonisation options which work in the UK alongside EU models of digital resilience. Government should aim to work with ENISA (the EU agency for cybersecurity) to coordinate approaches.

The UK would benefit from extending the assessment of public sector organisations against the cyber assessment framework to include a **new assessment framework for digital resilience**. This would expand the existing cybersecurity assessment frameworks to include elements such as data privacy, risks related to outages of digital services, assessment of data sharing across departments, other measures of collaboration, and any other measures which could help assess the non-cyber-threat elements of digital resilience.

With some excellent examples of best practice, the UK should **formalise a lessons-learned or best-practice forum** where leading public sector organisations could provide guidance and training to share what they know. Some government departments in the UK are held up as exceptional in this sphere, but there is no sharing of their knowledge and expertise more widely. A best practice forum could provide this opportunity, as well as a regular space held to discuss potential new and upcoming threats.

Endnotes

1 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

2 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

3 Central Digital and Data Office, Government Functional Standard GovS 005: Digital, available here https://www.gov.uk/government/publications/government-functional-standard-govs-005-digital accessed at 20/11/23

4 NHS England – Transformation Directorate, What Good Looks Like framework, available here https://transform.england.nhs.uk/digitise-connect-transform/what-good-looks-like/what-good-looks-like-publication/ accessed at 20/11/23

5 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

6 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

7 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

8 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

9 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

10 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

11 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

12 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

13 National Cyber Security Centre, Active Cyber Defence, available here https://www.ncsc.gov.uk/section/active-cyber-defence/introduction accessed at 20/11/23

14 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

15 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

16 National Cyber Security Centre, Financial sector cyber collaboration centre (FSCCC), available here https://www.ncsc.gov.uk/information/financial-sector-cyber-collaboration-centre-fsccc accessed at 20/11/23

17 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

18 Central Digital and Data Office, Government Functional Standard GovS 005: Digital, available here https://www.gov.uk/government/publications/government-functional-standard-govs-005-digital accessed at 20/11/23

19 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

20 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

21 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

22 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

23 Central Digital and Data Office, Government Functional Standard GovS 005: Digital, available here https://www.gov.uk/government/publications/government-functional-standard-govs-005-digital accessed at 20/11/23

24 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

25 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

26 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

27 Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, available here https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 accessed at 20/11/23

28 Red teaming in this context is explained in the glossary of the GCSS, available here: https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

29 National Cyber Security Centre, NCSC CAF guidance, available here https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework accessed at 20/11/23

30 NHS England, Transformation Directorate (2021), What Good Looks Like framework, available here https://transform.england.nhs.uk/digitise-connect-transform/what-good-looks-like/what-good-looks-like-publication/ accessed 13/10/2023

31 NHS England – Transformation Directorate, What Good Looks Like framework, available here https://transform.england.nhs.uk/digitise-connect-transform/what-good-looks-like/what-good-looks-like-publication/ accessed at 20/11/23

32 NHS England, Transformation Directorate (2021), The Digital Technology Assessment Criteria (DTAC), available here https://transform.england.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac/ accessed 13/10/2023.

33 NHS England – Transformation Directorate, What Good Looks Like framework, available here https://transform.england.nhs.uk/digitise-connect-transform/what-good-looks-like/what-good-looks-like-publication/ accessed at 20/11/23

34 Department of Health and Social Care (2022), A plan for digital health and social care, available here https://www.gov.uk/government/publications/a-plan-for-digital-health-and-social-care/a-plan-for-digital-health-and-social-care accessed 13/10/2023.

35 Open Access Government, True digital levelling up is within reach for local authorities, available here https://www.openaccessgovernment.org/digital-levelling-up-local-authorities/142997/ accessed at 20/11/23

36 Department for Levelling Up, Housing and Communities, The Local Digital team, Future Councils: Delivering pathways for councils to become modern and resilient organisations, available here https://dluhcdigital.blog.gov.uk/2022/10/25/future-councils-delivering-pathways-for-councils-to-become-modern-and-resilient-organisations/ accessed at 20/11/23

37 Department for Levelling Up, Housing and Communities, The Local Digital Team, Piloting a Cyber Assessment Framework for Local Government, available here https://dluhcdigital.blog.gov.uk/2022/08/31/local-government-cyber-assessment-framework/ accessed at 20/11/23

38 Department for Levelling Up, Housing and Communities, The Local Digital team, Future Councils: Delivering pathways for councils to become modern and resilient organisations, available here https://dluhcdigital.blog.gov.uk/2022/10/25/future-councils-delivering-pathways-for-councils-to-become-modern-and-resilient-organisations/ accessed at 20/11/23

39 Department for Levelling Up, Housing and Communities, The Local Digital team, Future Councils: Delivering pathways for councils to become modern and resilient organisations, available here https://dluhcdigital.blog.gov.uk/2022/10/25/future-councils-delivering-pathways-for-councils-to-become-modern-and-resilient-organisations/ accessed at 20/11/23

WPI Economics Limited

5-6 St Matthew Street
London
SW1P 2JT

@WPI_Economics

wpieconomics.com

WPI Economics Limited, registered address 28 Church Road, Stanmore, Middlesex, England, HA7 4XR, is a registered as a limited company in England and Wales under company number 10086986.

November 2023