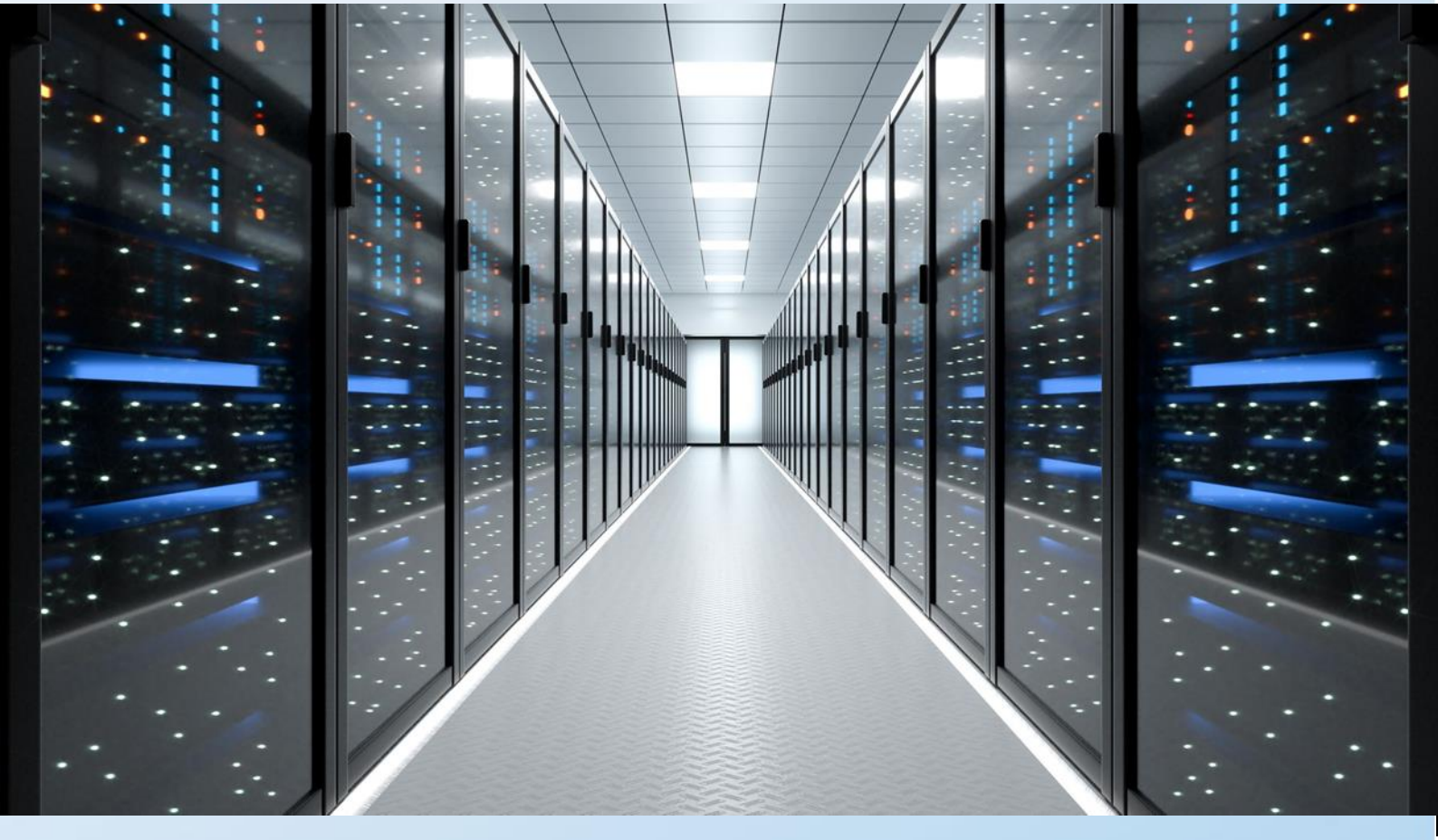
wsp

Department for Science, Innovation & Technology

Study report

THE CHANGING CYBER THREAT PROFILE AND POTENTIAL IMPACT ON LOCAL COUNCILS



Department for Science, Innovation & Technology

Study report

THE CHANGING CYBER THREAT PROFILE AND POTENTIAL IMPACT ON LOCAL COUNCILS

DATE: 28 APRIL 2025

WSP

3rd Floor
11 Westferry Circus, Canary Wharf
London
E14 4HD

WSP.com

CONTENTS

EXECUTIVE SUMMARY

WSP has undertaken this study on behalf of the Department for Science, Innovation & Technology (DSIT) into the potential cyber risks which emerge from English local councils' digital projects in a selection of critical areas including: Communications, Emergency Services, Energy, Food, Government, Health, Transport or Water. *DSIT Note*: While these are Critical National Infrastructure (CNI) 'sectors', it should be noted that the digital projects in this research are not to be considered CNI.

The evolving cyber threat landscape presents significant challenges for local councils, with various risks targeting critical infrastructure and services. These threats often exploit weaknesses within systems, putting both the security of sensitive data and the continuity of vital services at risk with the potential to cause serious harm to human life/health or extensive disruption to our daily lives.

The study has drawn on desktop research and direct engagement with local councils through online surveys and structured interviews to investigate these threats.

The current global cyber risk trends and landscape

As outlined in the National Cyber Security Centre Annual Review 2024, the current threat landscape has seen a significant increase in cyber-attacks, with the National Cyber Security Centre incident management team handling 1,957 reports in 2024, a 15% rise from 2023. Notably, 89 incidents were nationally significant, and 12 were severe, a threefold increase from the previous year. Geopolitical risks from global conflicts and the use of Artificial Intelligence by nation-state actors and cyber criminals have amplified the overall cyber threat.[1]

Emerging threats include ransomware, which is shifting from encryption to data exfiltration extortion, and phishing, which is expected to rise with Artificial Intelligence (AI) and deep fake technologies. The proliferation of low-skill commodity cyber tools and the exploitation of SOHO (small office / home office) devices for Internet of Things botnets, Distributed Denial-of-Service attacks, credential stuffing, firmware exploits, and Man-in-the-Middle attacks are also notable concerns.

Third-party system supplier risks are heightened by the complexity of the evolving cloud ecosystem, with numerous providers and services increasing the risk posture. Misconfigurations and poor security practices continue to drive large-scale data breaches, particularly in local government. Hybrid infrastructures which blend cloud and non-cloud technology solutions are prime targets for cyber attacks due to their potential for bidirectional lateral movement.

An overview of local council CNI sector digital projects

Based on the responses to the study survey, the digitalisation in CNI areas was prevalent, with local councils actively deploying smart technologies to enhance public services in the selected critical areas, chosen for their relevance to LAs. While Communications and Health projects led the transformation, other sectors, including Transport, Emergency services, and Energy, are also experiencing significant digital investment and innovation. The only critical sector not reportedly touched on in an example by respondents was Food.

Key areas of digital projects/services (within the shortlist of CNI sectors included in the survey) raised by respondents were:

- Communications : Wi-Fi, 5G infrastructure, fibre cabling improvements
- Health: IOT devices for adult social care home telecare and monitoring; and for damp monitoring in housing stock
- Emergency services: vehicle telematics for fire and rescue services, data sharing with law enforcement, CCTV (security and surveillance), Emergency Services Network for secure communications, digital emergency resilience planning
- Transport: urban traffic management control (sometimes including AI), smart street light management systems, autonomous and connected vehicle pilots, AI for predictive road maintenance, road tunnel systems, people movement sensors (Bluetooth)
- Energy and environmental: systems managing waste-to-energy plants, IoT air quality monitoring sensors
- Government (inter-agency digital platforms for information exchange)
- Water: IoT flood and drainage monitoring sensors

The four most prevalent technology types mentioned in survey responses were use of Cloud Computing services; use of IoT devices; use of third-party services; and AI or Machine Learning.

Cyber threats and vulnerabilities for local councils in these critical sector digital projects

The study explored with participants the main categories of threats and vulnerabilities they perceived for their critical sector digital services and projects.

Many of the local councils voiced confidence that they can effectively deal with these threats and vulnerabilities, acknowledging instead that many of the biggest vulnerabilities relate to the knowledge and practices of employees and third parties in relation to existing cyber security policies and emerging risks.

The key areas of vulnerabilities raised were:

- Being specifically targeted (as local government bodies) for denial-of-service attacks
- Increasingly sophisticated phishing attacks (including AI-enabled)
- Third party supply chain vulnerabilities
- Accessing via poorly secured IoT Remote Sensors
- Insufficient access to security expertise and resources
- User awareness and behaviours
- Lack of multifactor authentication

[1] National Cyber Security Centre Annual Review, 2024
https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf

- Insufficient preparedness for Incident Response
- Insufficient early involvement of in-house cyber expertise in new digital projects

Notably, a theme from interview participants was simply the scale and diversity of technology projects within the local council environment. Ensuring that such a wide variety of Information and Operational Technology systems remain compliant with current security standards is challenging.

Identified gaps in cyber practice and maturity within local councils

Survey and interview data provided evidence for a relatively high level of cyber maturity across participating local councils, with evidence of good practice. However, several key gaps in common cyber practice emerged. A reactive approach to cyber threats rather than a proactive strategy in some authorities was clear. Specifically, key gaps emerged in areas such as incidents exposure and response, board level representation, susceptibility to attacks, misplaced reliance on external entities, threat monitoring, user awareness and behaviour, and automation and real-time response.

Guidance and regulation which local councils currently use

The majority of participating local councils referred to at least one form of cyber security guidance when discussing their critical sector projects, with over half from the survey and interviews utilising multiple sources. Among the most widely referenced were:

- National Cyber Security Centre (NCSC) guidance[2]
- International Organisation of Standardisation (ISO) 27001
- NCSC's Cyber Assessment Framework (CAF)
- Public Services Network (PSN) Code of Connection

In addition to frameworks such as Cyber Essentials, National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standard (PCI-DSS), references were also made to government departments ike the Ministry of Housing, Communities and Local Government (MHCLG), and initiatives such as the Health and Social Care Network (HSCN). This highlights the diverse approaches taken across local councils and the wide array of sector specific guidance issued by central government bodies and professional associations.

However, the range of guidance from different sources, relating to different sectors, made compliance and conformance with all of these a complex challenge for a local council to be on top of, and was felt by some that it might be inefficient.

Additional guidance and support that might be needed

Despite good engagement with a range of existing guidance, the effectiveness of current frameworks was often felt to be inconsistent, particularly with gaps in approach to enforcement and examples of practical detailed technical application.

Specific requests for further support can be themed into three areas:

[2] Such as the NCSC Cloud Security Principles and Ten Steps to Cyber Security

1. Consolidating national guidance and enhancing standardisation for local government. For example, a mandatory cyber security baseline for local councils, ensuring consistency across the sector. Current frameworks such as the National Cyber Security Centre's Cyber Assessment Framework should incorporate clearer, tangible targets, aligned with established international standards.
2. Advice and guidance on future-proofing current and legacy systems against emerging threats: Provide strategic direction on emerging risks such as quantum-resistant cryptography and evolving security threats (including 'hijacked' Connected Autonomous Vehicles).
3. Ensuring the right eco-system of support mechanisms:
    .a Supporting enhanced collaboration between local councils e.g. shared training resources and procurement frameworks, could reduce duplication and improve cyber resilience across the sector.
    .b Funding and Insurance: Introduce flexible funding mechanisms that align with local council budget cycles and consider the provision of specific insurance to help recovery after a successful attack.
    .c Encourage greater deployment of Security Operations Centres (SOC) for local councils, to provide continuous monitoring and rapid incident response, mirroring successful models used in the NHS. This might build on the current trial being undertaken by Ministry of Housing, Communities and Local Government (MHCLG) Digital where ten authorities are sharing a joint SOC support service.

INTRODUCTION

1 INTRODUCTION

On behalf of the Department for Science, Innovation & Technology (DSIT), WSP has undertaken this study into the potential cyber risks which emerge from English local councils' (LA's) digital projects in Critical National Infrastructure (CNI) areas, particularly those using new and more innovative technologies.

Cyber security breaches in such projects have the potential to cause serious harm to human life/health or extensive disruption to our daily lives. This study seeks to understand where the highest areas of risk may be and whether there is opportunity for improved policy guidance or legislation to help reduce those risks.

1.1 CRITICAL NATIONAL INFRASTRUCTURE SECTORS AND LOCAL GOVERNMENT

CNI in the UK refers to the systems, assets, and services that are vital for the country's national security, economic stability, and public safety. These are the elements of infrastructure crucial for the functioning of society and the economy, and their disruption or destruction would have significant consequences including potential loss of life.

CNI encompasses a wide range of sectors, including energy (such as electricity and gas supply), water, transportation (like highways, railways and airports), communications, health services, financial services, and emergency services.

DSIT Note: It is important to note that, as set out by the National Protective Security Authority (NPSA), not everything within a CNI sector is judged to be 'critical'. In most cases throughout this paper, while local councils managed technologies that fall within a defined CNI sector they are not to be considered 'critical', and as such should not be considered CNI. The UK government's official definition of CNI is:

> *'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*
>
> *a) Major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or*
>
> *b) Significant impact on national security, national defence, or the functioning of the state.'*

While local councils do not have direct responsibility for CNI, they can be responsible for various services or infrastructure that fall within a CNI sector. Whilst these will vary, authority to authority, an illustrative list might include:

1. Communications e.g. telecoms or 5G towers, Wi-Fi services
2. Emergency Services, e.g. tracking software for ambulances, data sharing with the police of local council managed CCTV and facial recognition.
3. Energy e.g. local council managed energy companies, renewable energy projects (solar, wind etc).
4. Food e.g. technologies supporting local council managed food banks.
5. Government e.g. digital devices used to facilitate communications between government agencies that exceed that used in private sector (i.e. excluding software such as Microsoft Teams, mobile telephones)
6. Health and Social Care e.g. smart technologies used to monitor vulnerable people in their homes, health programmes not managed by the NHS / DHSC.
7. Transport e.g. road tunnel systems, AI traffic light systems and other 'smart' traffic management systems, autonomous vehicles.
8. Water e.g. waste management monitoring, early warning flood systems, digital depth sensors in reservoirs.

The study reports on which of these areas participants have as live digital projects or services.

1.2 INCREASED DIGITISATION AND CYBER RISKS

The UK has seen a significant push towards the digitisation of public services, aimed at improving accessibility, efficiency, and user experience. This transformation is part of a broader government strategy to harness digital technology to meet the evolving needs of citizens.

Local councils are also adopting digital technologies to improve service delivery. Many now offer online portals for residents to report issues, pay bills, and access local services. The use of data analytics and artificial intelligence is becoming more prevalent, helping authorities to make more informed decisions and deliver more personalised services. Overall, the digitisation of public services is creating a more connected, efficient, and user-friendly public sector, ultimately benefiting citizens and local councils alike. However, increasingly this means that those projects in critical areas delivered by local councils also have increasingly more significant digital elements which might be open to cyber-attacks.

There have been a number of examples in the last few years of cyber impacts on local government services. A range of recent local government incidents are explored in section 3.

1.3 EMERGING TECHNOLOGIES

Emerging technologies are particularly vulnerable to cyber risks due to several factors. The rapid development and deployment of these technologies can lead to security being an afterthought, with potential vulnerabilities overlooked. Their complexity and interconnectivity increase the attack

surface, providing more entry points for bad actors. Additionally, the lack of standardisation and insufficient security awareness can result in inconsistent security measures and poor practices, making these technologies easier targets for cyber-attack.

Moreover, sophisticated threats such as advanced persistent threats (APTs) and zero-day exploits are continually evolving to exploit new technologies. Regulatory and compliance challenges also contribute to the vulnerability, as frameworks may lag the pace of technological advancement.

Addressing these vulnerabilities requires a proactive approach to security, including incorporating security by design, ongoing risk assessments, and staying informed about the latest threats and best practices. By prioritising security by design from the outset, local councils and their partners can help minimise the cyber risks associated with emerging technologies.

This study has particularly sought to draw out specific local council experience across eight emerging technologies:

1. Artificial Intelligence & Machine Learning (AI/ML)
2. Internet of Things (IoT) & Operational Technology (OT)
3. Cryptocurrencies & Blockchain
4. Remote Work & Collaboration Tools
5. Supply Chain & Third-Party Services
6. Biometric & Identity Systems
7. Quantum Computing (Emerging Risk)
8. Connected and Autonomous Vehicles (CAV)

These technologies were selected after identifying technologies with higher cyber risk through a combination of authoritative sources including national cyber security agencies and industry threat reports. This list was reviewed and finalised by WSP's Cyber Expert group.

1.4 THE LOCAL GOVERNMENT LANDSCAPE

In England, local government is organised into several tiers, each with distinct responsibilities and functions. The primary tiers are county councils, district councils, and unitary authorities. County councils cover larger geographical areas (typically a rural and town mix) and are responsible for services such as education, transport, and social services. Within these counties, district councils handle more localised services like housing, planning applications, and waste collection. In some areas, unitary authorities combine the functions of both county and district councils, providing all local government services within a single administrative body.

Metropolitan areas, like Greater London or Greater Manchester, have their own unique structures. For example, the Greater London Authority oversees strategic functions across London, whilst 33 individual borough councils (including the City of London) manage local services. This multi-tiered system ensures that local governance is tailored to the needs of different communities, providing a balance between broad oversight and localized attention.

Combined Authorities are a type of local government structure in England that allow multiple local councils to collaborate and make decisions on a regional basis. These authorities are established through agreements between two or more local , typically within a metropolitan area or a region with shared economic and social interests. The aim is to improve coordination and efficiency in delivering services and implementing policies that affect the entire region.

Combined Authorities often have responsibilities for areas such as transport, economic development, housing, and skills training. They are usually led by a directly elected mayor, who has additional powers and funding to drive regional growth and development. Examples include the Greater Manchester Combined Authority and the West Midlands Combined Authority.

Given the diversity in structures, responsibilities, local leadership and assets, no two local councils are alike, therefore whilst we the study has sought representation from different authorities (type, size, projects in different technical domains), only on a per-authority basis can the extent of the risks and impacts be fully understood. Therefore, this study sets out indicative impacts that individual authorities may wish to consider.

1.5 RESEARCH QUESTIONS

This study has sought to advance understanding using five key questions:

1. What are the current global cyber risk trends?
2. What kinds of CNI area digital projects are local councils undertaking?
3. What are the cyber threats and vulnerabilities to which local councils are exposed in these CNI area digital projects?
4. What are the gaps in cyber practice and maturity exhibited by these local councils?
5. What guidance and/or regulation do local councils currently use for their CNI areaprojects and services, and what additional guidance/regulation might they need?

1.6 STUDY APPROACH

The study has used a methodology developed and agreed with DSIT. It has drawn on desktop research and direct engagement with local councils through an online qualitative survey and structured interviews. Throughout the report the findings are illustrated with direct quotations from interview participants (which typically included multiple participants from an authority in the same interview).

There may be a risk of self-selection bias, where only participants with specific confidence levels in their domain knowledge chose to participate.

This report is structured around each of the research questions such that:

- Section 2 sets out the methodology of the study, explaining how the data were collected
- Section 3 sets out an overview of current global cyber security risks and trends, particularly as they relate to local government bodies (Question 1)
- Section 4 provides further detail on the CNI and digital landscape in local councils (Question 2)

- Section 5 sets out what the cyber risks and impacts could be on the local council critical sector infrastructure (Question 3)
- Section 6 summarises the cyber security practice and maturity within local councils (Question 4)
- Section 7 details the existing cyber security guidance and identifies recommendations for future additional guidance for local councils (Question 5)
- Section 8 provides a summary of the study

In support of the findings, five case studies have also been developed. These are composites and reflect different scenarios that authorities who took part in the study reported. These include different levels of maturity and challenges with potential solution strategies for overcoming those challenges.

The picture can't be displayed.

METHODOLOGY

2 METHODOLOGY

2.1 INITIAL CYBER THREAT, VULNERABILITIES AND MITIGATIONS DESKTOP RESEARCH

This work was undertaken to identify the range of potential threats, vulnerabilities and mitigations relevant to local council critical sector projects in support of subsequent research activities. (To note: these projects are not themselves classified as CNI).

The desk-based research adopted a structured approach, drawing from a range of authoritative sources across governmental, commercial and academic industries. Data for our project was gathered from entities such as the ICO, NIST, the FBI and NCSC, as well as highly trusted cybersecurity platforms such as CVE details and MITRE. A list of sources reviewed can be found in Annex G.

The sources were reviewed critically, and then categorised into thematic areas. The areas included vulnerability trends, sector specific incident reports, and emerging risks-with a particular focus on Artificial Intelligence. Quantitative data had then been extracted into spreadsheets and analysed to identify the historical patterns and forecast any emerging risks. The structuring WSP used allowed for comparative analysis of different sources, which helped to surface meaningful insights aligned to the research aims.

2.2 PARTICIPANT RECRUITMENT FOR INTERVIEW AND SURVEY

A purposive approach was taken to recruit participants for the survey and interviews. The goal was to gather participants from local councils at the ‘leading edge’ of digital deployment, ideally with clear critical sector digital projects. The recruitment pool for invitation to complete the survey was 120 local councils, of which a smaller sub-set were invited to participate in in-depth interviews.

To start recruitment, an initial desktop research exercise was undertaken to identify the long list of English local councils with associated Chief Executives' contact information. This was expanded during the research to include local councils in Wales and Scotland, with the aim of increasing participation rates. In addition to the Chief Executive's contact information, methods for identifying stakeholders more appropriate for research activities (e.g., Heads of IT, Cyber Security Managers, etc.) were gathered using the following approaches:

- Publicly available information from local council websites, such as leadership structures.
- Sending communication to Chief Executives to engage local councils in project activities. Request that details be forwarded to appropriate personnel within the local council.
- Using WSP's existing relationships with local council stakeholders to identify relevant participants

WSP began by contacting and recruiting larger local councils (e.g. Combined Authorities), followed by smaller city and district councils, to achieve a spread of size and location. A privacy notice outlining how data would be handled was provided with the invitation to participate for both the survey and the interviews.

2.3 SURVEY

The electronic survey was delivered using the SmartSurvey software platform to collect responses, and was live from 21st February until 28th March 2025.

Participants were asked for their email address to allow for follow up in-depth interviews.

The survey included an initial filtering question about critical sector projects, directing participants to the end of the survey if they were not engaged in digital projects in critical sectors or did not know that they were. Our purposive sampling approach aimed to limit the number of local councils who were not appropriate, though a third of completers indicated they were not involved with critical digital projects.

Both the survey and interview topic guide (found in Annex B and Annex C respectively) refer to local council projects that are described as 'falling under' CNI, CNI projects involving local councils, and 'CNI areas'. This framing was intended to clearly define the scope of interest for participants and align the research with the sectors and questions outlined. However, as mentioned in the earlier explanatory note, the projects discussed are not considered 'critical' under the NPSA definition of CNI. . This distinction was made explicit through examples provided to participants (such as the use of digital technology in waste management monitoring) which illustrate that while the projects operate within critical sectors, the digital initiatives themselves do not constitute CNI. To ensure accuracy, the findings shared later in this report are clarified as relating to projects situated in critical sectors, though are not formally part of CNI.

To support as high a response rate as possible, the survey was designed to take under 10 minutes to complete.

As well as questions related specifically to critical sectors, a small selection of questions from the Human Affected Cyber Security (HACS) framework[3] were included to allow a partial cyber maturity level to be assigned. The full HACS framework includes upwards of 70 questions to do a thorough mapping to cyber maturity levels which was too many for this brief survey. 22 relevant questions from the full set were selected jointly with DSIT, as those most supportive of answering the study research questions. The cyber maturity levels assigned to each respondent organisation should be taken as indicative.

The survey window was extended twice to encourage more responses, including promotion to members from ITS (UK), Local Government Association (LGA) and the Welsh Local Government Association (WLGA).

30 survey responses were recorded from local councils in England. No responses were received from Welsh or Scottish local councils.

2.4 INTERVIEWS

15 interviews were then conducted between 18th February and 11th April 2025 with local councils to explore cyber security in digital critical sector projects more deeply, eight of whom also completed

[3] ibid

the accompanying survey. Of the 15 interviews, one was conducted in person and the remaining were held online.

Across the 15, the goal was to achieve a spread of:

- **CNI areas**
- **Project stage**
- **Technology used**

To aid this, a log was kept of the CNI areas, project stage and technologies discussed in each interview to focus on unexplored areas in interviews with subsequent local councils. A good spread was achieved though no local councils reported projects in certain CNI areas (e.g. Food), nor with certain of the technologies (e.g. Quantum). A range of local councils' size and region was also achieved.

A topic guide was developed and followed for these interviews (Annex D). Each interview lasted around an hour and was recorded and auto-transcribed.

2.5 ANALYSIS

The analytical approach justified by this exploratory work and the research questions is more qualitative than quantitative. The analysis and reporting has highlighted the *kinds* of risks (threats and vulnerabilities) which were found and from where they emerged (the kinds of technologies and projects) as well as the *kinds* of actions in place (mitigations) to manage them, rather than providing an in-depth quantitative assessment of *the extent of those risks*. Where charts are provided, they describe the survey sample rather than giving indication about the whole local council population.

The interviews were analysed to draw out emergent themes. Two researchers listened to the interview recordings independently and outlined the main themes. These themes were then collated across interviews and consensus between the researchers reached. Quotations have been used to support points made throughout this report. Where a quotation is used, it is accompanied by a high-level description of the type of individual from which the quotation came i.e., Team leader or team member, working in either an IT, cyber, security, or data role. Specific job descriptions have not been included in order to protect the identity of the individual and their local council.

The five case studies were also formed from the interview data with the goal of providing compelling, evidenced-based stories about cyber risk in local council critical sector projects, to support DSIT and local councils in identifying both risky and resilient practice.

2.6 LIMITATIONS

Whilst care was taken in the development of the survey questions and the interview topic guide, there are a number of limitations to the data collection methods used in this study.

Both methods are prone to a number of biases, such as social desirability bias (saying the 'right' thing) and sampling bias (only certain 'types' of people respond):

- Given the potentially sensitive nature of the topic (cyber security), which can involve concerns to reputation, survey respondents and interview participants *may* have presented viewpoints in a socially desirable manner.

- Whilst a broad spread of local councils were invited to participate in the survey, a relatively small number did so. The interview sample is also likely to biased towards organisations with a level of confidence in their cyber security practice.

The interviews adopted a semi-structured interviewing approach: using a small set of questions to guide the conversation, but allowing for flexibility in the development of the conversation. This is valuable in obtaining insights which are specific to individual participants. However, it also means that interviews are difficult to compare (and as such findings have not been quantified as the survey has done). It may also explain differences in findings between the surveys and the interviews, as the interviewer may ask bespoke questions which lead to insights which could not be obtained from the survey alone. Comparison between responses is also limited by the fact that survey respondents and interview participants have different roles and responsibilities at their respective local council.

These limitations mean the findings cannot be said to be representative of the whole local council population, nor are they generalisable to other local councils. Nevertheless, they do provide useful insights into the ways in which local councils are experiencing and implementing cyber security.

The picture can't be displayed.

GLOBAL CYBER SECURITY TRENDS AND DEVELOPMENTS

3 GLOBAL CYBER SECURITY TRENDS AND DEVELOPMENTS

Our desktop research provides the insight and analysis for the upcoming sections.

As digital technology transforms and accelerates, organisations must be equipped to anticipate and respond to the risks which arise. Recognising these trends is essential when ensuring the resilience of critical systems. Technological advancements and shifts in cybercriminal tactics emphasise the importance of understanding previous attacks and mitigation strategies.

Analysis during the desktop research presented key patterns and developments (as of early 2025), to provide understanding of the type of threats which local councils may face. The research highlights new methods of cyber attacks driven by emerging technologies .

This analysis[4] also includes a summary review of historical cyber-attack data from the past five years, alongside an assessment of the risk posture associated with emerging technologies.

3.1 ANALYSIS OF RECENT HISTORICAL CYBER INCIDENTS IN THE UK

THREAT ACTORS

In general, there are two groups of threat actors:

- Advanced Persistent Threats (APTs) who are often backed by nation-states or organisations with geopolitical, military, or ideological goals. Their goals include espionage, disruption, stealing intellectual property and compromising national security.
- Cybercriminals, who are primarily motivated by profit. These actors focus on extortion, fraud and theft of credit card data and / or cryptocurrency.

Both APTs and Cybercriminals have attacked UK government and local government systems, and this trend is expected to increase in the future.

CLASSIFICATION OF INCIDENTS

The classification of attack types are summarised below:

- Brute force attack – when an attacker tries a large number of possible keyword or password combinations to gain unauthorised access to a system or file.
- Denial of service – when a network or server, such as a website, is maliciously flooded with manufactured traffic (typically using botnets) to either cause it to fail or flood it with so much traffic that legitimate users can't access it.

[4] Historical Cyber-attacks - To identify trends of cyber-attacks (incidents) and vulnerabilities we collected data from:
- UK and US Government sources (NCSC, NIST, CISA, ISO, FBI)
- Commercial Services and Vendors (MITRE, CVEdetails, Shodan)
- Cyber Security Community (www.hackmageddon.com)

- Malware – a general term used to refer to a variety of forms of hostile or intrusive software including computer viruses, worms, Trojan horses, spyware, adware, scareware, and other malicious programs. Malware is short for 'malicious software'.
- Phishing – an attempt to obtain information by posing as a trustworthy entity, deceiving recipients into sharing sensitive information (such as usernames, passwords, or credit card details) or by encouraging them to visit a fake website.
- Ransomware – a type of malware that unlawfully encrypts a user's files and demands a ransom to unencrypt files, usually in the form of cryptocurrency.
- Unauthorised access – an unauthorised individual has gained access to personal data. This can include unauthorised disclosures. This incident type is used both in instances where an individual has unlawfully accessed or disclosed information and where a third party has forcibly accessed a system.

VOLUME OF INCIDENTS

In 2024, the NCSC Incident Management (IM) team received 1,957 reports of cyber attacks covering a range of sectors. These were triaged into 430 incidents requiring support from the IM team. Of these incidents, 89 were nationally significant, 12 of which were at the top end of the scale and more severe in nature.

Specifically, within the local government domain (directly or indirectly) we can see a number of significant incidents since 2020 including:

a) In October 2020, Hackney Borough Council in London experienced a significant cyber-attack that severely disrupted IT systems. The attack led to the encryption of data, affecting various public services and operations. The specific attackers were not publicly identified, but the incident was indicative of ransomware attacks targeting public sector organisation.

b) In December 2021, Gloucester City Council suffered a significant Data Breach and Ransomware attack as more that 240k files were transferred to a file sharing site in New Zealand.

c) In March 2023, Capita -who provide services to many UK local councils, private companies, and public sector organisations - suffered a data breach, which was a significant cyber security incident that affected one of the UKs largest outsourcing and IT service provider.

d) In October 2024, there were a series of Distributed Denial of Service (DDoS) attacks that disrupted services from nine councils by the pro-Russian hacktivist group (NoName057(16)) that emerged in the context of the ongoing Russian-Ukraine conflict.

FORMS OF ATTACK

The Information Commissioners Office (ICO) collate information on data security breaches that have been reported to them by UK organisations. Examination of the ICO's data dashboard on Data

Security Incident[5][6] shows that Phishing is the most prevalent reported security incident, with 1,078 reported incidents in the first three quarters of 2024.

> "We get phishing attacks all the time… There are all sorts of things going on all of the time… Looking for vulnerabilities is constant, but that's just par for the course." **Interview participant 13, Team leader, IT and cyber security**

Ransomware is the second most prevalent at 603 reported incidents. The third most prevalent reported incident at 550 in the first 3 quarters of 2024, is described as 'other cyber incident'.

ICO figures on reported incidents in UK local government show Ransomware was the most prevalent (37) in the first three quarters of 2024. 'Other' was the second most prevalent incident category at 24, and Phishing was the third most prevalent at 22 reported incidents for local government.

3.2 ANALYSIS OF RECENT CYBER VULNERABILITIES

The NCSC reported recent historical vulnerabilities (Figure 1). Figure 1 shows that cross-site scripting continues to be the most reported vulnerability, although the total is down from last year. Information disclosure continues to be the second most reported vulnerability, with an increase from 2023.

[5] https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-security-incident-trends/

[6] Figures reported here were extracted by WSP from the ICO's Data Security Incident Trends dashboard. The dashboard was filtered to the first three quarters of 2024, and to show 'Cyber' as the Incident Category'. Data for each 'Incident Type' was then analysed to assess the most commonly reported types of incident. The dashboard was further filtered to show 'Local government' as the Sector for figures reported on local government.

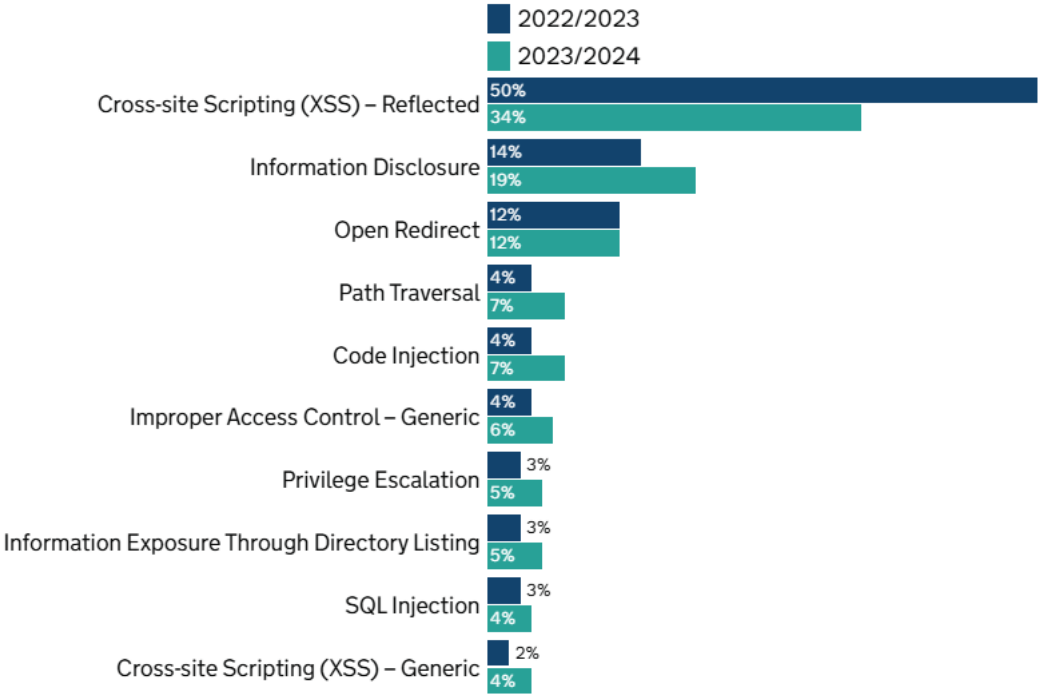


Figure 1:[78]

3.3 ANALYSIS OF TRENDING AND EMERGING TECHNOLOGY AND THREAT VECTORS

In this section we focus on the use of emerging technologies and the digital risk they present. We have grouped technology into three areas of maturity:

- **Established** – represents technology widely used and understood, with high maturity Technology Readiness Levels (TRL[9] 8 – TRL 9)
- **Trending** – represents emerging technology that have started to be adopted, products are available on the market, standards are being proposed (TRL 5 – TRL 7)
- **Emerging** – represents technology in active research, validating feasibility of theoretical concepts and testing components integrate within a laboratory environment (TRL 3 – TRL 4)

7

8 Source https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024

9 Technology Readiness Levels (TRLs) are an international standardised framework to assess the maturity of technologies, particularly in research, development, and innovation contexts. These levels range from 1 to 9, with each step marking a higher stage of development.

For the purposes of this study, we will focus technologies and digital services that represent either a high or critical cyber risk due to their widespread use, data sensitivity, and attractiveness to threat actors.

Table 1 shows the five levels of risk applied and Table 2 shows the breakdown of high-risk categories and their associated overall cyber risk level. We have selected nine technologies and digital services that represent higher cyber risk especially when deployed on critical sector projects. All score 'Elevated' and above, which means that as a minimum any of the selected technologies / services have a moderate chance of a cyber-attack happening with serious impacts requiring mitigation. The following sections describe the technologies, their vulnerability to cyber-attacks, and how these might be mitigated.

Table 1: Risk level definition

Risk level	Definition
Low	Unlikely to occur with negligible impact.
Moderate	Low chance of happening with minor impacts.
Elevated	Moderate chance of happening with serious impacts requiring mitigation but manageable.
High	Highly probably and could occur frequently with major consequences, potentially crippling the organisation or system.
Critical	Almost certain and may occur regularly with catastrophic impact, potentially crippling the organisation or system.

Table 2: Technology classification and risk level[10]

Technology	Classification	Risk level
Cloud Computing & Virtualisation	Established	Elevated
Internet of Things (IoT)	Trending	High
Artificial Intelligence (AI) & Machine Learning (AI/ML)	Trending	Elevated
Remote work & collaboration tools	Established	High
Supply chain & third-party services	Established	Elevated
Biometric & Identity Systems	Trending	Elevated

[10] This classification uses a combination of different cyber risk level classifications, in which likelihood and impact are integrated into a single descriptive category in order to better simplify risk for this study.

Technology	Classification	Risk level
Connected and Autonomous Vehicles (CAV)	Trending	Elevated
Quantum Computing	Emerging	Elevated
Cryptocurrencies & Blockchain	Trending	Elevated

Artificial Intelligence & Machine Learning (AI/ML)

Cybercriminals increasingly use AI for phishing scams, while foreign state actors exploit it for disinformation. Wider AI-driven cyber-attacks are expected as technology matures. The rise of connected and autonomous vehicles (CAVs) will expand vulnerabilities, necessitating stronger cyber security measures.

Cloud Computing & Virtualisation

Key risks include data breaches, account hijacking, shared resource vulnerabilities, and insecure APIs. DoS attacks threaten availability, while regulatory and supply chain risks add complexity. Strong vendor management and security controls are essential.

Supply Chain & Third-Party Services

Third-party breaches, software supply chain attacks, and misconfigurations expose organisations to data theft and operational disruption. Limited visibility and compliance issues increase risk, requiring strict security assessments and zero-trust frameworks.

Biometric & Identity Systems

Biometric data breaches are irreversible, with spoofing attacks and AI biases further compromising security. Centralised storage and poor encryption amplify risks, while regulatory compliance remains a challenge. Multi-factor authentication and robust encryption are essential.

Connected & Autonomous Vehicles (CAVs)

Cyber risks include remote hacking, V2X communication attacks, AI-driven sensor spoofing, and OTA update vulnerabilities. Fleet ransomware and data privacy issues also pose threats. Securing software, encrypted communications, and intrusion detection systems are critical.

Quantum Computing

Quantum threats could break encryption, enabling stolen data to be decrypted later. The slow transition to post-quantum cryptography poses additional risks, requiring urgent investment in quantum-resistant security measures.

Cryptocurrencies & Blockchain

Private key theft, exchange hacks, smart contract vulnerabilities, and '51% attacks'[11]. Regulatory gaps enable illicit transactions, while scalability issues impact performance. Strong encryption and audits are key mitigation strategies.

[11] Source: https://perkinscoie.com/insights/update/blockchain-attacks-and-fight-immutability

Internet of Things (IoT)

IoT networks, a key element of Connected Places, face widespread vulnerabilities due to poor implementation of security updates, weak encryption, and vast attack surfaces. Lack of processing power in devices limits security features, increasing risk exposure.

Remote Work & Collaboration Tools

Phishing, weak authentication, insider threats, and unpatched vulnerabilities make remote work environments high-risk. Without mitigation, frequent incidents could severely impact organisations.

3.4 SUMMARY

In summary, our desktop research identifies a changing cyber threat profile driven by the evolution in technologies:

The current threat landscape:

- The NCSC incident management team received 1,957 reports of cyber-attacks, triaged into 430 incidents requiring support, which is a 15% increase on 2023. 89 were nationally significant and 12 were severe which is a threefold increase on 2023.
- Overall cyber threat is amplified by geopolitical risks from global conflicts.
- Many nation-state threat actors and cyber criminals are already using artificial intelligence (AI) to increase the volume and heighten the impact of cyber-attacks.

Specific emerging threats:

- ICO data shows that for UK local government ransomware remains the most pervasive cyber threat. There is an industry consensus that ransomware attacks are shifting from encryption to data exfiltration extortion (rise of 'infostealers').
- ICO data shows that for UK local government phishing is the second most prevalent cyber threat and is expected to increase in the next few years with the targeted application of AI and use of deep fakes (audio and video).
- There is an increasing proliferation of commodity cyber tools[12] that require low skill to weaponise.
- Cyber Threat Actors are exploiting SOHO[13] (small office / home office) devices to create IoT botnets for DDoS attacks, carry out credential stuffing, firmware exploits and Man in the Middle Attacks.

[12] https://www.ncsc.gov.uk/pdfs/news/cyber-experts-warn-of-rising-threat-from-commercial-hacking-tools-over-the-next-five-years.pdf

[13] https://www.ncsc.gov.uk/pdfs/news/ncsc-and-partners-issue-advice-to-counter-china-linked-campaign-targeting-thousands-of-devices.pdf

Third party system supplier vulnerabilities:

- The rapidly evolving ecosystem and the multitude of cloud providers, each offering dozens of services, terminologies, and security mechanisms, creates complexity that is hard to navigate and increases the risk posture[14].
- Known misconfigurations and poor security practices continue to play a significant role in driving large-scale data breaches, evident in some of the recent local government attacks.
- Cloud and non-cloud integrated (hybrid) infrastructure have become prime targets for cyber-attacks given their potential to facilitate bidirectional lateral movement[15].

[14] https://www.ncsc.gov.uk/collection/cloud/choosing-a-cloud-provider

[15] https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf

The picture can't be displayed.

LOCAL COUNCIL DIGITAL INITIATIVES

4 LOCAL GOVERNMENT DIGITAL INITIATIVES

This section provides an overview of local councils' engagement in CNI sector projects; the specifics of the domains and type of project; the stage of maturity of those projects; and the technologies being used in their delivery.

4.1 OVERVIEW OF LOCAL GOVERNMENT ENGAGEMENT

Out of 30 responding local councils to the survey, 20 (approximately 67%) reported active critical sector projects. While around a third of these 20 respondents mentioned only a single critical sector project, two-thirds had multiple initiatives, ranging from two to eight projects each. There was no apparent relationship between the size or function of a local council and its likelihood of having active critical sector projects. However, given the small sample size, it is not possible to determine or rule out with certainty the existence of such relationships. Further detail about these limitations can be found in section 2.

The interviews also highlighted that the approach within local councils differs as some internal technology teams are not directly involved with the cyber security aspects of some critical sector projects or services. Instead, the central technology (and cyber security) functions have more of an oversight or advisory role (e.g., in procurement) rather than having direct responsibility for ensuring that the projects are secure during implementation.

> "From an IT service point of view from where I sit, we don't really get exposure to that kind of thing [referring to critical sector projects]." **Interview participant 13, Team leader, IT and cyber security**

> "[Systems for] waste management… I don't think we do anything like that, I think it's different departments that cover all of that." **Interview participant 16, Team leader, cyber security**

4.2 SPECIFIC CNI SECTOR DOMAINS

Projects reported by respondents spanned all listed CNI sectors except for Food. Figure 2 shows the spread across the different domains as reported in the survey.

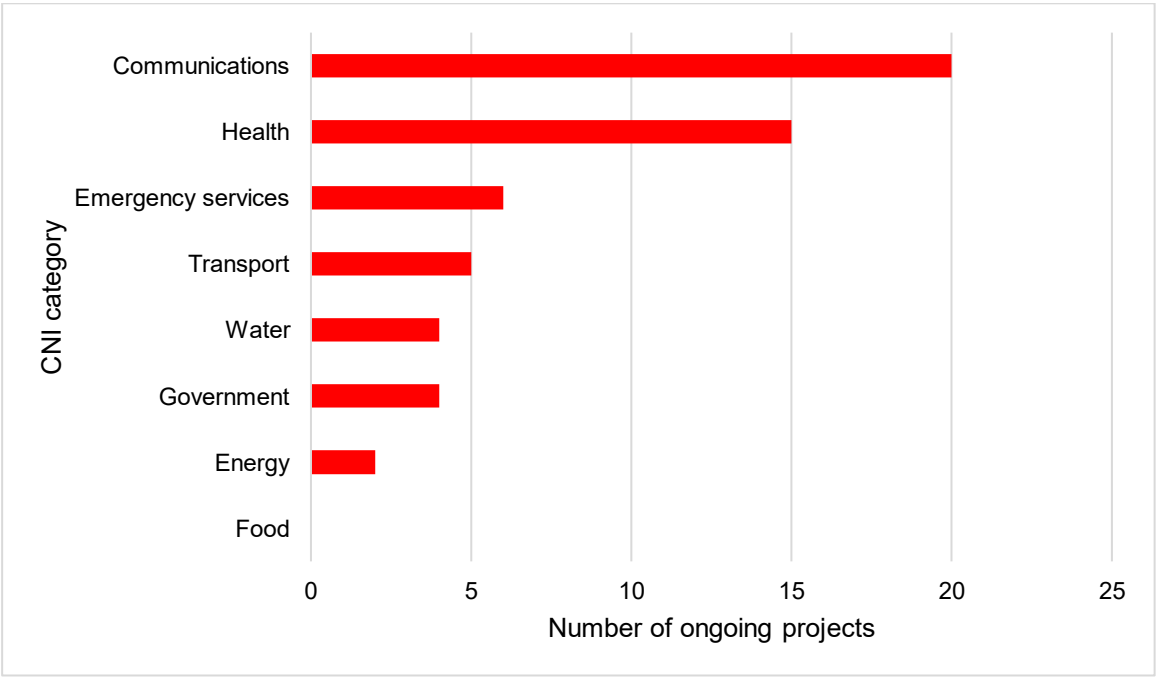


Figure 2: Prevalence of projects across CNI categories (Survey data, n=20)

Further detail gained from the survey and interviews about CNI sector projects is provided below by category.

Communications

From the survey alone, Telecommunications was the most common CNI sector project area with 50% of local councils participating in the survey implementing Wi-Fi initiatives. Additional projects included 5G infrastructure, LoRaWAN networks, and fibre optic connectivity improvements.

Telecommunications was also frequently discussed in the interviews, with participants describing projects in Wi-Fi networks, fibre networks; PSTN (Public Switched Telephone Network) replacement for digital transformation; and open roaming networks for seamless Wi-Fi access.

Health

Health was the second most reported category in the survey, including adult social care. IoT-enabled smart monitoring devices, home telecare systems, and digital healthcare integration initiatives were frequently reported.

Health was also frequently discussed in the interviews, with projects reported in: IoT-based health monitoring systems for vulnerable individuals; Damp and mould sensors in housing; and Telecare services (e.g., lifeline services, red pull cords[16]).

[16] Red pull cords are emergency signalling devices designed to alert caregivers or emergency services, commonly used in assisted living facilities, care homes, and smart-enabled homes for the elderly or vulnerable, and they typically form part of a nurse call or emergency alert system.

Emergency Services

Emergency services (including security) was the third and fourth most recorded domain for the survey and interview participants respectively. In the survey, several local councils reported investment in surveillance and security upgrades, including CCTV expansion, real-time vehicle telematics for fire and rescue services, and data-sharing systems for law enforcement.

The interviewees described projects in: CCTV monitoring (often managed under external contracts); Emergency Services Network (ESN) for secure communication; and cyber security and digital twin programmes for resilience planning.

Transport

Transport was frequently discussed in the interviews, with participants describing a range of digital projects including: AI-controlled traffic lights, road tunnel systems, smart traffic management (Urban Traffic Management Control - UTMC); Mass transit planning (trams, buses, autonomous vehicles); Smart streetlights with central monitoring; and connected vehicle pilots with infrastructure-to-vehicle communication.

In the survey, Transport projects were not as prominent as a topic area compared with other areas. Projects mentioned here included AI-enhanced traffic light systems, autonomous vehicle research, and smart sensor deployment for traffic and tolling.

Energy and environment

Interviewees described a range of projects such as: air quality monitoring using IoT sensors; Waste-to-energy plants; collaboration with third parties on energy infrastructure; Local council involvement in energy efficiency projects. In other instances, there were energy projects authorities were involved with but all responsibilities for associated systems were with third party operators.

In the survey, local councils described implementing renewable energy initiatives, such as a 1MW solar farm, along with smart grid management solutions.

Government

In the survey, local councils reported investments in shared data centres and digital communication platforms to enhance inter-agency collaboration. No interviewees described projects in this area and digital services supporting democratic functions (electoral roll management etc) were not mentioned.

Water

A smaller but notable number of projects from the survey focused on flood monitoring systems (particularly in relation to the interface with the highway), gully water-level IoT sensors, and waste management enhancements. No interviewees described projects in this area.

Food

No digital projects were reported in this sector in the survey or the interviews.

4.3 PROJECT LIFECYCLE AND STATUS (SURVEY)

Figure 3 provides the critical project lifecycle stage information collected from the survey data. This provides insight into the wider maturity of specific digital projects being deployed:

- **Scoping/Pre-proof of concept**: 2 (4%) reported projects are in discovery phases
- **Proof of concept**: 11 (20%) projects remain in the early validation phase
- **Pilot phase**: 8 (14%) projects are currently in pilot stages
- **Being rolled out**: 2 (4%) projects are in deployment but not yet operational
- **Operational service**: 30 (54%) projects are fully functional and in service

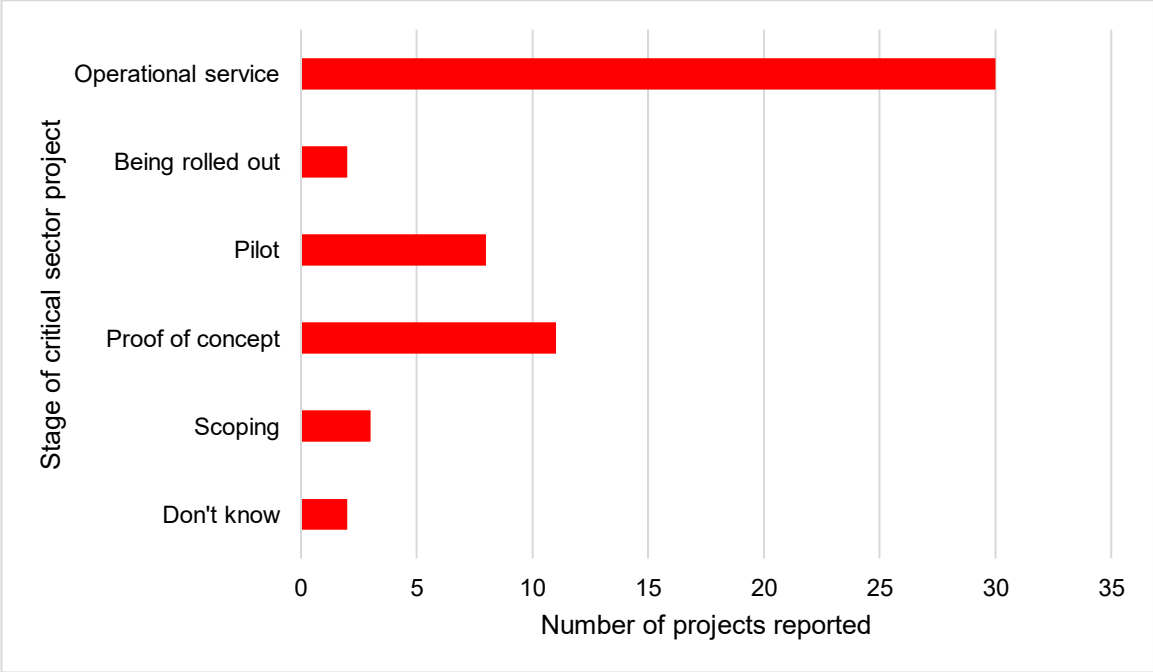


Figure 3: Lifecycle stages of critical sector projects referenced (Survey data, n=20)

Table 3 cross tabulates the information in Figure 2 and Figure 3 to show the prevalence of specific combinations of critical sector projects' sector and lifecycle stage. Table 3 shows that the most prominent combination is Communications projects which are operational. These were most commonly wi-fi services hosted by the local council. Some Communications projects were also being piloted. Health-related projects were also most commonly already being delivered by the local council, while some were in the proof of concept stage.

Table 3: Lifecycle stages of sector projects by CNI area (Survey data)

	Scoping	Proof of concept	Pilot	Being rolled out	Operational service	Don't know	Total number reported
Communications	0	2	5	1	12	0	**20**
Health	2	4	1	0	7	1	**15**
Emergency services	0	1	1	1	3	0	**6**
Transport	1	1	0	0	2	1	**5**
Water	0	1	1	0	2	0	**4**
Government	0	1	0	0	3	0	**4**
Energy	0	1	0	0	1	0	**2**
Food	0	0	0	0	0	0	**0**
Total number reported	**3**	**11**	**8**	**2**	**30**	**2**	**56**

4.4 TECHNOLOGIES UTILISED (SURVEY)

Figure 4 provides the frequency of reported technologies used on the projects from the survey data. These were selected by participants from a pre-defined list.

Figure 4 shows that:

- 40 different projects reported using **cloud computing and virtualisation**, which is essential for data storage, scalability, and remote access to services
- 31 different projects included technology relating to **supply chain & third-party services**
- 31 different projects included **IoT & operational technology**, which was used extensively in transport, health, and emergency services
- 13 different projects reported including **AI & machine learning**, which was deployed in smart traffic systems and in predictive maintenance

- Several other technologies were utilised on a smaller number of projects. These included **biometric and identity systems, connected and autonomous vehicles, cryptocurrency and blockchain, and quantum computing**.

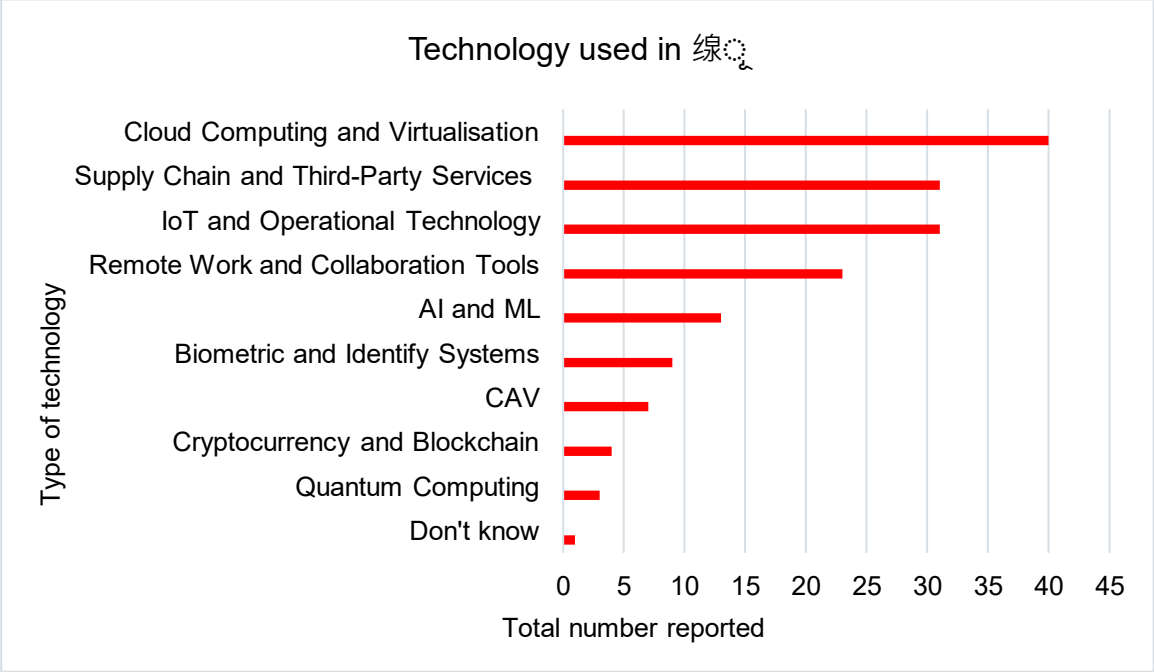


Figure 4: Technologies used on the critical sector projects (Survey data, n=20)

4.5 SUMMARY OF FINDINGS

Based on the responses to the study survey, the digitalisation of critical sector projects was prevalent, with local councils actively deploying smart technologies to enhance public services. While Communications and Health projects lead the transformation, other sectors, including Transport, Emergency services, and Energy, are also experiencing significant digital investment and innovation.

CYBER THREATS AND VULNERABILITIES IN LOCAL GOVERNMENTS' CRITICAL SECTOR DIGITAL PROJECTS

5 CYBER THREATS AND VULNERABILITIES IN LOCAL COUNCILS' CRITICAL SECTOR DIGITAL PROJECTS

The evolving cyber threat landscape presents significant challenges for local councils, with various actors targeting critical infrastructure and services. These actors often exploit vulnerabilities within systems, putting both the security of sensitive data and the continuity of vital services at risk.

This section outlines the primary threats and vulnerabilities facing the local councils we engaged with.

5.1 DENIAL OF SERVICE ATTACKS TARGETING LOCAL COUNCILS

A recurring threat across multiple sectors is the risk of cyber attacks targeting high-profile events and government systems. Cybercriminals frequently target local councils and other public-sector bodies due to their management of sensitive data and critical infrastructure. These organisations are vulnerable to a range of cyber attacks, which can disrupt services, undermine public confidence, and cause significant operational damage. In particular, Denial of Service (DoS) attacks on public-facing websites have emerged as a critical threat, with some websites being inadequately protected by defences such as Web Application Firewalls (WAFs) or anti-distributed DoS (DDoS) measures.

> "We've had denial of service attacks on our websites…a few times last year and the year before we got on a list of a Russian sympathising group who then launched denial of service attacks at… a set of transportation linked websites in the UK and that took one of our transport websites down for a number of times over those periods." **Interview participant 2, Team leader, cyber security**

> "There's all sorts of things going on all of the time… Looking for weakness, looking for access, looking for vulnerabilities is constant, but that's just par for the course." **Interview participant 13, Team leader, IT and cyber security**

One particular threat which did not fit the typical definition of a DDoS attack was also raised by one interview participant. This threat consisted of AI mass producing Freedom of Information requests to place a huge burden on local council personnel, rather than on IT systems (as is the conventional understanding of a DDoS attack).

> "We need to be cognisant of the fact that AI could be used against us… better crafted phishing emails, better crafted Freedom of Information (FOI) requests, which could… [cause] public sector organisations no end of problems because they have to reply to them… So that's why we feel very strongly that the organisation needs to be matured and trained in AI…" **Interview participant 14, Team leader, IT**

5.2 PHISHING ATTACKS

Several local councils highlighted phishing as a significant primary threat, which they were taking active steps to reduce the risk of, and mitigate any damage resulting from, such attacks. This largely involved conducting simulations to identify specific weak users who might need additional training.

> "[P]hishing is obviously the biggest risk, I think, in terms of something bad happening. That's how it's going to come in. We do phishing simulations so we kind of know that users will click on things and they will submit credentials – not loads of users, but enough to make you worry a little bit, and therefore putting technical controls in place to make that less likely that if they do something stupid they [the attacker] can't gain access." **Interview participant 2, Team leader, cyber security**

> "[T]he bulk of the threats still come through malware, through phishing attacks, and increasingly sophisticated ones. So if the tools [referring to AI] can help us to spot those, then that's great. At the moment we run a phishing exercise regularly to understand the sort of things that people are falling for, what level of skills are, and also how quickly that first person will flag it so we can block it." **Interview participant 18, Team leader, IT**

5.3 THIRD PARTY VULNERABILITIES

Local council respondents highlighted concerns regarding the vulnerabilities within the supply chain such as an instance of curtailing projects associated with IoT deployment in the transport domain (e.g., Bluetooth sensors to monitor the volumes of people travelling on certain corridors) due to concerns over third party suppliers of devices cyber maturity.

> "That's the new attack vector at the minute. If you can't get into your main target, you get to somebody who they're working with… the times that we have been compromised have all been through third party. We've never been compromised as such; our third parties have been attacked." **Interview participant 16, Team leader, cyber security**

> "The supply chain is one of the biggest links that we have within the cyber world. All procurements now have set sort of questionnaires that we put in there just to kind of tease out some of the cyber elements, and there's a lot more looking into the contractual stuff around cyber insurance and all that kind of thing." **Interview participant 13, Team leader, IT and cyber security**

5.4 RESOURCES

Another vulnerability highlighted by local councils was insufficient resourcing. While there was confidence in members of staff and existing cyber practices to deal with challenges, local councils typically said they would benefit from more staff resources and expertise.

> "The reality is it's done on best endeavours by my security officers. They are conscientious and professional IT security people who've been in that role for quite a while… they take it very seriously … they've got the alerts and things come through on their phones or through their personal devices to manage mailboxes... So [if] something happens out of hours, they will often just jump in and try and deal with it if they spot suspicious account activity." **Interview participant 14, Team leader, IT**

> "The only thing that it's stopping us from running our own Security Operations Centre (SOC)[17][18] is that we don't know how: it's knowledge, expertise and resource availability. The technical side is all there and it's already done." **Interview participant 15, Team leader, IT**

5.5 USER AWARENESS AND BEHAVIOURS

A small number of respondents raised the issue of many users being unaware of the threats or not acting appropriately, with an increased focus going on continual education measures to improve vigilance:

> "We do phishing simulations so we kind of know that users will click on things and they will submit credentials – not loads of users, but enough to make you worry a little bit, and therefore putting technical controls in place to make that less likely that if they do something stupid they [the attacker] can't gain access." **Interview participant 2, Team leader, cyber security**

> "To be honest, I consider that [email phishing and virus protection] old school stuff. Really, our primary focus is one of education in recent years in terms of ensuring that the user passes through mandatory training... It's just making sure that the users are aware because it's, more often than not it's the user is the weak link and it's, you know, clicking an e-mail which installs a bit of malware or provide your credentials to a site. That kind of stuff which is usually the attack vector 99% of the time in these kind of cases these days. So education has been a huge focus recently." **Interview participant 14, Team leader, IT**

5.6 LACK OF MULTI-FACTOR AUTHENTICATION

The lack of Multi-Factor Authentication (MFA) was highlighted by one interview participant as one area of vulnerability, which had resulted in a previous successful ransomware attack in a number of

[17] A Security Operations Centre (SOC) is a centralised unit where cyber security professionals monitor, detect, and respond to security threats in real-time. It enhances an organisation's threat detection, response, and prevention capabilities. Some local council participants stated that they already use such a service.

[18] The Ministry of Housing, Communities and Local Government (MHCLG) undertook a Security Operations Centre pilot with 10 local councils, to gather evidence and explore how best to support the local government sector with incident detection and monitoring.

schools within the local council's jurisdiction. MFA reduces the risk of security breaches because it requires more than just a password to access an account.

> "One of the things that we knew, we found out from it, is the schools beforehand didn't have MFA enabled, and the attack came from a phishing e-mail." **Interview participant 12, Team leader, IT**

5.7 ACCESS THROUGH REMOTE SENSORS

Most of the local councils interviewed reported using IoT remote sensors on projects in the environment, transport and social care domains. The fact that they represent a vulnerability was mentioned by a number of interviewees.

> "I think though, as people see the value of IoT and sensors… and it becomes more embedded as part of the infrastructure connected infrastructure. Of how we do things in our place, I think that's where the risk is. As people start joining all of this up more, joining up all of these vulnerabilities because they haven't been taught about it from the outset." **Interview participant 21, Team leader, data**

5.8 INCIDENT RESPONSE PREPAREDNESS

The ability to respond to cyber security incidents is another critical area where vulnerabilities exist. A prompt and effective response can minimise the ultimate scale of impact. One local council previously lacked a comprehensive incident response plan that was visible beyond the core security team until they faced a critical incident.

> "… We created a cyber incident response plan which, even as a council, at the time we didn't have. We now have what we consider quite a mature one, and that plan has been shared with the local Resilience Forum." **Interview participant 12, Team leader, IT**

5.9 LACK OF EARLY INVOLVEMENT OF IN-HOUSE CYBER EXPERTISE

A final vulnerability highlighted by local councils was the inhouse cyber security experts being seen as blockers which some colleagues sought to 'work around'. This had established a behavioural trend of the cyber security expertise not being involved in initiatives soon enough to make the biggest difference (i.e. secure by design).

> "But we are, I think, perceived as being...blockers in a lot of cases. And that's not how we want to be... I don't think we have as much visibility of what else is happening in the organisation. And as a result, we probably don't get involved in initiatives quite early enough." **Interview participant 17, Team leader, cyber security**

5.10 CONFIDENCE IN RISK MANAGEMENT

However, many local councils were confident in their cyber security practices and incident response plans, suggesting that while the threats and vulnerabilities listed above were frequently cited, they were often considered to be well managed.

> "from a cyber perspective, we were not particularly worried because the whole thing is quite tight and closed up. The only integration happens in a Demilitarized Zone [DMZ] externally and that is only reachable through a Virtual Private Network [VPN] and has to go through two firewalls, one on our side, one on the other side… There is a particular remediation in place that has been tested, which is that if the whole thing for whatever reason went down, one member of [our] control room would move into the [other organisation's] control room carrying a laptop, connect to Internet in there, open a VPN to our own system, then show them physically on the screen whatever they needed to see." **Interview participant 15, Team leader, IT**

Moreover, some gave examples of when they had shown resilience in the face of cyber attacks:

> "that was hosted by a third party provider; it's not one of our in house ones so we had access to the threat intelligence quite quick. And we have good relationships with NCSC, so we were tipped off by them, but also had third party intelligence to see it was happening… Our telemetry picked it up anyway. So we mitigated that relatively quickly to be honest. It was, I think it was only down for a couple of hours out of the space of a full 24 hour attack... It was a good test if that's [not] an awful thing to say." **Interview participant 13, Team leader, IT and cyber security**

> "We've never been down for a long time through a cyber breach, I can't even think when we've been down longer than like an hour or something like that." **Interview participant 16, Team leader, cyber security**

Others gave examples of how their testing approaches ensured that they found and addressed vulnerabilities promptly:

> "As part of our, kind of, scanning around the risks, we have actually – certainly from our CCTV perspective – had some penetration testing done, it was literally just to try and understand any potential weaknesses that we have… there wasn't any kind of red light, red warning lights for us. There was some things around passwords and password changes and the like… it was very low risk." **Interview participant 10, Team leader, security**

Another described how they were piloting the use of Microsoft Copilot AI on a limited basis to understand the value it could bring the organisation but also whether it might introduce any new vulnerabilities.

> "As I said, the [AI] is quite limited, but it's more about discovery at the moment. The finding out what the art of the possible is. We're very conscious about just not throwing it out into the wild." **Interview participant 13, Team leader, IT and cyber security**

5.11 SUMMARY

Overall, threats to and vulnerabilities within local councils do exist. Indeed, one theme is the failure to adopt security best practices in a timely manner by some organisations who had experiences of only implement critical measures in response to cyber incidents, rather than proactively strengthening their defences beforehand.

This reactive approach increases risk exposure and highlights the need for better preparedness and stronger cyber resilience planning. However, many of the participating local councils do have confidence that they can effectively deal with these threats and vulnerabilities (and have evidenced that they are doing so), acknowledging instead that many of the biggest vulnerabilities relate to the knowledge and practices of wider employees in relation to existing cyber security policies and emerging risks.

5.12 RECOMMENDATIONS

To mitigate risks, organisations must implement comprehensive cyber security strategies that include stronger access controls, enhanced user education, proactive incident response frameworks, and continuous security monitoring. Strengthening resilience and adopting best practices ahead of time will be essential to ensure the safety and continuity of public-sector services in the face of evolving cyber threats. Table 4 below highlights typical interventions that could be implemented to address these concerns:

Table 4: Recommended local interventions to address key vulnerabilities identified

Key area of vulnerability raised	Recommended intervention
Being targeted for denial-of-service attacks	▪ Continuous security monitoring including automation and real-time response mechanisms ▪ Incident response processes in place
Increasingly sophisticated phishing attacks	▪ Continuous security monitoring including automation and real-time response mechanisms Incident response processes in place
Third party supply chain vulnerabilities	▪ Enforced software security update protocols ▪ Cyber security framework including minimal expected standards and compliance checks ▪ Setting expectation at procurement stage
Accessing via IoT Remote Sensors	▪ Enforced software security update protocols ▪ Cyber security framework including minimal expected standards and compliance checks ▪ Setting expectation at procurement stage
Insufficient access to security expertise and resources	▪ Maximise opportunities for automation ▪ Collaboration on shared functions with other authorities

Key area of vulnerability raised	Recommended intervention
User awareness and behaviours	▪ Staff training (onboarding and regular refresher), regularly updated ▪ Behavioural testing (‘dummy’ phishing attempts) ▪ Leadership behaviour setting
Lack of multifactor authentication	▪ Implementation of multi-factor authentication ▪ Cyber security framework including minimal expected standards and compliance checks
Insufficient preparedness for Incident Response	▪ Incident response processes in place ▪ Clear definition of roles including CISO
Insufficient early involvement of in-house cyber expertise in new digital projects	▪ Cyber security framework including minimal expected standards and compliance checks ▪ Leadership behaviour setting

CYBER SECURITY MATURITY AND CHALLENGES IN LOCAL COUNCILS

6 CYBER SECURITY MATURITY AND CHALLENGES IN LOCAL COUNCILS

This section summarises the survey and interview respondent feedback pertaining to the cyber practice and maturity in their local councils.

6.1 CYBER MATURITY

Cyber-risk maturity is crucial for organisations because it provides a strong indicator of their proactivity to limit threats and preparedness for dealing with the impacts if an attack is successful. Strong maturity levels give confidence to stakeholders and minimises the risk and costs of impacts to staff and citizens.

The maturity ratings applied in this study are based on a very limited question set (22 questions out of a potential 133 questions[19]) from the Human Affected Cyber Security Framework (HACS)[20]. These 22 questions were considered to be the most relevant questions to ask while trying to maintain the survey's brevity. This reliability tested and validated questionnaire can be mapped onto maturity levels represented by the acronym GRADE, named by taking the first letter from each maturity level. Answers from respondents were then mapped to the maturity levels described in Table 5.

Table 5: GRADE – human related cyber security maturity

Growing	Basic awareness of cyber threats exists but understanding and practices are inconsistent. Cyber security is not yet embedded in daily behaviour.
Reactive	Users respond to incidents as they occur but lack proactive habits or training. Security behaviour is driven by events rather than awareness.
Alert	Users have a moderate understanding of threats and exhibit cautious behaviour. Regular training exists, and individuals are beginning to recognize and report suspicious activity
Developed	Cyber security is integrated into routine practices. Staff are regularly trained, aware of threats, and contribute to organizational security by following good practices and reporting risks.

[19] Questions 2, 3, 5, 7, 9a, 10a, 10c, 15, 21, 22, 25, 29, 30, 34, 44, 50, 52, 59a-c, 66, 73

[20] Humans and Cyber Security – How organisations can enhance resilience through human factors. Amanda Widdowson. CRC Press 2025.

Enhanced	Security-conscious culture is well-established. Individuals act as proactive defenders, often promoting best practices, participating in simulations, and helping to improve overall cyber resilience.

Due to the limited number of questions used, the evidence provides only a broad suggestion of maturity level, which is nevertheless useful for illustrating the range in maturity across those local councils who responded.

GENERAL CYBER MATURITY

Out of a total of 18 local councils, four were scored as 'alert' (receiving a three out of five), eight as 'developed' (receiving four out of five), and six receiving 'enhanced' (receiving five out of five). No authorities received a lower categorisation than 'alert', indicating that there is clearly a moderate level of knowledge across local councils. Moreover, at least six local councils interviewed stated that they already sub-contract or are trialling the use of a Security Operations Centre.

However, alongside good practice, interview data also identified several key gaps in common cyber practice. These will be explored further below.

CYBER MATURITY SPECIFIC TO CRITICAL SECTOR PROJECTS

Survey data showed that while all respondents have cyber security policies, only one had cyber security policies for specific critical sector projects. Similarly, all but one survey respondent said that they had physical security measures in relation to critical sector projects, but not all said that these measures were often or always enforced (around a quarter did not).

6.2 CYBER PRACTICE SPECIFICS

INCIDENT EXPOSURE, RESPONSE AND COMMUNICATION

Several local councils reported being affected by denial-of-service (DoS) attacks. One attack detailed (see Section 2) had disrupted critical services, particularly those linked to transportation.

Despite common incidents such as these, some local councils demonstrated a lack of robust DDoS mitigation strategies, highlighting weaknesses in resilience against persistent threats. Additionally, the reliance on visibility rather than response capability suggests that while attacks are detected, the ability to effectively counteract could be improved.

All but one of the survey respondents indicated that they share cyber security incidents with their Local council Board and relevant external organisations. However, interview data suggests that leadership engagement in such incidents remains focused on major breaches, while minor incidents receive little attention to prevent senior leaders from being overloaded with information:

> "We have a structured process where the Gold Team, which consists of senior leadership, is only notified of major incidents. This prevents them from becoming overwhelmed with minor issues" **Interview participant 1, Team leader, incident management**

BOARD LEVEL REPRESENTATION

While ten of the 18 survey respondents who were conducting critical sector projects stated that their Chief Information Security Officer (CISO) had either a high or very high level of influence, five did not have a CISO position or equivalent role at all.

REACTIVE NOT PROACTIVE PRACTICE

A small number of local councils reported a largely reactive approach to cyber security, responding to incidents rather than using proactive threat intelligence to inform their practice. This reactive stance is illustrated by an example outlined above of a successful ransomware attack in a number of primary and secondary schools within one local council's jurisdiction which resulted from the delayed implementation of Multi-Factor Authentication (MFA):

> "One of the things that we found out is the schools beforehand didn't have MFA enabled, and the attack came from a phishing e-mail. Immediately after they moved 90% of their systems …to the cloud, they ran MFA... they listened to the advice they were given by NCSC cybercrime [team] and the cyber team within Department for Education as they rebuilt their structure for themselves and the primary schools" **Interview participant 12, Team leader, IT**

Risk discussions in these reactive local councils occur on a scheduled basis rather than being continuously assessed at moments that matter. Moreover, while over half of the survey respondents said that their organisation completes risk assessments, only a third of these repeat risk assessments once recommendations have been implemented.

THIRD PARTY EXPOSURE

Susceptibility to attack also exists in the supply chain for critical sector projects. Over half of survey respondents did not know whether their local council provided advice/training to their supply chain about cyber security regulations or guidance in relation to specific critical sector projects. Moreover, a quarter of survey respondents not regularly include cyber security requirements at all in contractor or supplier contracts.

However, evidence from the interviews does suggest that most local councils recognise the risk that supply chains have to their critical sector projects and do undertake due diligence before working with suppliers as far as possible:

> "We would make sure that our third parties are also up to that same level [as us]. We'll start to bring everything more aligned. It does make things a bit more difficult because not everybody wants to be Cyber Essentials certified or they can't afford [to be] or they think it's a waste of money." **Interview participant 16, Team leader, cyber security**

This includes looking for ISO certification:

> "Most of the questions on the due diligence are going to be not mandatory if they can present a certain number of security certifications that are relevant for the system that we are subcontracting. So it's basically a shortcut. If you [the supplier] can show that you're using the ISO 27001 in one of your services, this block [of questions] is not relevant." **Interview participant 15, Team leader, IT**

It also includes supporting others within the local council with procurement advice, assurance and supplier management:

> "when somebody buys an IT system or goes out to market for one, I supply them with… my cloud services template statement of requirements, which includes sections on … security, accessibility, all that kind of functionality, compatibility with our systems performance, operational, all that stuff. So, the security section is quite extensive." **Interview participant 19, Team leader, cyber security**

> "On the whole, we're able to work through with those third parties and get things resolved and we're very good at that. To be fair, I think we… have held them to account on a number of times and we're very good picking up with third parties where they've dropped the ball somewhere… we get much more involved in supplier management, supplier relationship management and contract management than we ever used to" **Interview participant 14, Team leader, IT**

OVERCONFIDENT RELIANCE ON EXTERNAL ENTITIES

One local council had a dependency on its cloud provider, assuming that only nation-state actors, or another significant actor (such as a powerful cybercriminal group, hacktivist collective, or similar entity) would have the ability to amount an attack that could significantly impact that infrastructure.

> "All of our infrastructure is based in [Microsoft] Azure. So you know, it'd have to be probably a significant actor or nation-state to really be able to affect Microsoft." **Interview participant 4, Team member, cyber security**

Greater reliance on external entities often emerged from the respondents who had more limited internal resource. Three quarters of survey respondents did not agree that their local council had enough competent personnel for critical sector projects.

> "I think the biggest issue we have is resources and therefore being able to do anything here requires resource… as I've said, I'm the only cyber security person in the organisation." **Interview participant 2, Team leader, cyber security**

> "If money was no object, we'd have far better tools and a far bigger security service than we currently have. I mean, I've just had approval to increase it to a third person in my organisation, so we'll have three IT security officers from April onwards. But even that in an organisation of 6,000 people, in my opinion, isn't enough" **Interview participant 14, Team leader, IT**

CONSISTENCY OF THREAT MONITORING

While the majority of survey respondents said that they do monitor system anomalies, this is not undertaken consistently all of the time at their local council.

USER AWARENESS AND BEHAVIOUR

While all but one survey respondent said that their critical sector projects had policies to mitigate issues like email based phishing risks and using unauthorised software, the in-depth interviews indicated that user awareness training requires ongoing consistent efforts to meaningfully reduce the risk of cyber attacks:

> "We have to do work to educate and remind people that if they are going to consume any new service, they need to make us aware so we can help them with it. I guess that's been a journey… to raise that awareness and get more and more people to do these things, but we do analyse what's being used on our network." **Interview participant 18, Team leader, IT**

LACK OF AUTOMATION AND REAL-TIME RESPONSE

Through the interview responses it was evident that there is minimal emphasis on automation in cyber incident response e.g. an absence of Security Orchestration, Automation, and Response (SOAR) technologies or similar automated mechanisms. This suggests inefficiencies in handling large-scale incidents. Instead, reliance on static playbooks limits the ability to detect and respond to threats in real-time, ultimately weakening overall cyber resilience.

> "So, we've got a lot of playbooks that run through what you do with an on-premises system or compromise an on-premises system, but not so many to do with the cloud services. And as we make that shift from on-premises to cloud, I think they [the playbooks] could bear some updates there, particularly with the use of the things like [Microsoft] 365 services, [we have] a reliance on those." **Interview participant 19, Team leader, cyber security**

6.3 SUMMARY OF FINDINGS

Survey and interview data provided evidence for a relatively high level of cyber maturity across local councils, with evidence of good practice. However, several key gaps in common cyber practice emerged. A reactive approach to cyber threats rather than a proactive strategy in some authorities was clear. Specifically, key gaps emerged in areas such as incidents exposure and response, Board level representation, susceptibility to attacks, misplaced reliance on external entities, threat monitoring, user awareness and behaviour, and automation and real-time response.

6.4 RECOMMENDATIONS FOR IMPROVEMENT TO CYBER PRACTICE AND MATURITY

Based on the findings, key areas of action to encourage at a local level which would drive improvement in cyber practice and maturity within local government organisations include:

- **Stronger Leadership Engagement**: Ensuring decision-makers are involved in all levels of cyber incident management, not just major breaches. Virtual CISOs, who can be an external, part time security executive to offer leadership without the cost implications of a full-time role could be a useful option.
- **Proactive Threat Intelligence and Risk Management:** Implementing early warning mechanisms and continuous risk assessment to anticipate threats rather than responding after incidents occur.
- **Resilient Cyber Defences:** Enhancing capabilities to prevent and mitigate DDoS attacks, phishing, and other cyber threats.
- **Internal Capacity Building:** Reducing reliance on external organisations by strengthening internal expertise and resources.
- **Automation and Real-Time Response Mechanisms**: Integrating automated security responses to improve detection and mitigation speed.

The picture can't be displayed.

EXISTING AND FUTURE CYBER SECURITY GUIDANCE AND SUPPORT

7 EXISTING AND FUTURE CYBER SECURITY GUIDANCE AND SUPPORT

This section provides a summary of the findings about the guidance currently used by participating local councils and their views on any specific further guidance and/or support that would be useful to help them manage the cyber risks of their Critical National Infrastructure digital portfolios in the future.

7.1 USE OF AND ATTITUDE TO CURRENT GUIDANCE

The majority of participating local councils actively refer to at least one form of cyber security guidance, with over half from the survey and interviews utilising multiple sources. Among the most widely referenced were:

- NCSC guidance
- International Organisation of Standardisation (ISO) 27001
- NCSC's Cyber Assessment Framework (CAF)
- Public Services Network (PSN) Code of Connection

In addition to frameworks such as Cyber Essentials, the National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standard (PCI-DSS), references were also made to government departments like the Ministry of Housing, Communities and Local Government (MHCLG), and initiatives like Health and Social Care Network (HSCN). This highlights the diverse approaches taken across local councils and the wide array of sector-specific guidance issued by central government bodies and professional associations.

30% of respondents to the survey expressed no need for additional support, indicating satisfaction with existing resources. However, another 30% of survey respondents did ask for further general guidance, while the remaining 40% outlined specific requests. This spread of opinion was also reflected in the interviews.

Despite this engagement with guidance, the effectiveness of current frameworks, respondents describe that its use remains inconsistent, with gaps in enforcement and practical application. The following sections provide more detail about these findings.

7.2 THE NEED FOR CONSISTENCY

While existing guidance provides a foundation, its voluntary nature and varied enforcement have resulted in inconsistencies in application between local councils.

> "NCSC's CAF is an important step in ensuring cyber security is at the forefront of CNI project delivery, but its execution is still somewhat vague. It needs to provide more tangible targets in line with the NIST Cyber Security Framework. Encryption standards such as FIPS 140-3 should be mandatory." **Survey respondent 15**

One interviewee explained:

> "It would be helpful to have some guidelines… along the lines of the old Public Services Network (PSN) or Government Data Network (GDN) … that did define processes, policies and the requirements that you had to follow to be in a compliant state." **Interview participant 17, Team leader, cyber security**

In a similar vein, one local council (Interview Participant 16) highlighted that they had experienced the NCSC Cyber Essentials certification differently each time they had completed it, depending on the understanding of the assessor, and requested a more standardised approach with how this was delivered.

7.3 STREAMLINING

Local councils identified that there are multiple assurance mechanisms, and that while each has their own specific strengths, benefit could be gained from some consolidation. One authority thought that the CAF ought to be the sole approach:

> "Use CAF to replace all the other assurance mechanisms that you have to follow… it should be one recognised approach that everybody uses and therefore you'd have … a consistent level of trust and we don't have to spend resources … on adhering to multiple standards, improving our security in multiple ways when we could just do it once." **Interview participant 18, Team leader, IT**

In addition, local councils report that different central government departments have requested information in different ways, and at different levels, even when using the same framework:

> "We're kind of saying 'one CAF to rule them all' … just 'one framework to rule them all'…There'll be a central government version, there'll be an NCSC version – it was the original – then the NHS will do their own spin on it... So I think there needs to be a merge [consolidation]." **Interview participant 13, Team leader, IT and cyber security**

> "… different departments and different legal entities across the government make different requirements for [local councils] in terms of reporting back. 'What are you doing in terms of cyber security?' which is perfectly sensible and reasonable… and thankfully they're all asking the same, which is NCSC CAF, which is great. The problem… is that they are… asking at the different levels and for different scopes. So we're going to be… telling the same thing to ten different people at different points in time. That puts the burden on the teams running those governance and controls… So some consolidation would be well received." **Interview participant 15, Team leader, IT**

Similarly, one local council stated that they felt it was a poor use of resources for multiple local councils to be each assessing the cyber security of their supply chains in cases where multiple local councils use the same supplier. They shared their view that this was something which could be more efficiently done centralised and done to a higher standard:

> "Why are we all trying to assess their [suppliers] cyber security maturity as individual authorities. Why are we doing it 400 times? That's the kind of thing could be done to a better level once nationally, and then effectively offering an accreditation, [as] a confidence level that allows you to then assess your own deployment or your integrations … rather than looking at the whole thing. I think there's definitely … supply chain assurance that could be done in a more joined up way." **Interview participant 18, Team leader, IT**

7.4 THE IMPACT OF NATIONAL GOVERNMENT CHANGES

One local council highlighted that around the time of any change in national government, there can be confusion as to whether existing guidance still applies:

> "[For accessing guidance] the change of government… can be sometimes problematic. Now the problem is you tend to find if you go and look at a set of standards on uk.gov, it's usually 'has it been superseded?' It's usually a big old thing at the top of the page that goes 'this was done under [previous] government' and you're [wondering] so is it valid or not anymore? … we're having to wait for a lot of that information… but I don't think that's a particularly big risk or a huge issue" **Interview participant 14, Team leader, IT**

I

7.5 GUIDANCE FOR EMERGING RISKS

There was a request for greater guidance on emerging risks, such as quantum computing:

> "..., quantum computing needs to be tackled now before it becomes a problem. the standards need to be in place so that we're applying those to current security standards, so that by [bad actors] hoarding this stuff [data] it won't make a difference later on." **Interview participant 6, Team leader, security**

However, it was also recognised that guidance on some areas of emerging risks have been usefully covered:

> "…they've done a really good job, DSIT, commissioning the report on AI usage. And that's evolved into those principal documents. I think there was a really good report… on the AI readiness of the UK Government" **Interview participant 14, Team leader, IT**

7.6 OTHER SUPPORT MECHANISMS

EXPERT RESOURCE

The request for a structured, accessible support team was highlighted by one survey participant, expressing the need for expert guidance beyond written documentation.

In the interviews, this desire was particularly noted for local councils without existing Security Operations Centres, who said that they would benefit from this additional capability:

> "… we're looking at security operations centres at the moment and I know the National Health Service has an NHS SOC. I think a Local Government SOC has been a requirement for a long time, so …anything to push towards that, that would be great" **Interview participant 8, Advisor, security**

SPECIFIC TECHNICAL INFRASTRUCTURE SUPPORT

One example of specific technical support was a request for a centrally managed network infrastructure for IoT and remote-sensing devices, accessible via regional gateways. This was proposed to enhance security and streamline access management:

> "A centrally managed network infrastructure [would be helpful] for IoT/remote sensing devices, accessible via regional gateways; on-site devices connecting using Internet Protocol Security IPSEC or similar encrypted communications - importantly this communication channel should be available on a short lease, compared to the 12,24- or 36-Month contracts available from existing national providers." **Survey respondent 14**

FINANCIAL RESOURCE

In terms of funding and resources, participants simply requested more of it. For example:

> "... but funding is tight, funding is really, really tight... And there are compromises that we have to make. So these kind[s] of decent grants that are being made available, we need more of that." **Interview participant 6, Team leader, security**

INSURANCE

One interviewee highlighted wider sector discussions about a need for centrally-organised insurance arrangements for local councils to participate in, given the severe negative financial implications that can arise from a cyberattack:

> "there should be insurance options .. for councils with regard to cyber threats. ..A cyber incident is an extremely costly process to recover from, especially around critical national infrastructure… that's resulted in some lobbying by senior local council leaders to government to actually put in place some kind of insurance arrangements that that councils could sign up for and pay for. That would give some sort of financial safety net… that's something that I know is being lobbied for quite heavily and something I would support" **Interview participant 14, Team leader, IT**

7.7 SUMMARY OF FINDINGS

The majority of local councils actively refer to at least one form of cyber security guidance, with over half of survey respondents stating that they utilise multiple sources. Despite this engagement with guidance, the effectiveness of current frameworks remains inconsistent, with gaps in enforcement and practical application. Specific requests for further support ranged from structured best-practice

case studies to detailed architectural patterns for secure remote access and IoT integrations. There were also calls for government intervention in supplier security ratings, funding for cyber security initiatives and insurance, and greater direction on emerging threats. Additionally, suggestions were made for a more distributed, resilient approach to data centres in the UK.

7.8 RECOMMENDATIONS FOR GUIDANCE AND SUPPORT

Ultimately, while current cyber security guidance is in use, inconsistencies in enforcement and applicability hinder its effectiveness. By consolidating guidance, enhancing standardisation, funding, procurement strategies, and real-time support, DSIT can play a crucial role in ensuring local government cyber security is both resilient and future-ready.

Specifically, Central Government could consider several targeted actions:

CONSISTENCY AND STREAMLINING

- Implement a mandatory cyber security baseline for local councils, ensuring consistency across the sector. Current frameworks such as the NCSC CAF should incorporate clearer, tangible targets, aligned with established international standards such as NIST's Cyber security Framework and encryption standards like FIPS 140-3.
- Provide clarity about what guidance remains current when there is a change of Government.
- Strengthen procurement frameworks to provide consistency and leverage economies of scale.
- Future-Proofing Against Emerging Threats: Provide strategic direction on emerging risks such as quantum-resistant cryptography and evolving security threats to ensure local councils remain ahead of adversaries as mentioned in the interviews.

OTHER SUPPORT MECHANISMS

- Consider supporting enhanced collaboration between local councils, through shared training resources, security standards, and procurement frameworks, could reduce duplication and improve cyber resilience across the sector.
- Funding and Insurance: Introduce flexible funding mechanisms that align with local council budget cycles and consider the provision of specific insurance.
- Security Operations Centres (SOC) for Local Government: Expand SOC capabilities to provide continuous monitoring and rapid incident response, mirroring successful models used in the NHS as mentioned in the interviews

The picture can't be displayed.

SUMMARY AND CONCLUSIONS

8 SUMMARY AND CONCLUSIONS

In summary, we reflect below on the five original research questions with the key findings explored in previous sections. Finally, we conclude by summarising the suggested recommendations for improvements which can be led at local government level and those which may require Central Government to enable.

8.1 Q1 WHAT ARE THE CURRENT GLOBAL CYBER RISK TRENDS?

Within the UK, the NCSC incident management team received a 15% increase in reports of cyber attacks requiring support in 2024 compared to 2023. Of these, 89 were nationally significant and 12 were severe which is a threefold increase on 2023.

The overall cyber threat is amplified by geopolitical risks from global conflicts. This has been evident in the study as an impact on some local councils who have appeared on targeted lists for disruption.

Emerging threats include:

- Many nation-state threat actors and cyber criminals are already using artificial intelligence (AI) to increase the volume and heighten the impact of cyber attacks.
- Ransomware remains the most pervasive cyber threats to UK organisations, but this is shifting from encryption to data exfiltration extortion (rise of ‘infostealers’).
- Phishing is the second most prevalent current cyber threat and is expected to increase in the next few years with the targeted application of AI and use of deep fakes (audio and video).
- There is an increasing proliferation of commodity cyber tools that require low technical skills to weaponise.
- Cyber Threat Actors are exploiting SOHO (Small Office/Home Office) devices to create IoT botnets for DDoS attacks, to carry out credential stuffing, exploiting firmware and Man in the Middle Attacks.
- An increasing area of vulnerability is with third party system suppliers.
- The rapidly evolving ecosystem and the multitude of cloud providers, each offering dozens of services, terminologies, and security mechanisms, creates complexity that is hard to navigate and increases the risk posture.
- Known misconfigurations and poor security practices continue to play a significant role in driving large-scale data breaches.
- Cloud and non-cloud integrated (hybrid) infrastructure have become prime targets for cyber attacks given their potential to exploit any vulnerability to facilitate bidirectional lateral movement.

8.2 Q2 WHAT KINDS OF CNI SECTOR DIGITAL PROJECTS ARE LOCAL COUNCILS UNDERTAKING?

Based on the responses to the study survey, the digitalisation of CNI sectors was prevalent, with local councils actively deploying smart technologies to enhance public services in the selected areas, chosen for their relevance to LAs. While Communications and Health projects led the transformation, other sectors, including Transport, Emergency services, and Energy, are also experiencing significant digital investment and innovation. The only critical area not reportedly touched on in an example by respondents was Food.

Key areas of digital projects/services raised were:

- Communications: WiFi, 5G infrastructure, fibre cabling improvements.
- Health: IOT devices for adult social care home telecare and monitoring; and for damp monitoring in housing stock.
- Emergency services: vehicle telematics for fire and rescue services, data sharing with law enforcement, CCTV (security and surveillance), Emergency Services Network for secure communications, digital emergency resilience planning.
- Transport: urban traffic management control (sometimes including AI), smart street light management systems, autonomous and connected vehicle pilots, AI for predictive road maintenance, road tunnel systems, people movement sensors (Bluetooth) etc.
- Energy and environmental: systems managing waste-to-energy plants, IoT air quality monitoring sensors.
- Government (inter-agency digital platforms).
- Water: IoT flood and drainage monitoring sensors.

The four most prevalent technology types mentioned in survey responses were use of Cloud Computing services; use of IoT devices; use of third-party services; and AI or Machine Learning.

8.3 Q3 WHAT ARE THE CYBER THREATS AND VULNERABILITIES TO WHICH LOCAL COUNCILS ARE EXPOSED IN THESE CNI AREA PROJECTS?

Overall, threats to and vulnerabilities within local councils and their CNI sector services and projects do exist and are broadly representative of the threats experienced by the wider public and private sector organisations (as identified in the desktop review). The study notes examples from participants that highlighted a failure to adopt security best practices in a timely manner. In some of these incidents, the local councils only implemented critical measures in response to cyber incidents, rather than proactively strengthening their defences beforehand. This reactive approach increases risk exposure and highlights the need for better preparedness and stronger cyber resilience planning.

Many of the local council participants had a good level of confidence that they can effectively deal with these threats and vulnerabilities (and have evidenced that they are doing so), acknowledging

instead that many of the biggest vulnerabilities relate to the knowledge and practices of employees and third parties in relation to existing cyber security policies and emerging risks.

The key areas of vulnerabilities raised were:

- Being targeted for denial-of-service attacks
- Increasingly sophisticated phishing attacks
- Third party supply chain vulnerabilities
- Insufficient access to security expertise and resources
- User awareness and behaviours
- Lack of multifactor authentication
- Accessing via IoT Remote Sensors
- Insufficient preparedness for Incident Response
- Insufficient early involvement of in-house cyber expertise in new digital projects

8.4 Q4 WHAT ARE THE GAPS IN CYBER PRACTICE AND MATURITY EXHIBITED BY THESE LOCAL COUNCILS?

Survey and interview data provided evidence for a relatively high level of cyber maturity across local councils, with evidence of good practice. However, several key gaps in common cyber practice emerged. A reactive approach to cyber threats rather than a proactive strategy in some authorities was clear. Specifically, key gaps emerged in areas such as incidents exposure and response, board level representation, susceptibility to attacks, misplaced reliance on external entities, threat monitoring, user awareness and behaviour, and automation and real-time response.

8.5 Q5 WHAT GUIDANCE AND/OR REGULATION DO LOCAL COUNCILS CURRENTLY USE FOR THEIR CNI AREA PROJECTS AND SERVICES, AND WHAT ADDITIONAL GUIDANCE, REGULATION OR SUPPORT MIGHT THEY NEED?

The majority of local councils actively refer to at least one form of cyber security guidance, with over half utilising multiple sources. Despite this engagement with guidance, the effectiveness of current frameworks remains inconsistent, with gaps in enforcement and practical application.

Specific requests for further support ranged from structured best-practice case studies to detailed architectural patterns for secure remote access and IoT integrations. There were also calls for government intervention in supplier security ratings, funding for cyber security initiatives and insurance, and greater direction on emerging threats. Additionally, suggestions were made for a more distributed, resilient approach to data centres in the UK.

8.6 RECOMMENDATIONS

LOCAL IMPROVEMENTS TO CYBER PRACTICE AND MATURITY

Key areas of action to encourage at a local level which would drive improvement in cyber practice and maturity within local government organisations include:

- Stronger Leadership Engagement: Ensuring decision-makers are involved in all levels of cyber incident management, not just major breaches. Virtual CISOs, who can be an external, part time security executive to offer leadership without the cost implications of a full-time role could be a useful option.
- Proactive Threat Intelligence and Risk Management: Implementing early warning mechanisms and continuous risk assessment to anticipate threats rather than responding after incidents occur.
- Resilient Cyber Defences: Enhancing capabilities to prevent and mitigate DDoS attacks, phishing, and other cyber threats.
- Internal Capacity Building: Reducing reliance on external organisations by strengthening internal expertise and resources.
- Automation and Real-Time Response Mechanisms: Integrating automated security responses to improve detection and mitigation speed.

To mitigate risks, organisations must implement comprehensive cyber security strategies that include stronger access controls, enhanced user education, proactive incident response frameworks, and continuous security monitoring. Strengthening resilience and adopting best practices ahead of time will be essential to ensure the safety and continuity of public-sector services in the face of evolving cyber threats.

OPPORTUNITIES FOR GOVERNMENT TO DRIVE IMPROVEMENTS

Ultimately, while current cyber security guidance is in use, inconsistencies in enforcement and applicability hinder its effectiveness. By consolidating guidance, enhancing standardisation, funding, procurement strategies, and real-time support, DSIT can play a crucial role in ensuring local government cyber security is both resilient and future-ready.

<u>CONSISTENCY AND STREAMLINING</u>

- Implement a mandatory cyber security baseline for local councils, ensuring consistency across the sector, removing some of the ‘noise’ of multiple sets of guidance from different government departments.
- Streamlining expectations of reporting by local government bodies back to Central Government to minimise requests from different departments for similar or function specific information.
- Current frameworks such as the NCSC CAF should incorporate clearer, tangible targets, aligned with established international standards such as NIST’s Cyber security Framework and encryption standards like FIPS 140-3.
- Provide clarity and continuity about guidance during changes of Government

- Strengthen procurement frameworks to provide consistency and leverage economies of scale.
- Future-proofing current and legacy systems against emerging threats: Provide strategic direction on emerging risks such as quantum-resistant cryptography and evolving security threats to ensure local councils remain ahead of adversaries as mentioned in the interviews.

OTHER SUPPORT MECHANISMS

- Consider supporting enhanced collaboration between local councils through shared training resources, security standards, and procurement frameworks, this could reduce duplication and improve cyber resilience across the sector.
- Funding and Insurance: Introduce flexible funding mechanisms that align with local council budget cycles and consider the provision of specific insurance.
- Monitor and support the Ministry of Housing, Communities and Local Government (MHCLG) Digital trial where 10 authorities are sharing a joint SOC support service into a shared Security Operations Centres (SOC) for Local Government with a view to expanding successful SOC capabilities to provide continuous monitoring and rapid incident response, mirroring successful models used in the NHS as mentioned in the interviews.

ANNEX A: CASE STUDIES

The following five case studies are based on composites of different local councils who participated in this study (see section 2 for more detail). Each case study reflects the status and maturity of an authority along with a pressing challenge that they are presented with. These aim to provide an understanding of what mitigation mechanisms, if any, are in place to prepare similar authorities to deal with potential cyber risks and vulnerabilities that may arise as a direct or indirect result of their technology investments.

These case studies are:

1. The cautious authority
2. Worried about blind-spots
3. Outsourcing cyber capability
4. Barriers with leadership and organisational culture
5. The aspirational authority

CASE STUDY 1: THE CAUTIOUS AUTHORITY

This local council has a mature cyber security culture in comparison to many of its peers, considering the impact of cyber security threats in the delivery of their public services and projects – regardless of their impact on critical national infrastructure. The local council is proactive with considering and managing potential areas of threat, understanding the risks these may pose to service delivery, and they plan to control, transfer or mitigate these.

They have successfully instilled cyber-awareness behaviours throughout the organisation with education programmes for new starters, existing staff and testing user behaviours (mock phishing exercises) to compare the maturity of different teams. Ownership of risks is held and understood in functional areas of the organisation (e.g. Communities, Education, Adult Social Care etc) and are supported by a well-resourced team of cyber security experts. They actively measure their maturity, benchmarking different teams with improvement plans to continually raise the bar.

They have a heightened understanding of risks which is seen by their leadership as a good thing, however this level of understanding means the organisation has become risk averse with undertaking new digital projects and services – retreating from potential sources of danger which is stifling innovation. For example, they have decided to curtail or scale back some connected places pilot projects which used Internet of Things (IoT) technologies, e.g., Bluetooth detection in the transport sector, as they did not have sufficient confidence in the cyber maturity of some of the technology providers involved. These were primarily, but not exclusively Small & Medium Enterprises. Similarly, they have chosen to limit their digital interfaces with partner organisations in the public sector such as NHS Foundation Trusts, which inform the delivery of Adult Social Care services (amongst others) and proactively upskill partner organisations (e.g. use of multi-factor authentication in schools). They have also withdrawn some technology communication services (Wi-Fi serving deprived areas) in part due to the security concerns but primarily because commercial

services were felt to be sufficiently accessible and affordable to citizens that this local council no longer needed to supplement the gap in provision.

The local council recognises that this cautious approach may be limiting the ability to innovate with technology pilots and losing out on potential opportunities to improve efficiencies in digital delivery. This could lead to reduced value for citizens in due course if it cannot find the right balance.

Solutions identified by the study's authors to address this include:

- Use of the DSIT guidance - Secure Connected Places Playbook which provides tailored advice to local councils on the cyber security of connected place (smart city) technologies.
- Improved public sector technology procurement standards, which draw on NCSC supply chain cyber security guidance and apply NCSC's supplier assurance questions.
- An accreditation process for compliance with the above standards, so that there is confidence that third party equipment suppliers meet a certain level of performance.
- Apply the Cyber Assessment Framework (CAF) for local government to broader local public sector bodies to help improve confidence with interfaces between bodies, particularly the health sector.
- As an organisation, consideration of cyber risk earlier in the project lifecycle, before any supplier commitments are made and planning for mitigations which do not prevent innovation but do retain good levels of security. This approach is encapsulated in the 'secure by design' principle, ensuring risks are addressed from the outset.

CASE STUDY 2: WORRIED ABOUT BLIND SPOTS

This local council has a dedicated but small team of cyber security expertise as a central function. That team of experts provides guidance and advice where required but they themselves do not have an overview and understanding of all the digital services and projects being undertaken across the local council.

The concept of CNI sectors and how this applied to services and projects delivered by the local council is not well understood.

The local council has a concern that they do not have sufficient capacity within their team of experts to understand the full digital portfolio, the risks within them and what mitigations may be required.

Given these constraints, the authority wants to better understand how they should prioritise their efforts to minimise the potential impacts of any vulnerabilities.

Solutions identified by the study's authors to address this include:

- Ensuring the right approach is present at a leadership level including a designated Chief Information Security Officer, with an understanding of good practice in cyber risk management across all digital endeavours, such that there is a full understanding of the extent of the digital portfolio, with risks and impacts.
- Consider applying the lens of CNI as a tool for prioritising the digital infrastructure to focus on, where the most meaningful impacts will be.

- Embed behaviour change through the organisation to ensure there is consideration of cyber risk early in the project lifecycle and expertise is involved:
    - Training for internal project managers to understand their obligations
    - Procurement processes which mandate involvement of internal experts
- Active collaboration with other local councils for knowledge sharing, best practice and informal benchmarking.
- Once the full scale of support is needed, explore options such as collaborative delivery, use of third parties to address areas of concern and ensure leadership understand any deficits in provision.

CASE STUDY 3: OUTSOURCING CYBER CAPABILITY

This local council has largely outsourced cyber-risk prevention measures to external third parties, particularly in the form of cloud systems and/or Security Operations Centres (SOCs) for monitoring and managing incidents.

The current organisation structure limits the remit of its central information security services function such that is doesn't have full involvement end-to-end remit for the cyber protection of all digital projects and services delivered.

Involvement from the internal information technology team instead predominantly involves providing guidance to parts of the business during procurement about third party/supplier requirements, and/or responding to issues escalated by their SOC.

The concept of critical sectors and how this is applied to services and projects delivered by the local council is not well understood, and there is not a centralised awareness of its maturity and digital risk profile of the organisation at large. For example, while Internet of Things projects have been undertaken by the local council, these have been in collaboration between functional areas with university partners and have had little involvement with the inhouse IT service. Similarly, only after a particular cyber incident in the local council has it been realised that the functional department in question's business continuity plan has not been as comprehensive as it might have been.

In light of this, this local council is not 100% confident that risks are being fully managed by the contracted third parties.

Solutions identified by the study's authors to address this include:

- Implementing common procurement certification standards, particularly for SMEs.
- Strengthening the auditing process of third-party requirements and performance.
- Ensuring that an experienced Chief Information Security Officer is in place.
- Increasing internal accountability and responsibilities to understand where vulnerabilities and weak points lie within the organisation.

CASE STUDY 4: BARRIERS WITH LEADERSHIP AND ORGANISATIONAL CULTURE

In the wider context of service delivery risks and challenges, this local council does not view cyber security threats as posing significant problems. While major cyber incidents are dealt with appropriately, giving them the attention they deserve at levels of senior leadership (in a similar manner to all other types of major incident), minor cyber incidents are treated as relatively insignificant and frequently go unreported.

There is a certain level of complacency in senior management: given the low numbers of major incidents, things are assumed to be working adequately, and therefore there is no need for experienced representation for information technology risk management at the highest levels of leadership.

By not regularly reporting minor incidents to a senior level, potential vulnerabilities are not given their due attention, which could lead to the next major incident which might impact the delivery of Critical National Infrastructure services. This local council needs to know how incidents can be more effectively coordinated and managed across its different departments.

Solutions identified by the study's authors to address this include:

- Ensuring an experienced Chief Information Security Officer is in place.
- Following best practice guidance such as the Local Government Association (LGA)'s 'Building a Cyber Resilient Service: Guidance for Directors of Council Services' document that aims to support council directors in developing proactive strategies to enhance the cyber resilience of their services.
- Increased collaboration with other local councils to enable benchmarking and greater sharing of best practice.
- Auditing the management approach to identify vulnerabilities.

CASE STUDY 5: THE ASPIRATIONAL AUTHORITY

This local council is a visible leader in cyber security practices in the local government sector, valuing its workforce and contributing its expertise through wider guidance and leading collaborative efforts. They are ahead of many of their peers with the technology utilised and the countermeasures implemented, having been using an AI based security system for five years.

They have led engagement efforts with other organisations to learn from those who have experienced cyber attacks; share best practice incident response plans; and work towards implementing a shared SOC. Internally, they regularly run phishing and similar exercises to learn which of their wider employees might need some extra cyber security training.

Despite limited human resourcing in some cases, their staff are knowledgeable and conscientious professionals, who take their roles seriously, keep themselves up to date on emerging risk and trends, and will react to risks, threats, and suspicious activity out of hours. They are aware that their strong cyber performance is heavily dependent on their staff, and so do the best they can to retain their existing workforce by keeping them as skilled as possible.

However, this local council is cognisant that past performance does not reflect tomorrow's risks, and they need guidance on how to best prepare for future threats. Risks identified by the local council include: the use of AI crafting more plausible phishing emails or deepfake impersonations of senior or political leaders. Also of concern is quantum-resistant cryptography, which might lead to more serious data breaches in the future; even if data is merely stolen today, it could be stored and kept for decryption later. Another fear is of the potential for connected and autonomous vehicles to be hijacked and used as weapons.

Solutions identified by the study's authors to address this include:

- Tailored NCSC and DSIT guidance on how to reduce the risk of exposure to bad actors stealing data (which might be secure today but susceptible to being decrypted in the future).
- A government-led cyber insurance scheme, which local councils can pay into and benefit from support during the recovery phase if they do suffer from a cyber attack.

ANNEX B: COMMON ABBREVIATIONS IN THIS REPORT

Abbreviation	Meaning
AI	Artificial Intelligence
APT	Advanced Persistent Threat
API	Application Programming Interface
BCP	Business Continuity Plan
BIA	Business Impact Assessment
BYOD	Bring Your Own Device
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
CCTV	Closed Circuit Television
CTI	Cyber Threat Intelligence
CTR	Cyber Threat Resilience
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DSIT	Department for Science, Innovation and Technology
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
GRC	Governance, Risk, and Compliance
GDPR	General Data Protection Regulation
GDN	Government Data Network
IAM	Identity and Access Management
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IoT	Internet of Things
IPSEC	Internet Protocol Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
LA	Local council
LMS	Learning Management System
MFA	Multi-Factor Authentication
ML	Machine Learning
MSP	Managed Service Provider
NCSC	National Cyber Security Centre
NDA	Non-Disclosure Agreement
NHS	National Health Service
NIS	Network and Information Systems (Regulations)

NIST	National Institute of Standards and Technology
OT	Operational Technology
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PoC	Proof of Concept
PSN	Public Service Network
RBA	Risk-Based Approach
RBAC	Role-Based Access Control
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SaaS	Software as a Service
SIEM	Security Information and Event Management
SME	Subject Matter Expert
SOC	Security Operations Centre
SOP	Standard Operating Procedure
SSL/TLS	Secure Sockets Layer / Transport Layer Security
TPRM	Third-Party Risk Management
TRL	Technology Readiness Level
UEBA	User and Entity Behaviour Analytics
UTMC	Urban Traffic Management Control
VPN	Virtual Private Network

Department for Science, Innovation & Technology

ANNEX C: CNI CYBER SURVEY

CNI Cyber Survey

1. Intro

Local Authority experiences of digital trends and cyber management

A survey from WSP on behalf of the Department for Science, Innovation & Technology (DSIT)

Thank you for agreeing to take part in our survey. It should take you less than 10 minutes to complete.

What is this survey about?

Local authorities are increasingly managing services which full under Critical National Infrastructure (CNI). CNI includes lots of things, from Energy and Water to Communications and Emergency Services.

We are interested to know what local authorities are doing in the CNI space, to ensure that government guidance, support, and legislation is adequately meeting the threat landscape, and the needs of local authorities.

Your data will be protected in line with the privacy notice which was included within the invitation email that contained the link to this survey. If you did not receive this for any reason, please contact here.

1. Please enter your email address so that we can follow up with you if necessary:

2. Critical National Infrastructure Projects

We are interested in ALL of the digital projects you have in a Critical National Infrastructure (CNI) area.

Eight CNI areas are described below with some examples of the kinds of projects we mean.

You may have projects in these areas we have not listed.

If in doubt, tell us about them.

CNI areas with project examples

- **Communications** e.g. telecoms or 5G towers, public Wi-Fi
- **Emergency Services**, e.g. tracking software for ambulances, data sharing with the police of local authority managed CCTV and facial recognition.
- **Energy** e.g. local authority managed energy companies and renewable energy projects.
- **Food** e.g. technologies supporting local authority managed food banks.
- **Government** e.g. digital devices used to facilitate communications between government agencies that exceed that used in private sector (i.e. excluding software such as Microsoft Teams, and mobile telephones)
- **Health** e.g. smart technologies used to monitor vulnerable people in their homes, health programmes not managed by the NHS / DHSC.
- **Transport** e.g. AI traffic light systems and other 'smart' traffic management systems, autonomous vehicles.
- **Water** e.g. waste management monitoring, early warning flood systems, and digital depth sensors in reservoirs.
-

2. Looking at the above list, please answer the following question(s):

Do you have digital projects in any of these CNI areas?

Yes

No

Don't know

3.

Here is a reminder of the CNI areas with project examples

- **Communications** e.g. telecoms or 5G towers, public Wi-Fi
- **Emergency Services**, e.g. tracking software for ambulances, data sharing with the police of local authority managed CCTV and facial recognition.
- **Energy** e.g. local authority managed energy companies and renewable energy projects.
- **Food** e.g. technologies supporting local authority managed food banks.
- **Government** e.g. digital devices used to facilitate communications between government agencies that exceed that used in private sector (i.e. excluding software such as Microsoft Teams, and mobile telephones)
- **Health** e.g. smart technologies used to monitor vulnerable people in their homes, health programmes not managed by the NHS / DHSC.
- **Transport** e.g. AI traffic light systems and other 'smart' traffic management systems, autonomous vehicles.
- **Water** e.g. waste management monitoring, early warning flood systems, and digital depth sensors in reservoirs.
-

3. Please tell us about all of the CNI Digital projects you have.

	CNI Area and specific project (e.g. Energy - renewable energy project)
CNI Digital Project 1	
CNI Digital Project 2	
CNI Digital Project 3	
CNI Digital Project 4	
CNI Digital Project 5	
CNI Digital Project 6	
CNI Digital Project 7	
CNI Digital Project 8	

4. For each project you have told us about, which stage is the project at (choose from the drop-down menu)?

Department for Science, Innovation & Technology

	Project Lifecycle stage
CNI Digital Project 1	
CNI Digital Project 2	
CNI Digital Project 3	
CNI Digital Project 4	
CNI Digital Project 5	
CNI Digital Project 6	
CNI Digital Project 7	
CNI Digital Project 8	

5. If you said 'other' for any of your projects, please explain:

6. Please tell us ALL of the kinds of technology you are using for each project. Tick all that apply

	Cloud Computing & Virtualisation	Artificial Intelligence & Machine Learning (AI/ML)	Internet of Things (IoT) & Operational Technology (OT)	Cryptocurrencies & Blockchain	Remote Work & Collaboration Tools	Supply Chain & Third-Party Services	Biometric & Identity Systems	Quantum Computing (Emerging Risk)	Connected and Autonomous Vehicles (CAV)	Don't Know	Other
CNI Digital Project 1											
CNI Digital Project 2											
CNI Digital Project 3											
CNI Digital Project 4											
CNI Digital Project 5											
CNI Digital Project 6											
CNI Digital Project 7											
CNI Digital Project 8											

7. If you said 'other' to any of the kinds of technology, please explain:

8. What Government guidance/regulations (if any) do you use to help manage the cyber security of your organisation's digital CNI projects? Please list the guidance you use or if you do not use any, please write None.

9. Thinking particularly about cyber security for CNI projects, what else could the Government (or others) provide to support your organisation in managing cyber security on CNI projects?

4. Cyber Security Approach

10. We are interested in your Cyber Security policies

	Yes	No	Don't Know
Does your organisation have a general cyber security policy?			
Does your organisation have a specific cyber security policy(ies) for CNI projects?			

11. We are interested in cyber security risk assessments

	Never	Rarely	Sometimes	Often	Always	Don't know
How often does your organisation						

	Never	Rarely	Sometimes	Often	Always	Don't know
do cyber security risk assessments?						
How often does your organisation repeat cyber security risk assessments after recommendations have been implemented?						

12. Are system anomalies monitored?

Never

Rarely

Sometimes

Often

Always

Don't know

5. Staffing and Assets

13. Please indicate the Chief Information Security Officer's (CISO's) level of influence in your organisation (Pick one)

Very High

High

Moderate

Low

Very Low

Don't Know

We do not have a CISO

14. Please indicate the extent to which you agree with the following statement:

We have enough competent cyber security personnel for our CNI projects

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

Don't know

15. Please indicate the frequency of each of the following measures for your CNI project(s)

	Never	Rarely	Sometimes	Often	Always	Don't know
Cyber security requirements are included in contractor/supplier contracts for CNI projects						
Contractors and suppliers for CNI projects are provided with training						

	Never	Rarely	Sometimes	Often	Always	Don't know
in your organisation's cyber security policy and procedures						

16. Are software patches kept up to date on CNI projects?

Yes

No

Don't Know

6. Training and Awareness

17. Has your organisation provided advice/training about regulations or guidance specific to CNI projects?

Yes

No

Don't know

18. If yes, please provide further information about the content, the frequency and who is invited:

7. Processes and Procedures

19. Please consider the following questions in relation to your CNI project(s)

	Yes	No	Don't Know
Is there a password policy in place?			
Do you have policies to mitigate email based cyber security risks (e.g. emails marked when from an external source, spam filtering)?			
Is there an access log for important sensitive systems?			
Is anti-virus protection implemented?			
Is the use of a VPN enforced?			

8. Physical Working Environment

20. Please consider these questions in relation to your CNI project(s):

Does your cyber security policy include physical security measures such as a clear desk policy; access passes for offices for staff and visitors; and locking server rooms?

Yes

No

Don't know

21. Is this policy enforced?

Never

Rarely

Sometimes

Often

Always

Don’t Know

22. Is there a way of reporting breaches of this policy?

Yes

No

Don't know

9. Incident Management

23. If you have cyber security incidents, do you share them with:

	Yes	No	Don't Know
The board?			
All employees?			
External organisations, when the incident is significant?			

24. If you do share incidents with external organisations, which one(s)?

10. Closing Question

25. Is there anything else you would like to mention about your organisations' cyber security relating to its CNI projects?

ANNEX D: INTERVIEW TOPIC GUIDE

Background and Introduction – *3 minutes*

Thanks very much for joining us today. My name is xxx and this is my colleague xxx and we work for an external consultancy called WSP.

We are talking to you today as part of a piece of work commissioned by the Department for Science, Technology and Innovation (DSIT).

To re-assure you, the discussion will be informal. There are no right or wrong answers.

As you will be aware, local authorities are increasingly managing a diverse range of digital assets. This includes systems that might be classified as Critical National Infrastructure. These might include assets and projects in areas like Communications, Emergency Services, Energy, Food, Government, Health, Transport or Water.

Digital growth in these sectors brings new challenges and risks that require careful consideration and management. DSIT have commissioned WSP to undertake some research to better understand these emerging risks. So far, we have done some desk-based research, looking at global digital trends. Now we need to focus in on local authorities to identify where and how the most significant areas of digital risk are emerging in your context. +

If you wish to end the discussion at any time, please let me know. Your participation in this research is voluntary.

The contents of our discussion are completely confidential, and all findings are reported on anonymously. This means that no identifiable information will be shared with the Department for Science, Innovation and Technology or any other parties.

We would like to record the interview to make sure we gather all the insights you bring as this helps with making notes and analysis? Recordings are used only for analysis purposes and are stored securely in line with the Privacy Notice we shared with you in our email invite. I have a copy here if you would like another chance to read that?

Do we have your consent to record?

MODERATOR TO TURN ON RECORDING

GDPR added consent (MODERATOR TO ASK ONCE RECORDER IS ON)

Our legal basis for processing your data is as a **Public Task**. This means processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, to inform future government policy.

Your participation is voluntary. You can withdraw your consent for your data to be used at any point.

Can I check that you are happy to proceed?

IF YES – PROCEED.

Role and Responsibility – *3 minutes*

1. Before we get going, could you tell us a little bit about yourself and your role?

Critical National Infrastructure Projects and Cyber set-up – *50 minutes (25 minutes per project)*

2. **We would like to explore some of the Critical National Infrastructure Projects that your LA is involved in.** Here is a reminder of the kinds of things you talked about in the survey OR Here is a reminder about the questions we provided in our invitation.

Cloud Computing & Virtualisation	Artificial Intelligence & Machine Learning (AI/ML)	Internet of Things (IoT) & Operational Technology (OT)	Cryptocurrencies & Blockchain	Remote Work & Collaboration Tools	Supply Chain & Third-Party Services	Biometric & Identity Systems	Quantum Computing (Emerging Risk)	Connected and Autonomous Vehicles (CAV)	Don't Know	Other

CNI Digital
Project 1

Cloud Computing & Virtualisation	Artificial Intelligence & Machine Learning (AI/ML)	Internet of Things (IoT) & Operational Technology (OT)	Cryptocurrencies & Blockchain	Remote Work & Collaboration Tools	Supply Chain & Third-Party Services	Biometric & Identity Systems	Quantum Computing (Emerging Risk)	Connected and Autonomous Vehicles (CAV)	Don't Know	Other
CNI Digital Project 2										
CNI Digital Project 3										

MODERATOR PRE-WORK – IF THE PARTICIPANT HAS COMPLETED THE SURVEY, REFER TO THEIR **SURVEY RESPONSE**. WHERE AVAILABLE SELECT ONE OR TWO PROJECTS WHICH ARE IN A CNI AREA/TECHNOLOGY COMBINATION NOT YET COVERED IN PREVIOUS INTERVIEWS (CHECK THE **'INTERVIEW CNI TABLE'** DOCUMENT FOR GAPS TO BE COVERED OFF).

a. Can you tell us more about [project A] – UNPROMPTED RESPONSE INITIALLY BUT IF NECESSARY USE THE FOLLOWING PROMPTS:

- What stage of the project lifecycle is it at?
  - e.g. Pilot, Proof of Concept, Operational Service
- Where do you see the main cyber risks emerging from in this project?
  - Are there suppliers or other organisations involved and have any associated cyber risks been considered?
- Have you had any cyber incidents/concerns with this project?
- What Government guidance/regulations (if any) do you use to help manage the cyber security?
- What else could the Government (or others) provide to support your organisation in managing cyber security on CNI projects?

b. We now want to explore the cyber aspects of the technology further. (MODERATOR TO FOLLOW THE TECHNOLOGY-SPECIFIC SET OF QUESTIONS ENTITLED **'DSIT CNI TECHNOLOGY QUESTIONS'**).

Repeat a. and b. for [project B and C] as time allows.

Close out – *4 minutes*

3. We are coming to the end of our questions now. Is there anything else you would like to tell us that we haven't covered?

We will be producing a report and case studies for DSIT which will be published in due course.

Thanks very much for your time, today.

MODERATOR STOP RECORDING.

ANNEX E: PRIVACY NOTICE

Department for Science, Innovation & Technology

Study into the changing cyber threat profile and its potential impact on local authorities

Privacy Notice

The Department for Science, Innovation and Technology (DSIT) has commissioned WSP (UK) Ltd to develop an assessment of the largescale, emerging trends in digital risk, and their potential impact on local authorities. This risk assessment will support the development of UK Government's future strategic approach to cyber. This study will be informed by engagement with local government organisations.

This notice sets out how we will process your personal data, and your rights. It is made under Articles 13 and/or 14 of the UK General Data Protection Regulation (UK GDPR).

For data protection purposes, DSIT is the data controller and WSP (UK) Ltd is acting as DSIT's data processor to carry out the survey and compile results on our behalf.

1. Your Data

We will process the following personal data:

1. Basic Personal Information: This includes name, contact details (email address), local authority office address and job role (identified at the time of this privacy note last updated)
2. Communication records: This includes both stakeholder interview meeting minutes (recorded and transcribed) and online survey data, as well as other forms of recorded communication such as emails in relation to this study.

Where personal data has not been obtained from the data subject

Your personal data were obtained by WSP from published information on your applicable local government website and/or subsequent discussions with those initial contact points to identify the appropriate organisation representatives for the study.

2. Purpose

The purpose(s) for which we are processing your personal data is:

- To understand Critical National Infrastructure projects being undertaken by local authorities.
- To follow up with surveys and / or interviews that we may conduct with you and your organisation (with your option as whether to participate)

3. Legal basis of processing

The legal basis for processing your personal data under Article 6 of the UK GDPR is:

1(e)Public task: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, to inform future government policy.

4. Recipients

Your personal data will be processed by WSP UK Ltd and data protection assurance is provided through contractual agreements. As part of WSP's IT infrastructure, your personal data will be stored on systems provided by the supplier - Microsoft Services. They will not share personal data with this entity; rather, they are technical service providers who host infrastructure supporting on their IT systems.

WSP will also utilise SmartSurvey to capture survey responses including personal data of survey respondents. SmartSurvey's privacy notice can be viewed at: Privacy Policy – SmartSurvey[1].

5. Retention

Your personal data will be kept by WSP until no later than 1st September 2025, to inform a report for DSIT on local authority managed CNI is completed, after which it will be deleted by WSP. There will be no personal data included within the study report.

6. International Transfers

Our contracted partner for the purposes of this study, WSP UK Ltd, will comply with their Privacy Policy at: Privacy Policy – WSP[2] as this contains additional information about how they process personal data and international transfers.

As WSP will utilise SmartSurvey in order to administer survey(s), you should also review their privacy policy at: Privacy Policy - SmartSurvey[1] as this contains additional information about how they process personal data and international transfers.

7. Your Rights

You have the right to request information about how your personal data are processed, and to request a copy of that personal data.

You have the right to request that any inaccuracies in your personal data are rectified without delay.

You have the right to request that any incomplete personal data are completed, including by means of a supplementary statement.

You have the right to request that your personal data are erased if there is no longer a justification for them to be processed.

You have the right in certain circumstances (for example, where accuracy is contested) to request that the processing of your personal data is restricted.

You have the right to object to the processing of your personal data where it is processed for direct marketing purposes.

*Where the lawful basis is Public Task or Legitimate Interests y*ou have the right to object to the processing of your personal data.

To exercise your rights please contact the Data Protection Officer using the contact details below.

8. Contact Details

The data controller for your personal data is DSIT, you can contact the DSIT Data Protection Officer at: dataprotection@dsit.gov.uk

DSIT Data Protection Officer
Department for Science, Innovation &Technology
22-26 Whitehall
London
SW1A 2EG

If you are unhappy with the way we have handled your personal data, please write to the department's Data Protection Officer in the first instance using the contact details above.

9. Complaints

If you consider that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is an UK independent regulator. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113

https://ico.org.uk/make-a-complaint/

Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

10. Updates to this notice

If this privacy notice changes in any way, we will place an updated version on this page. Regularly reviewing this page ensures you are always aware of what information we collect, how we use it, and under what circumstances we will share it with other parties. The 'last updated' date at the bottom of this page will also change.

If these changes affect how your personal data is processed, we will take reasonable steps to let you know.

Last updated: 20 February 2025

ANNEX F: EMERGING TECHNOLOGY: RISK QUESTIONS

To supplement the structured interview topic guide, where interview time allowed, the following technical question set was used as prompts to explore local council participants experience and maturity in the different technologies being applied on their CNI sector digital projects or services.

Mitigation	Questions related to identified CNI project that employs Cloud Computing & Virtualisation
Strong encryption, access controls, multi-factor authentication, regular security audits	How do encryption, access controls, multi-factor authentication, and regular security audits contribute to securing cloud computing and virtualisation environments employed in the CNI project?
Regular backups, disaster recovery plans, versioning	Can you confirm whether backups, disaster recovery plans, and versioning are used to mitigate data loss in cloud computing and virtualization environments within the CNI project?
Implement least-privilege access, role-based access control (RBAC), IAM policies	Can you describe how you implement Identity and Access Management and confirm whether least privilege access, role based access control and IAM policies are used in the cloud computing and virtualization environments within the CNI project?
Implementing rate-limiting, traffic filtering, Distributed Denial of Service (DDoS) mitigation tools	Can you confirm that you have protections in place against Denial of Service (DoS) attacks? Do you implement rate-limiting, traffic filtering, and Distributed Denial of Service (DDoS) mitigation tools?
Regular patching, isolation of virtual machines, secure configurations	Can you confirm that you have protections in place against Shared Technology Vulnerabilities. Do you implement regular patching, isolation of virtual machines, and secure configurations?
Secure API gateways, token-based authentication, encryption	Can you describe how you secure APIs in the CNI project? Do you implement Secure API Gateways, token-based authentication and encryption?
Regular audits, compliance frameworks, risk assessments	Can you explain how you prove compliance with regulatory adherence for the CNI project?
Data localisation, choosing cloud providers with regional data centres, legal agreements	Can you explain how you manage data sovereignty in your cloud and virtualisation environment in the CNI project?
Cloud configuration best practices, automation tools, regular security checks	Can you explain how you ensure your cloud and virtualisation environment are configured correctly?
Multi-cloud strategy, portability of data and applications	Can you describe how you ensure that you not locked into one cloud vendor?

Mitigation	Questions related to identified CNI project that employs Artificial Intelligence & Machine Learning (AI/ML)
Encryption, access controls, regular audits, data minimisation	How do encryption, access controls, data minimisation and regular security audits contribute to securing AI & ML employed in the CNI project?

Robust model training, adversarial testing, anomaly detection	Can you explain how you protect against adversarial attacks that exploit weakness in AI models to deceive the model to make incorrect predictions.
Data integrity checks, secure data pipelines, robust validation	Can you explain how your protect against model manipulation and data poisoning attacks in your AI & ML models employed in the CNI project?
Diverse training data, bias audits, fairness metrics	Can you describe how manage bias and discrimination in your AI & ML models employed in the CNI project?
Explainable AI frameworks, model interpretability tools	Can you describe how ensure you understand how the AI model makes decisions and visibility into AI processes?
Model watermarking, encrypted storage, access restrictions	How do you ensure you protect your AI & ML assets from intellectual property theft?
Continuous monitoring, version control, rigorous testing	Can you briefly describe your monitoring, version control and testing processes for your AI & ML assets?
Compliance audits, legal reviews, AI governance frameworks	Can you briefly describe how you ensure ethical and regulatory compliance of your AI & ML models employed in the CNI projects?

Mitigation	**Questions related to identified CNI project that employs IoT & Operational Technologies**
Strong device authentication, firmware updates, network segmentation	Can you briefly describe how you protect IoT devices employed in CNI projects from being compromised?
End-to-end encryption, secure protocols (TLS/SSL), VPNs	Can you briefly explain how you protect IoT devices & Operational Technology employed in CNI projects from unlawful data interception?
Anti-malware solutions, regular updates, secure configurations	Can you briefly explain how you protect IoT devices and or Operational Technology employed in CNI projects from Malware and Ransomware?
Secure supply chain practices, hardware security modules, component validation	Can you briefly explain how you protect IoT devices and or Operational Technology employed in CNI projects from supply chain attacks?
Network segmentation, firewalls, intrusion detection systems	Can you briefly explain you ensure IoT devices and or Operational Technology employed in CNI projects had adequate network segmentation?
Strong authentication, multi-factor authentication (MFA), role-based access controls (RBAC)	Can you briefly describe how you ensure IoT devices and or Operational Technology employed in CNI projects are authenticated and authorised ?
DDoS mitigation strategies, traffic filtering, rate-limiting	How do you protect IoT devices and or Operational Technology employed in CNI projects from Denial of Service attacks?
Regular updates, system modernization, sandboxing legacy systems	Can you briefly describe how you protect legacy operational technology employed in CNI projects from cyber threats?
Physical access controls, surveillance, tamper-evident packaging	Please describe how you protect IoT devices and or operational technology employed in CNI projects from physical security vulnerabilities?

Compliance audits, adherence to regulatory standards, continuous monitoring	Can you briefly describe how you ensure regulatory compliance of your IoT devices and or Operatinal Technology employed in the CNI projects?

Mitigation	**Questions related to identified CNI project that employs Cryptocurrencies & Blockchain**
Multi-factor authentication, cold wallets for storage, regular security audits	n/a
Strong encryption, multi-signature wallets, phishing prevention	Can you briefly describe what measures you apply to protect your cryptocurrency wallets employed in CNI projects from theft?
Smart contract auditing, code review, formal verification	How do you protect cryptocurrency smart contracts employed in the identified CNI project?
Legal consultations, compliance with local regulations, stay informed about regulatory changes	Can you briefly describe how you stay abreast of regulatory and legal changes for cryptocurrency technology employed in the identified CNI project?
Risk diversification, stablecoins, hedging	Can you explain how you mitigate for price volatility in cryptocurrency technology employed in the identified CNI project?
Proof-of-work changes, decentralized consensus mechanisms	How do you protect against a blockchain attack (51% attack) in cryptocurrency technology employed in the identified CNI project?
Thorough vetting of ICOs, regulatory frameworks for ICOs, due diligence	n/a
Blockchain governance, transparency in code, effective dispute resolution	Can you briefly describe how you protect immutability of the blockchain technology employed in the identified CNI project?
Implementing privacy coins, KYC/AML regulations, transaction monitoring	How you protect identify of addresses used in blockchain transactions employed in the identified CNI project?
Shift to Proof-of-Stake, energy-efficient mining practices, carbon offset initiatives	n/a

Mitigation	**Questions related to identified CNI project that employs Remote Work & Collaboration Tools**
End-to-end encryption, multi-factor authentication, secure file sharing practices	How do you protect against data breaches in the remote work and collaboration technology employed in the CNI project?
Email filtering, anti-phishing training, regular awareness campaigns	Can you briefly explain how you protect against phishing attacks through the remote working and collaboration technology employed in CNI projects ?

Secure communication tools (e.g., encrypted video calls), VPNs	Can you briefly explain how you protect against actors intercepting communications through the remote working and collaboration technology employed in CNI projects?
Privileged access management, monitoring, employee training, least-privilege access	Can you briefly explain how you protect against insider threats on technology employed in CNI projects?
Cloud security best practices, regular audits, secure configurations	Can you explain how you ensure your cloud and virtualisation environment are configured correctly?
Regular patch management, automated update tools, vulnerability scanning	Can you explain how you identify vulnerabilities and manage patches to protect technology in CNI projects?
Shadow IT monitoring, app whitelisting, employee education	How do you protect against employees installing shadow IT in the identified CNI project?
Strong password policies, multi-factor authentication (MFA), Single Sign-On (SSO)	Can you explain how you apply authentication to protect technology in the identified CNI project?
DDoS mitigation strategies, traffic filtering, cloud-based DDoS protection	Can you explain what protections are in place against Denial of Service (DoS) attacks in the identified CNI project?
Regular compliance audits, selecting compliant tools, understanding legal obligations	Can you briefly describe how you ensure regulatory compliance of remote work & collaboration tools employed in the CNI project?

Mitigation	**Questions related to identified CNI project that employs Supply Chain & Third-Party Services**
Vendor risk assessments, encryption, contractual security requirements	How do you protect against third party data breaches in the supply chain & third-party services employed in the CNI project?
Code signing, software bill of materials (SBOM), continuous monitoring	How do you protect against software supply chain attack on technology employed in the CNI project?
Secure supply chain protocols, component validation, hardware security modules	How do you prevent hardware components from being compromised on technology employed in the CNI project?
Multi-factor authentication (MFA), least-privilege access, password rotation	How do you protect 3rd party credentials on the technology employed in the CNI project?
Vendor patching policies, vulnerability scanning, zero-trust architecture	How do you mitigate third-party unpatched software vulnerabilities in the technology used for the CNI project?
Diversification of suppliers, risk assessments, contingency planning	Do you employ one supplier in your supply chain delivering the technology used for the CNI project?

Background checks, strict access control, continuous monitoring	How do you protect against 3rd party insider threats in the technology used for the CNI project?
Redundancy planning, multi-cloud strategies, SLAs with uptime guarantees	How do you mitigate service provider outages in the technology used for the CNI project?
Vendor compliance audits, contract clauses for regulatory adherence	How do you ensure that your supply chain complies with regulations applicable to the CNI project?
Secure logistics, hardware verification, blockchain tracking	How do you protect against physical supply chain attacks in the technology used for the CNI project?

Mitigation	**Questions related to identified CNI project that employs Biometric & Identity Systems**
Biometric encryption, secure storage, multi-factor authentication (MFA)	How do you protect against biometric data breaches in the biometric & identity systems employed in the CNI project?
Liveness detection, multi-modal biometrics, AI-based anomaly detection	How do you protect against spoofing and presentation attacks in the biometric & identity systems employed in the CNI project?
Secure transmission, cryptographic hashing, challenge-response authentication	How do you protect against frauduant use of stored biometric data in the biometric & identify systems employed in the CNI project?
Adversarial AI detection, robust training data verification	How do you protect against model poisioning in AI based Identity verification in the biometric & identify systems employed in the CNI project?
AI-driven fraud detection, continuous authentication, deepfake mitigation	How do you protect against identity theft from biometric cloning in the biometric & identify systems employed in the CNI project?
Legal frameworks, user consent enforcement, ethical AI guidelines	How do you ensure that biometric data is collected with proper consent and stored securely within biometric & identity systems employed in the CNI project?
Zero-trust access, database integrity checks, anomaly detection	How do you protect against biometric data poisoning within biometric & identity system employed in the CNI project?
Compliance with ISO/IEC 19794, NIST biometric standards	Can you identify whether your biometric & identify system employed in the CNI project complies with IEC 19794 and or NIST biometric standards?
Regular compliance audits, transparent data policies	How do you ensure that your biometric & identity systems employed in the CNI project comply with regulations ?
Continuous system testing, fallback authentication methods	How do you ensure protect against operational failures and false positives in the biometric & identity systems employed in the CNI project ?

Mitigation	Questions related to identified CNI project that employs Quantum Computing
Post-quantum cryptography (PQC), quantum-resistant algorithms	n/a
Immediate transition to quantum-safe cryptography	n/a
Longer passwords, quantum-resistant hashing (SHA-3, Argon2)	n/a
Quantum key distribution (QKD), end-to-end quantum encryption	n/a
AI explainability models, quantum-resilient AI security	n/a
Secure supply chain, hardware attestation	n/a
Early adoption of NIST PQC algorithms, hybrid cryptography	n/a
Quantum-resistant blockchain cryptography (Lattice-based, hash-based)	n/a
AI-based anomaly detection, behavioural analytics	n/a
Continuous monitoring of quantum regulations	n/a

Mitigation	Questions related to identified CNI project that employs Connected and Autonomous vehicles
Secure ECU design, intrusion detection systems (IDS), encrypted CAN bus	How do you protect against ECU and CAN bus attacks in the CAV fleet used in the CNI project?
Secure V2X protocols, cryptographic message authentication	How do you protect against V2X communication attacks in the CAV fleet used in the CNI project?
Multi-sensor fusion, adversarial AI detection	How do you protect against CAV sensor spoofing in the CAV fleet used in the CNI project?
Secure boot, code signing, encrypted update channels	How do you mitigate against over the air update exploit in the CAV fleet used in the CNI project?
AI model adversarial robustness, continuous validation	How you protect against manipulation of autonomous decision making with the CAV fleet used in the CNI project?
Network segmentation, zero-trust security, endpoint detection	How do you protect against ransomware targeting the CAV fleet management system used in the CNI project?

Hardware security modules (HSMs), supply chain risk management (SCRM)	How do you protect against hardware and software attacks on automotive systems used in the CAV fleet used in the CNI project?
GDPR compliance, anonymization, data access controls	How do you protect data privacy and in particular driver surveillance in the CAV fleet used in the CNI project?
EMI shielding, redundancy in critical systems	How do you protect against Electromagnetic interference and hardware disruptions in the CAV fleet used in the CNI project?
Adherence to ISO 21434, UN R155 & R156 regulations	Did you apply ISO 21434 , UN R155 & R15 in the design of the CAV vehicle fleet used in the CNI project?

ANNEX G: DESK BASED RESEARCH SOURCES

Chainalysis. (2023, February). *The 2023 Crypto Crime Report.* https://www.chainalysis.com/reports/

Cloud Security Alliance. (2024, August 5). *Top Threats to Cloud Computing 2024.* https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

Cybersecurity & Infrastructure Security Agency. (n.d.). *Known Exploited Vulnerabilities Catalog.* https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Department for Digital, Culture, Media & Sport. (2022, March 30). *Cyber Security Breaches Survey.* https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022

Department for Digital, Culture, Media & Sport. (2023, April 19). *Cyber Security Breaches Survey.* https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023

Department for Digital, Culture, Media & Sport. (2024, April 9). *Cyber Security Breaches Survey.* https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024

European Union Agency for Cybersecurity. (2021, July 19). *Threat Landscape for Supply Chain Attacks.* https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

European Union Agency for Cybersecurity. (2023, October 19). *ENISA Threat Landscape 2023.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Federal Bureau of Investigation. (2024). *Internet Crime Report.* https://www.aha.org/system/files/media/file/2025/05/2024-fbi-internet-crime-report.pdf

Feldis, K. R. (2019, February 19). *Blockchain attacks and the fight for immutability*. https://perkinscoie.com/insights/update/blockchain-attacks-and-fight-immutability

Information Commissioner's Office. (n.d.). *Data security incident trends*. https://ico.org.uk/action-weve-taken/complaints-and-concerns-data-sets/data-security-incident-trends/

Microsoft. (2023, October). *Microsoft Digital Defense Report*. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

MITRE. (n.d.). *Adversarial Threat Landscape for Artificial-Intelligence Systems.* https://atlas.mitre.org/

MITRE. (n.d.). *ATT&CK Data & Tools.* https://attack.mitre.org/resources/attack-data-and-tools/

MITRE. (n.d.). *CVE Security Vulnerability Database.* https://www.cvedetails.com/

National Cyber Security Centre. (n.d.). *Cloud security guidance*. https://www.ncsc.gov.uk/collection/cloud

National Cyber Security Centre. (2020, May). *Connected Places: Cyber Security Principles.* https://www.ncsc.gov.uk/files/NCSC-Connected-Places-security-principles-May-2020.pdf

National Cyber Security Centre. (2023, April 23). *Cyber experts warn of rising threat from commercial hacking tools over the next five years*. https://www.ncsc.gov.uk/pdfs/news/cyber-experts-warn-of-rising-threat-from-commercial-hacking-tools-over-the-next-five-years.pdf

National Cyber Security Centre. (2024). *NCSC Annual Review 2024*. https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf

National Cyber Security Centre. (2024, September 18). *NCSC and partners issue advice to counter China-linked campaign targeting thousands of devices*. https://www.ncsc.gov.uk/pdfs/news/ncsc-and-partners-issue-advice-to-counter-china-linked-campaign-targeting-thousands-of-devices.pdf

National Institute of Standards and Technology. (n.d.). *National Vulnerability database.* https://nvd.nist.gov/

National Institute of Standards and Technology. (2017, January 3). *Post-Quantum Cryptography.* https://csrc.nist.gov/Projects/post-quantum-cryptography

Verizon. (2024, March 6). *2023 Data Breach Investigations Report DBIR.* https://www.verizon.com/about/news/media-resources/attachment?fid=65e1e3213d633293cd82b8cb&msockid=030de7d4ece163aa0731f25eedb96274

Widdowson, A. (2025). *Humans and cyber security: How organisations can enhance resilience through human factors* (1st ed.). CRC Press.

3rd Floor
11 Westferry Circus, Canary Wharf
London
E14 4HD

wsp.com