
UK Resilience
Academy
UK Resilience
Lessons Digest
Learning from Cyber Incidents
Issue 6 | April 2025

Contents

Foreword

> "True Resilience is something in which we all have a stake and good cyber security matters more than ever."[1]

With the words of Anne Keast-Butler (Director of GCHQ*) at CYBERUK 2024 we welcome you to the 6th edition of the UK Resilience Lessons Digest.

Cyber vectors** and our ability to manage cyber incidents is a key aspect of the UK's resilience. The National Cyber Security Centre's (NCSC) 2024 Annual Review stated that ransomware perpetrated for profit remains the most immediate and disruptive cyber threat to our Critical National Infrastructure[2]. Cyber criminals targeted Synnovis in 2024, affecting some of the largest hospitals in the UK, and in doing so demonstrated that no target is off the table.

But Cyber is also a domain of state competition. The Director of GCHQ stated in May 2024 that "China poses a genuine and increasing cyber risk to the UK" and "the activities of Russia and Iran pose an immediate threat to the UK"[3]. Every organisation has a role to play in mitigating the threat posed by these actors to ensure our resilience.

Technological change poses another challenge. Technologies like Artificial intelligence (AI) and quantum technologies will transform our approach to resilience - for example the use of AI to support cyber defenders with analysis of logs and files, network traffic, supporting secure code development and testing, and threat intelligence.

---

* Government Communications Headquarters
** The method an attacker uses to gain unauthorised access to a computer system or device.
1 CYBERUK 2024: Anne Keast-Butler keynote speech
2 Chapter 01: The cyber threat - NCSC.GOV.UK
3 CYBERUK 2024: Anne Keast-Butler keynote speech

Resilience in today's world means evolving and being dynamic like never before so that we capitalise on the opportunities and stay ahead of the risks. The NCSC is taking steps to protect the UK by investigating and attributing malicious activity, assisting the disruption of cyber criminals, actively responding to incidents, and supporting UK organisations of all sizes to build their own cyber resilience. We support the UK through free resources like our suite of Active Cyber Defence services, which includes the Early Warning service that provides free notifications informing potential victims of malicious activity. We also have extensive publicly available advice and guidance on all aspects of cyber security and national frameworks like Cyber Essentials which can protect organisations of all sizes against the most common cyber threats. We are also nurturing the next generation of cyber security professionals through developing and embedding schemes like our CyberFirst program.

Responding to cyber threats is a shared responsibility. We welcome the theme of this issue of the UK Resilience Lessons Digest highlighting the importance of collaboration and coordination against cyber attacks. As ever the NCSC is here to support you in preparing for, responding to, and recovering from incidents as you play your part in making the UK the safest place to live and work online.

Jonathon Ellison
NCSC Director of National Resilience

Introduction

Welcome to Learning from Cyber Incidents

Welcome to the sixth edition of the UK Resilience Lessons Digest, 'Learning from Cyber Incidents'. This Digest is the first in our series to be brought to you by the UK Resilience Academy (UKRA). Having grown up and out of the Emergency Planning College (EPC), the UKRA aims to enhance the training and skills offer for the UK resilience community, contributing to greater societal resilience. As part of that vision, we are delighted to present this latest Digest in its updated format, which continues to deliver on the central commitment to synthesise and share lessons from exercises and emergencies[4].

Less than one week after publication of Digest 5 in November 2024, Richard Horne, Chief Executive Officer of the UK's National Cyber Security Centre (NCSC), confirmed that "hostile activity in UK cyberspace has increased in frequency, sophistication and intensity"[5]. He went on to emphasise the need for sustained vigilance in an increasingly aggressive online world[6], where hospitals, universities, local authorities, democratic institutions, and government departments have all been targeted by malicious cyber attacks in the space of just 24 months[7]. In response, the National Cyber Security Chief made a recent call for increased cyber security within and across the various sectors of society: "We need all organisations, public and private, to see cyber security as an essential foundation for their operations and a driver for growth. To view cyber security not just as a 'necessary evil' or compliance function, but as a business investment, a catalyst for innovation and an integral part of achieving their purpose."[8]

The thematic relevance and timeliness of a cyber-focussed Digest edition was further impressed by findings detailed in the NCSC's recent Annual Review. Between 1 September 2023 to 31 August 2024, the NCSC Incident Management (IM) team received 1,957 reports of cyber attacks. Of those attacks, 430 incidents required direct support from the IM team, and 89 were nationally significant. Compared to data from 2023, there was also a three-fold increase in attacks ranked at the top of the NCSC severity scale[9]. Beyond the statistics, associated human costs have been made increasingly salient through high profile

attacks like that on Synnovis in 2024[10] or the British Library in 2023[11], which targeted technology we depend on to access health services and national knowledge[12].

Despite the complex, dynamic nature of the cyber threat, the lessons brought together in this edition emphasise that the responsibility for cyber resilience is a shared one. As you will see from the transferable learning in this edition's analysis, technical expertise, training and the active execution of basic cyber hygiene (such as the timely installation of software updates), all play critical roles in collective cyber resilience.

The UKRA maintains the commitment to continually improve the Digest in response to feedback, to ensure it remains relevant to the resilience community. Please do share your thoughts, ideas, and feedback via the QR code to help inform future publications.

We look forward to hearing from you.

Iain Sirrell

Head of Learning and Development, UK Resilience Academy

Lianna Roast

Head of Thought Leadership, UK Resilience Academy

4 National Resilience Framework
5 NCSC's Annual Review 2024
6 NCSC News: 3rd December 2024
7 NCSC's Annual Review 2024
8 NCSC News: 3rd December 2024
9 NCSC News: 3rd December 2024
10 BBC: Synnovis
11 Learning lessons from the cyber-attack - Knowledge Matters blog
12 NCSC's Annual Review 2024

Executive summary

Learning to Manage Lessons

Executive Summary

The publicly available UK Resilience Lessons Digest is part of the Government's commitment to strengthen societal resilience[13]. It sits at the heart of a programme of work at the UK Resilience Academy to synthesise and share lessons identified from major exercises and emergencies.[14]

Each edition of the Digest adopts a thematic focus. All content, including the central learning analysis, is tailored to achieve the Digest's three key objectives:

- To **summarise** learning themes from a wide range of relevant sources.
- To **share** transferable lessons across responder organisations and the wider resilience community.
- To **coordinate** knowledge to drive continual improvements in doctrine, standards, good practice, training and exercising.

Sidelights
As in previous editions, the Digest continues to use Sidelights to provide helpful definitions, insights and related knowledge.

Make it active
The 'Make it active icon' highlights opportunities and ideas for putting Digest content into action in your setting.

Resources
At the end of the Digest the resources section provides a summary of transferable lessons from the analysed reports, along with links for further reading.

Summarise:

Learning from Cyber Incidents

This sixth edition of the Digest has a thematic focus on learning from cyber incidents. The central learning analysis summarises learning themes and shares transferable lessons from seven cyber incidents, to support and inform continual improvements in cyber resilience. Additional articles that explore the UK's cyber landscape, highlight lived experience of responding to and recovering from a cyber attack, and provide actionable academic insights are also included.

Over the last two years, hospitals, universities, local authorities, private sector organisations, and government departments have all been targeted in malicious cyber attacks[15]. Speaking at the launch event of the National Cyber Security Centre's Annual Review 2024, National Cyber Security Chief, Richard Horne, confirmed that "hostile activity in UK cyberspace has increased in frequency, sophistication and intensity". In response, a renewed call for increased cyber security within and across the various sectors of society has been made. This edition of the Digest acknowledges the dynamic challenges that cyber threats pose, summarising lessons from cyber incidents to support continual improvements in cyber resilience.

- Seven source documents detailing **a combined total of 100 findings, lessons and recommendations from significant cyber incidents between 2017 and 2023** were selected for analysis.
- The documents (including **reports, audits, reviews, and case studies**) were both sectorially diverse, and representative of different cyber attack methodologies.
- All incidents had direct or indirect impacts for UK citizens, services or businesses.

13 Resilience Framework
14 UK Resilience Academy | Share
15 FINAL - 17/07/24 King's Speech 2024 background briefing final GOV.uk.docx
16 Cyber Hygiene: 10 Everyday Practices for Enhanced Digital Security

Share: Learning themes and transferable lessons

Six dominant learning themes were identified through the analysis of the documents. These are detailed below in order of prevalence and presented in Figure 1.

Theme 1: Cyber security and hygiene

Much like personal hygiene, cyber hygiene refers to basic, routine practices that help to maintain the 'health' and security of an IT system. [13]Every report included at least an element of cyber hygiene, and commonly, the measures that might have reduced the severity of an incident's impacts – or perhaps mitigated an attack altogether – were basic in nature. This included a need for improvements in the application of software updates, strong passwords, anti-virus software, and multi-factor authentication.

Theme 2: Planning and preparedness

Learning in this theme fell broadly into one of four areas: 1) insufficient training leading to poor awareness of cyber threat and risk 2) the inadequacy of generalised business continuity and disaster recovery plans, necessitating the need for specific cyber incident plans 3) the need for increased cyber exercising in light of the threat; and 4) a need for improved preparedness for cyber incident detection, given that there was a lag between the start of the attack and the realisation that it was in process.

Theme 3: Cyber incident management

There were many challenges highlighted in the management of cyber incidents. Examples included the storage of incident response plans on electronic systems that were attacked, and problematic crisis response communications due to the usual means of internal communications, such as emails or instant messaging being unavailable. In some cases this was exacerbated by the fact that cyber attacks often occurred just before (or in) a holiday period, or at a weekend when less staff would be around. This is a known tactic of cyber criminals. External communications with key stakeholders, multi-agency partners and the public, were also very difficult, and cyber incident/emergency roles or leads, if an organisation had them, were not always easily identified.

Theme 4: Challenges in recovery

Challenges in recovery included technical aspects (back-ups), staff health and wellbeing, and the dynamic nature of new risks to be managed during a protracted recovery period. Back-ups were not always kept updated or stored on a separate system/location to the original data, and data asset registers were not always kept or maintained. The intensity of the response and its impacts on teams and individuals was also evident with cyber attacks bucking the 'traditional nature' of major incidents (i.e. very intense but over within a limited time, or long lasting but slower moving) creating the potential for a long running, highly intense incident[17].

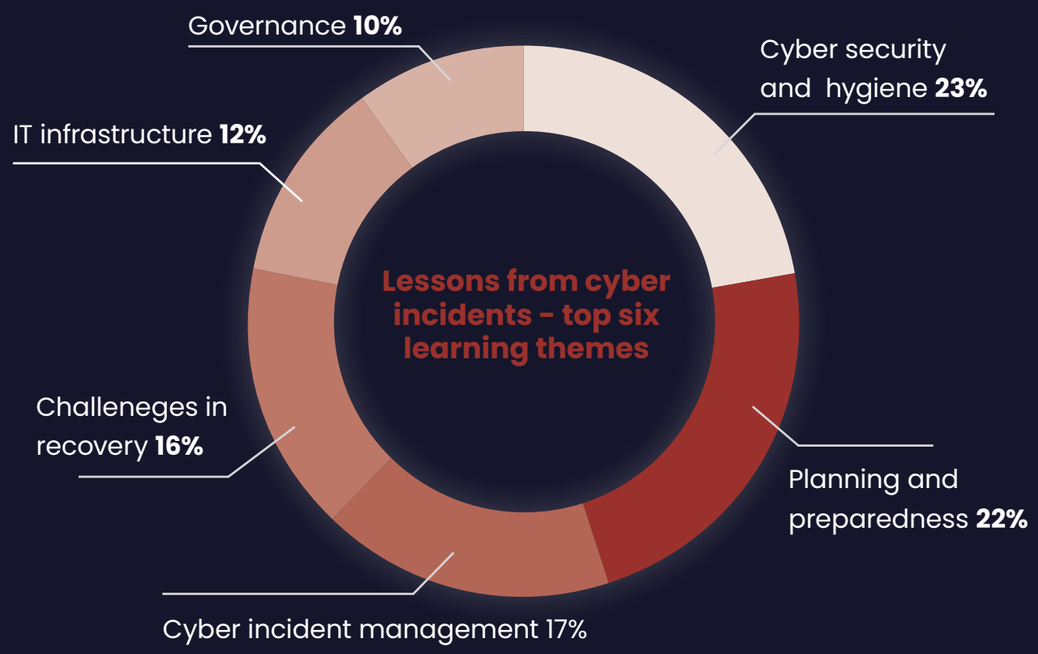
Theme 5: IT Infrastructure

This learning theme was the most technical by default. The most problematic infrastructure issues were legacy IT systems and software, bespoke and customised applications, and a lack of effective network segmentation. It highlighted the importance of sound IT skills and resources within an organisation, but also the high value that organisations place on expertise that they had kept available to them on retainer. The support of national cyber security professionals, and indeed other stakeholders and agencies that had lived experience of responding to an attack, was considered invaluable.

Theme 6: Cyber governance

Cyber governance was a smaller, but vitally important theme across reports. It particularly emphasised the critical role that leadership, and especially Board members have in ensuring their organisation has the understanding, expert oversight and cultural emphasis that underpin effective cyber security. This theme impressed that good cyber governance extends beyond policy review and ownership, to an understanding of the threat, strategic oversight of prevention and preparedness, and the readiness to respond in the event of an attack

Figure 1: Thematic areas of learning from cyber incidents



Coordinate: Shared experience, knowledge and insights

Learning from Cyber Incidents is supplemented by a range of supporting articles, to help the resilience community navigate the UK's cyber security landscape, learn from lived experience, and build resilience against evolving digital threats. A short overview of included articles is provided below.

Cyber Resilience: An Introduction

This introduction to cyber resilience is a helpful explainer on common cyber terms, the nature of cyber risk, and the characteristics of cyber attacks.

Building Resilience Against AI-Enabled Deception

Artificial Intelligence (AI) offers incredible potential and positive applications. However, it has also created new and evolving means for those with malicious intent to exacerbate the problem of whether we can trust online content[18]. In this article Di Cooke, a Fellow at the Center for Strategic and International Studies (CSIS) and researcher at King's College London, shares her academic insights and expertise on the risks that AI brings into the cyber security landscape. She also signposts to practical tips and helpful resources for managing AI risks, planning for related incidents and building cyber resilience.

18 Preserving integrity in the age of generative AI - NCSC.GOV.UK

Beyond Prevention: Minimising Cyber Impact in Local Government

It is now broadly understood that cyber-attacks on local government are a matter of 'when' not 'if'. In this article Alex Coley Deputy Chair of LGA's Improvement and Innovation Board from the Local Government Association (LGA) reflects on recent attacks, in view of the significant amounts of sensitive data that councils hold and their critical need to deliver uninterrupted services. The article highlights the amplified potential for disruptive impacts, impressing the urgent need for a greater focus on impact mitigation.

Working through WannaCry: Managing a Cyber Incident

In this article UK Resilience Academy Associate, Adam Bland, shares his lived experience of working in a leadership role during the 2017 WannaCry cyber incident response. His operational experiences and reflections highlight both the importance of cyber-specific incident planning, and the personal impacts that a protracted response can have on individuals and teams.

Cyber resilience

An Introduction

Cyber Resilience

Rapid advances in cyber capabilities have driven economic opportunities, supported scientific breakthroughs, and brought significant societal benefits. At an individual level, smartphones, devices, computers, and the internet are now such a fundamental part of modern life that it can be difficult to imagine coping in a world without them. However, as the Rt Hon Peter Kyle MP (Secretary of State for the Department for Science, Innovation and Technology) reminded us in January 2025, 'The growth of digitisation and the opportunities that it unlocks also presents an increasing and evolving cyber risk'.

Sidelight: Key terms

'Cyber' refers to anything involving or relating to computers, computer networks, information technology and the internet.

'Cyberspace' refers to the globalised, virtual environment in which these networks and digitised systems interact with people and with each other.

'Cyber threat' refers to anything capable of compromising the security of, or causing harm to, information systems and internet connected devices (to include hardware, software, and associated infrastructure), the data on them and the services they provide.

[1] NCSC Glossary

Cyber risk

Some cyber risks and related incidents, such as service outages due to technical fault or physical damage following a storm, are non-malicious. **Malicious cyber attacks** are those that intend to cause harm through unauthorised access to computers and networks. These attacks are a form of **cyber crime**, which by definition refers to any crime that uses computers or the internet[19]. In the context of this Digest edition, the terms 'cyber attack' and 'cyber incident' are used interchangeably.

19 Glossary of cyber security terminology | UK Cyber Security Council

Cyber attacks

Cyber attacks can target individuals or organisations, and they are increasing[20]. They occur when a 'threat actor(s)' (otherwise known as 'hackers' or cyber criminals) employ their skills to find and exploit cyber vulnerabilities. Some work alone, others work in organised groups, and some threat actors work on behalf of other states. Underlying motivations vary, but typically focus on gaining unauthorised access to data on an information system to cause disruption, inflict deliberate damage to cyber infrastructure, or achieve financial gains associated with data theft[21].

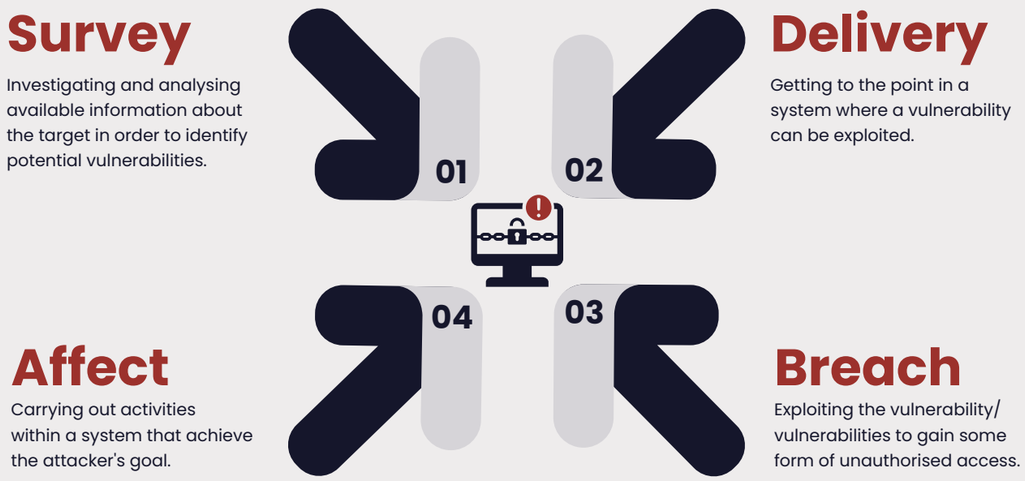
In 2023 the UK was the third most targeted country in the world for cyber attacks, after the US and Ukraine. The targets of these attacks are diverse, and the nature of cyber risk facing the UK is broad and complex. The effects and impacts of a cyber attack can create cyber incidents of varying severity.

The rise of **Artificial Intelligence (AI)** has also evolved the cyber risk landscape. For more infomration see the article **'Building resilience against AI-enabled deception'** on page 51

[1] How resilient is UK Critical National Infrastructure to cyber-attack? - Committees - UK Parliament

Cyber attacks commonly comprise four stages, as seen in **Figure 2** and set out in NCSC guidance. These stages can advance quickly, but increasingly strategic attacks may progress over much longer periods and develop access over time.

Figure 2: Stages of a cyber attack



20 NCSC News: 3rd December 2024

21 NCSC News: 3rd December 2024

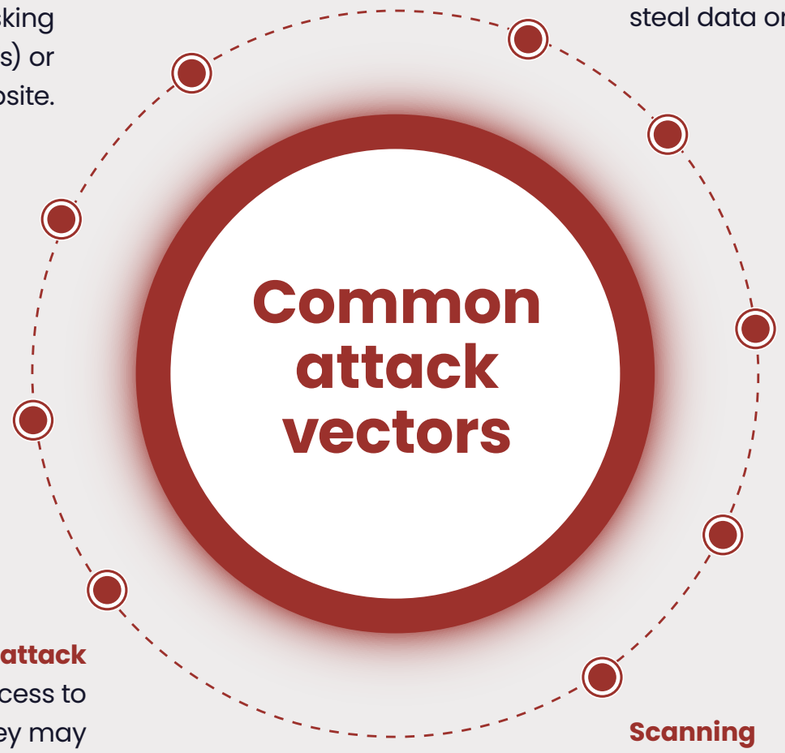
Cyber attacks can be targeted or untargeted in nature[22]. In the case of **targeted attacks**, an individual or organisation is singled out because the attacker has been paid to target them or has a specific interest in the business. These attacks can be especially damaging because they are likely to have been tailored to attack specific systems, processes or personnel, either in the office or occasionally at home.

More commonly, **untargeted attacks** take advantage of existing vulnerabilities and leverage internet access and to indiscriminately target as many devices, services or users as possible. In either case, the method that an attacker uses to gain unauthorised access to a computer system or device is known as an **'attack vector'[23]**, and can vary in its levels of sophistication.

22 Common_cyber_attacks_ncsc.pdf

23 NCSC Glossary

Figure 3: Common attack vectors. Adapted from: NCSC,Common cyber attacks: reducing the impact[24]



Phishing
Sending emails to large numbers of people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Watering hole attack
Setting up a fake website or compromising a legitimate one to exploit visiting users.

Ransomware
A type of malware that prevents you from accessing your computer (or the data that is stored on it). Usually, the victim is asked to contact the attacker to make a payment to unlock the machine or access the encrypted data.

Insider attack
An attack committed by anyone who has legitimate access to relevant systems, such as an employee or a contractor. They may be directly motivated by personal gain or grievances or have been subject to the influence, manipulation or deception of an attacker (i.e. social engineering).

Malware
Malicious software that can be hidden and delivered to a victim's computer via an attacker's server, website scripts, or in specific download links to capture system information, steal data or commit other cyber crimes.

DDOS (Distributed Denial of Service)
Targeted or untargeted attacks designed to overload a computer or system with requests from multiple computers or locations, so that genuine users can no longer access the service.

Subverting the supply chain
To attack equipment or software being delivered to the organisation. In general attackers will, in the first instance, use commodity tools and techniques to probe your systems for an exploitable vulnerability[25].

Spear-phishing
Sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software.

Scanning
Attacks that scan wide swathes of the internet at random, searching for vulnerabilities (like misconfigurations or software flaws) that are duly exploited. The exploitation of a newly identified vulnerability for which a software update has not yet been developed is known as a 'zero day' exploit.

24 common_cyber_attacks_ncsc.pdf
25 common_cyber_attacks_ncsc.pdf

Cyber Security

Cyber security is how individuals and organisations reduce the risk and impact of cyber attacks. Its core function is to protect and defend the information, services and devices we rely on from disruption, theft, or damage[26]. **Cyber security employs both technical and non-technical defence mechanisms** in tandem to protect:

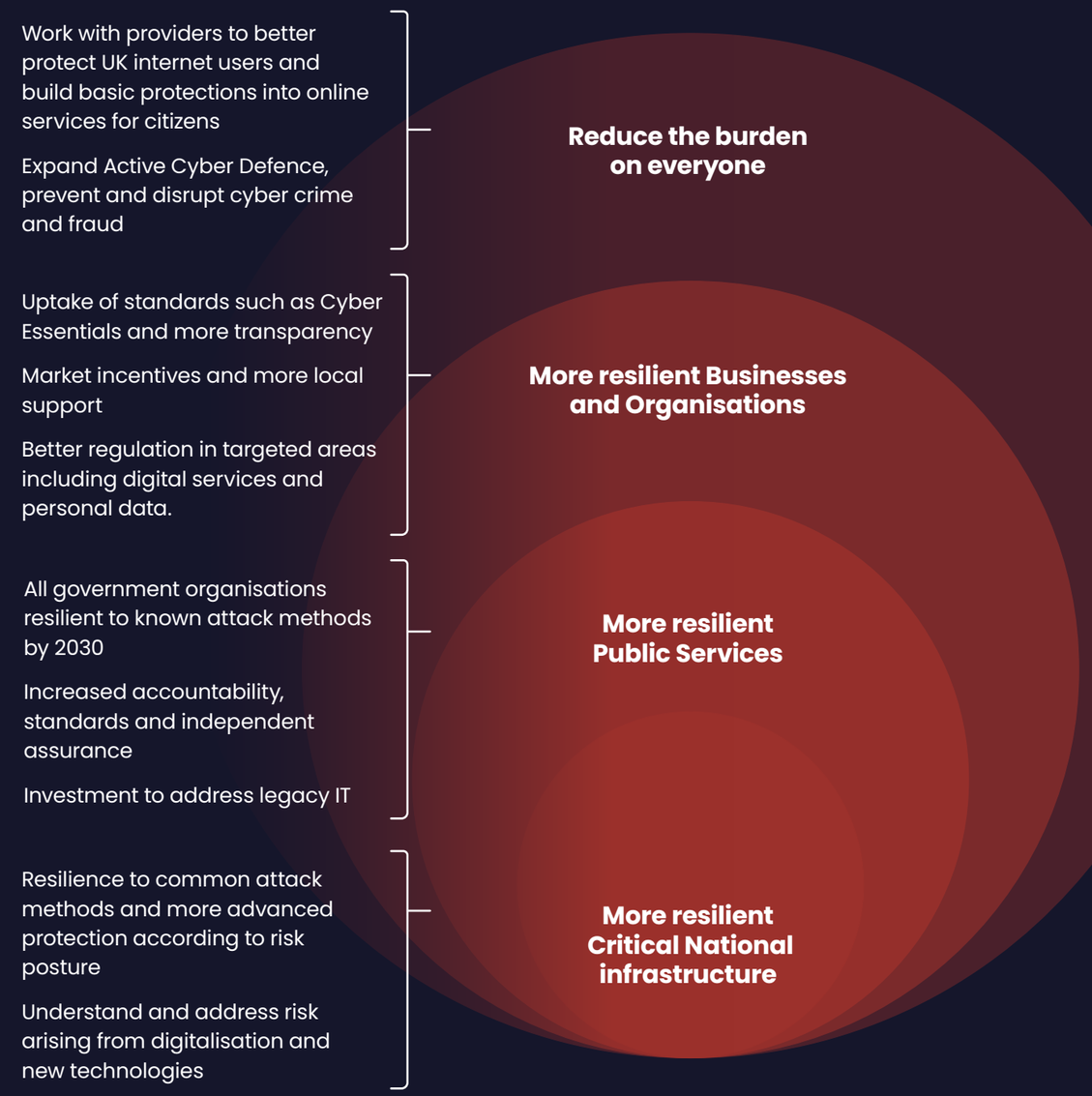
- Hardware, software and associated cyber infrastructure.
- Data and information stored or processed online and on devices.
- Digital systems and services[27].

At a personal level, cyber security plays a vital role in protecting data stored on individual devices and cloud-based software applications. At the organisational and institutional level, it plays a crucial part in making sure that our critical national infrastructure can operate effectively, and that governments can continue to provide the essential services that citizens depend upon[28].

Cyber Resilience

'Cyber resilience' is the ability for organisations to prepare for, respond to and recover from cyber attacks, security breaches or service outages. Importantly, **good cyber security facilitates better cyber resilience[29]**. The benefits of proactive cyber resilience are set out in **Figure 4**.

Figure 4: Benefits of cyber resilience: National Cyber Strategy 2022[30]



Further details, including good and leading practices in local cyber incident preparedness can be found in **National Resilience Standard: National Cyber Resilience Standard 14: Cyber incident preparedness.**

26 NCSC News: 3rd December 2024
27 Protect your charity from cyber crime - GOV.UK
28 What is cyber security?
29 What is cyber security?
30 Reproduced from National Cyber Strategy, page 67.

Learning analysis

Learning from Cyber incidents

Introduction

The importance of accurately identifying lessons from cyber incidents, including root causes, is impressed in NCSC's Cyber Assessment Framework (CAF)[31]. So too is the vital work of implementing learning thereafter, to minimise the impact of future cyber security incidents and improve the resilience of essential functions[32]. The importance of lesson identification and implementation are similarly set out in the Scottish Government's Public Sector Cyber Resilience Framework[34], which underscores the significance of the role that organisational post-incident review and learning activity plays in the improvement of cyber security measures.

Sidelight:
Did you know...

A staggering 7.7 million cyber crimes were experienced by businesses over the past year. That's around half of all businesses in the UK.

Cyber Essentials:
NCSC.GOV.UK

In line with the good and leading practices highlighted in these frameworks, and in response to the dynamic, evolving nature of the cyber threat, the purpose of this analysis was to synthesise lessons and recommendations from multiple, malicious cyber incident reports. The aims of doing so were to:

- Identify any **common learning themes** evidenced across reports, to support a shared and developed understanding of cyber risks.
- Highlight any specific, **transferable lessons** that could be used by the resilience community to inform practical cyber incident prevention and preparedness.
- Coordinate and signpost to existing knowledge relating to the learning themes in support of strengthened **cyber resilience**.

---

31 Principle D2 (CAF Objective D)
32 Principle D2 Lessons Learned - NCSC.GOV.UK
33 Scottish Government's Public Sector Cyber Resilience Framework, Category 16.4
34 Cyber resilience: framework and self assessment tool - gov.scot

'Learning themes' refer to common areas or patterns in findings, lessons and recommendations detailed across analysed reports.

'Transferable lessons' are key points of learning identified during the analysis, that have multi-stakeholder applicability, or are by nature 'risk agnostic' (i.e. could be leveraged to strengthen resilience in other risk scenarios beyond the report context).

Methodology

The Digest applied its usual methodology for synthesising selected documents and addressing the research questions[35]. This involves engaging with full report content, before drawing out key findings, lessons, and recommendations for analysis. Once the key points of learning from each had been identified, these were then reviewed for any common learning themes.

Analysis

A total of seven different documents were selected for the analysis. Each detailed learning from a significant, and in some cases international and high-profile, cyber incident.

All incidents occurred within the last six years (2017 – 2023), with direct or indirect impacts for UK citizens, services and/or business franchises. While not exhaustive, the combined total of 100 findings, lessons and recommendations were both sectorially diverse and representative of different cyber attack methodologies.

A selection of supporting materials, resources and documentation were also reviewed to inform additional, relevant insights with respect to both specific incidents and wider cyber security learnings. Source reports and relevant details are set out in Table 1, followed by a list of supporting documents.

35 UK Resilience Academy | Share
* Key Points of Learning

Year	Organisation(s)	Primary attack method	KPoL*
2017	**NHS England 2017** Lessons Learned Review: WannaCry Ransomware Attack	Ransomware attack	26
2017	**Equifax** Final Equifax Report.pdf United States Senate Permanent subcommittee on investigations Committee on Homeland Security and Governmental Affairs	Exploitation of software vulnerabilities	9
2018	**Marriott** Marriott International Data Breach	Exploitation of acquired software vulnerability, following company merger.	7
2020	**Scottish Environment Protection Agency (SEPA)** SEPA Internal Audit Report 2020/21 Cyber Attack – Lessons Learned	Ransomware attack	19
2021	**Gloucester City Council, England** Gloucester City Council: Managing a cyber attack	Phishing email, via compromised third-party supplier.	12
2023	**British Library** Learning lessons from the cyber-attack: British Library cyber incident review	Ransomware attack	21
2023	**St Helens Borough Council, England** St Helens Borough Council: Managing a cyber attack	Malware as a Service (MaaS) incident	6
Total			**100**

Supporting materials:

- Scottish Environment Protection Agency (SEPA). Police Scotland cyber response debrief
- Neil Daswani and Moudy Elbayadi. Big Breaches - Cybersecurity Lessons for Everyone. (Published by Apress Berkeley, CA © 2021)
- National Audit Office (NAO) Investigation WannaCry cyber attack and the NHS (Summary)
- INFOSEC, 2019. Lessons learned: the Marriott breach
- Copeland Borough Council, Wales: Copeland Borough Council: managing a cyber attack | Local Government Association

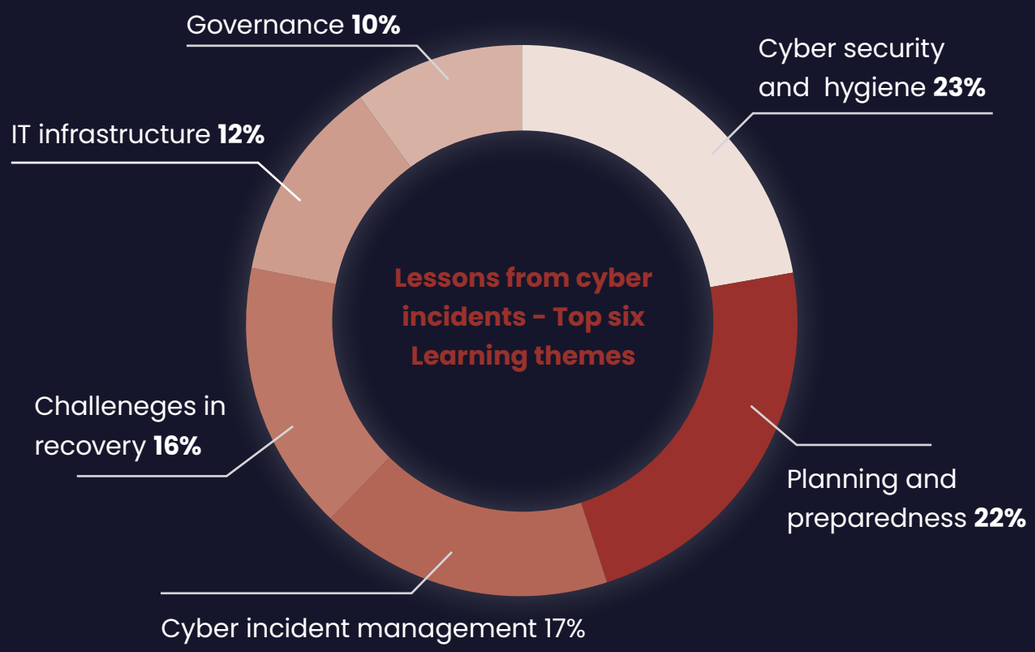
Findings

Six dominant learning themes were evident across all seven of the selected reports. In order of prevalence, the themes are listed below and visualised in Figure 2.

A summary of findings under each theme heading and a selection of transferable lessons can be found under the relevant thematic headings that follow.

- Theme 1: Cyber security and hygiene
- Theme 2: Planning and preparedness
- Theme 3: Cyber incident management
- Theme 4: Challenges in recovery
- Theme 5: IT Infrastructure
- Theme 6: Cyber governance

Figure 5: Prominent learning themes from reviews, reports and case studies of recent cyber incidents



Theme 1: Cyber security hygiene

The most prominent learning theme centred on the importance of **cyber security hygiene.** Cyber hygiene refers to basic, routine practices that help to maintain the 'health' and security of an IT system[36]. Every report included at least an element of cyber hygiene, and commonly, the measures that might have reduced the severity of an incident's impacts – or perhaps mitigated an attack altogether – were basic in nature. For example, in the report from NHS England following the WannaCry ransomware attack in 2017, it was noted that more than half of local NHS organisations had not patched systems (i.e. applied necessary updates) when required. This meant that known vulnerabilities were exploited before the available fixes had been applied. However, this also revealed that what can be 'basic' in theory does not always equate to 'easy' in practice.

36 Cyber Hygiene: 10 Everyday Practices for Enhanced Digital Security

In the case of the WannaCry report, it was found there was not adequate visibility on outstanding updates across the diverse and complex digital infrastructures within the NHS. Furthermore, the reasons that many updates had not been installed included the real-world pressures and concerns about the impact that the necessary downtime for updates would have on clinical services.

The need for continual improvement in cyber hygiene fundamentals was not unique to the WannaCry attack. Similar issues with outdated software[37], unmanaged and poorly governed update processes, weak passwords, and insufficient account management controls, all featured in respective reports as causal (or at least contributory) factors in the ability of cybercriminals to carry out their attacks.

Examples of transferable lessons in this theme are provided below:

Report	Transferrable lessons
Marriott	Marriott used an outdated version of software, which had known vulnerabilities that the attackers were able to exploit.
Equifax	Equifax had no standalone written corporate policy governing the patching of known cyber vulnerabilities until 2015. After implementing this policy, Equifax conducted an audit of its patch management efforts, which identified a backlog of over 8,500 known vulnerabilities that had not been patched.
SEPA	Many employees had administrative accounts to facilitate their roles. However, Privileged Account management controls required improvement. Once compromised, this vulnerability had facilitated lateral movement during the attack, and privilege escalation. The Authentication Password policy was not sufficiently secure. Multifactor authentication (MFA) was not used, or inconsistently used.
NHS England	All reviews of the WannaCry attack have noted that the vulnerabilities that were exploited could have been addressed through good IT management control. Over half of local NHS organisations reported they had not patched systems when required due to concerns about the impact of the necessary downtime on clinical services.

Make it active:

Given that most common cyber threats are relatively unsophisticated, using a set of good "cyber hygiene" measures can be very effective in securing digital information and protecting related assets[38]. Two important and effective cyber hygiene practices that relate directly to the transferable lessons are detailed below:

- **Ensure regular updates are managed and applied in a timely manner:** software updates often include crucial patches that address security vulnerabilities. Ensure regular software updates are actioned in a timely fashion, and that there are practical governance mechanisms in place to monitor this across the organisation[39].
- **Ensure privileged account access controls are in place and well managed:** It is vital to ensure that only authorised users can access relevant data or services[40]. Good practice promotes a tiered model for administrative accounts and the privileges that come with them, limiting the greatest access to the smallest group. In general terms, turning on two-factor (2FA) or multi-factor authentication (MFA) to help prevent unauthorised access to accounts or services is a vital step. So too is policy that drives the use of strong passwords in practice[41].

37 Godage, R.D., Marriott International Data Breach 2018.
38 Cyber security breaches survey 2023 - GOV.UK
39 Cyber Hygiene: 10 Everyday Practices for Enhanced Digital Security
40 Access controls_NCSC.GOV.UK
41 Identity and access management - NCSC.GOV.UK

Theme 2:
Planning & preparedness

Lessons and recommendations concerning planning and preparedness for cyber incidents came a very close second to the theme of cyber security hygiene. The findings broadly fell into one of four categories. These are expanded with related transferable lessons below.

1. Training – awareness of cyber threats:

Organisations shared that while basic cyber security awareness training was generally in place, or at least available, the regularity and emphasis of training for all staff could have been improved. Consequently, the communication of an accurate and up to date understanding of the evolved scale and nature of threat had been insufficiently appreciated and planned for. This left staff unprepared for the requirements they went on to face in the response.

This was especially well articulated in the report following the attack on the British Library in 2023, which emphasised that 'regular training and communications on both cyber security basics and emerging risk trends was essential for all staff and should be tailored to specific roles and levels of expertise[42]. Recommendations 13 and 14 from the WannaCry report also emphasised the importance of **extending cyber awareness to Board members**, and that staff should receive regular and targeted cyber and information security awareness training **in addition to mandatory and statutory training[43].**

Report	Transferrable lessons
British Library	**Regularly train all staff in evolving risks:** All staff have a part to play in ensuring the security of the organisation. Regular training and awareness communication, covering both cyber security basics and emerging risk trends, are essential for all staff, tailored to their role and level of expertise.
Gloucester City Council	Training on the **cyber threat, data protection and file management** was not adequate. More was later implemented to cover increased information about the cyber threat, data protection and file management.
NHS England	Many of the **staff involved in the WannaCry incident had not experienced a major cyber incident before, nor had they had any preparatory training** for such an event.

2. Cyber incident planning:

Post-incident, many affected organisations remarked that the incident response plans that were in place at the time of the attack were insufficient. Most frequently, the reason for inadequate planning was rooted in either:

a. The shortcomings in all staff cyber security training (as already detailed) which had resulted in an under-developed **assessment of cyber risks. This led to inadequate planning** for the breadth, depth, and longevity of incident impacts, which repeatedly exceeded the organisation's expectations and assumptions. For example, St Helens Borough Council found that **Business Continuity plans did not generally cover the possibility of long-term ICT outages[44].**

b. The absence of specific plans for cyber incidents. Several reports articulated that an **over reliance on generalised Business Continuity and/or Disaster Recovery plans** had meant that cyber-specific plans for the event of a cyberattack had not been drawn up. In these cases, the shortcomings of generalised plans quickly became apparent and, in some cases, the response had to be worked out on the go.

Report	Transferrable lessons
Gloucester City Council	It was noted that while [existing documents and plans] were **sufficient for dealing with smaller breaches, they were not sufficient for the incident that occurred.** The impact and duration of the attack and recovery was **far more significant** than the actions in the plans were intended for.
NHS England	Business Continuity plans should include the necessary detail around response to cyber incidents and must include a clear **assessment of the impact of the loss of these services** on other parts of the [health and social care] system…these **plans must identify critical third-party services**…setting out the impact of the loss of these services on their operations and…actions required to address the loss of such services.

42 LEARNING LESSONS FROM THE CYBER-ATTACK. British Library cyber incident review
43 Lessons Learned Review: WannaCry Ransomware Attack
44 St Helens Borough Council: Managing a cyber attack

3. Cyber exercising:

The challenges in training and planning above, when reading across reports, appeared to have impacted the extent and effectiveness of cyber incident exercising. For example, planning and preparedness for the second and third order impacts of an attack tended not to have been adequately considered or rehearsed. For example, cyber attack scenarios had not always been extended to include the possibility of an attack that impacted, or indeed originated from, a third-party organisation in an important supply chain.

Report	Transferrable lessons
NHS England	Many of the **staff involved in the WannaCry incident had not experienced a major cyber incident before, nor had they had any preparatory training** for such an event.
British Library	Practice comprehensive business continuity plans: **Business Continuity plans for the total outage of all systems need to be practised regularly**, in addition to those relating to individual systems and services.
NHS England	Plans should be r**egularly tested across local areas...**and reviewed and updated locally with **board level oversight.**

4. Cyber incident detection:

In some cases, the absence of technical security features limited the preparedness of organisations to detect that they had been attacked in the first instance. This means that there was a lag between the security breach and awareness of an attack, allowing the cyber criminals more time undetected to infiltrate systems and exfiltrate data. Lessons and recommendations in this area centred on the use of Security and Information Management Systems, or other retained specialist support, to aid detection going forward.

Figure 6: Percentages of Organisations that have the following measures in place for dealing with cyber security incidents

Adapted from: Department for Science Innovation and Technology (DSIT) Cyber Breaches Survey 2024

Report	Transferrable lessons
Equifax	Equifax Left Itself Open to Attack Due to Poor Cybersecurity Practices. Equifax was unable to detect attackers entering its networks because it failed to take the steps necessary to see incoming malicious traffic online.
Gloucester City Council	GCC did not have a managed security information and event management system (SIEM) installed prior to the cyber attack. This meant that suspicious activity was not being monitored or responded to in real time. This meant that it took time for the magnitude of the attack to emerge, as cloud-hosted systems (e.g. MS Teams and Emails) were unaffected. The ransomware attack also took place over a weekend.
Scottish Environment Protection Agency	Detecting an Attack: DA.1 Threat Detection The group responsible for the attack was identified in late 2019 however there was negligible threat intelligence available on the group's Tactics, Techniques or Processes (TTP's) prior to the incident. As a result of the attack, SEPA have considered ways in which they could enhance their ability to detect cyber attacks.

Make it active: Planning for the risk of cyber incidents

The nature of the cyber threat means that the anticipation of a cyber emergency is vital. This is the latest external version of the National Security Risk Assessment (NSRA) - the government's assessment of the most serious risks facing the UK.

Acute cyber risks: Released in January 2025 the National Risk Register (NRR) - 2025 edition provides information on 89 'acute risks' (i.e., those that may require an emergency response from government) under 9 risk themes. Cyber is one of those 9 acute risk themes. Details can be found in Chapter 4 of the register, with important planning assumptions, based following risk-based scenarios:

- cyber attacks on the health and social care system
- cyber attacks on the transport sector
- cyber attacks on telecommunications systems.

These scenarios are provided in addition to assessed risks of a targeted cyber attack on critical national infrastructure (e.g., oil, gas, electricity, or civil nuclear supplies).

Chronic cyber risks: The 2025 NRR edition also details 7 chronic risk themes identified within that assessment. One of these 7 chronic risk themes is Technology and Cybersecurity, which is being driven by:

- Changes in the nature of cyber security threats
- Impacts from the use of end-to-end encryption
- Impacts from reliance on digital platforms and digital services for services and interactions

Full details of NRR 2025 Edition updates can be found on page 7 of the NRR.

Theme 3:
Cyber incident management

Cyber incident management involves activities to identify, analyse, and determine the response to cyber security incidents, to minimise immediate and long-term business impacts[45]. All documents included at least one aspect of learning that came out of the response requirements following detection of a cyber attack. Some of the lessons and recommendations in the sub-themes listed resonate with those identified in response to a range of other emergency scenarios. However, some do exhibit important cyber security nuances that warrant consideration. For example, in one case the relevant incident response plans were in place, but stored electronically on the system that was attacked. This meant that the incident response plan was unavailable for the duration. This led to the recommendation for hard paper copies to be maintained going forward.

Crisis response communications during cyber incident response were also frequently problematic. While communications can always be improved, some challenges in response were cyber-incident specific. For example, with usual means of internal communications, such as emails or instant messaging unavailable, communicating with staff was often difficult or inhibited entirely by the nature of the incident. In some cases this was exacerbated by the fact that cyber attacks often occurred just before(or in) a holiday period, or at a weekend when less staff would be around. This is a known tactic of cyber criminals.

In other cases, external communications with key stakeholders, multi-agency partners and the public were also very difficult. For example, with systems offline it made it challenging to maintain the situational awareness required to deliver effective response communications. Equivalent cyber incident/emergency roles or leads, if an organisation had one, were not always easily identified, and the delineation between the gold (strategic) and silver (tactical) command levels were not always clear. Importantly, the impacts on the people delivering the response led to the identification of learning in terms of staff resourcing and the impacts on individual wellbeing.

45 Incident management - NCSC.GOV.UK

A list of transferable lessons is provided below:

Report	Transferrable lessons
SEPA	Plans such as the **Business Continuity Plan, Disaster Recovery Plan and Cyber Incident Response Plan could not be shared during the incident as there was no offline version or hard copy available.** The plans, along with all the other files on the Storage Access Network (SAN), became unavailable as a result of the incident.
NHS England	It is [therefore] recommended that each [partnership, system, area] **identify a cyber and information security lead** from across the organisations in their locality **to ensure the coordination of cyber security issues.**
St Helens Borough Council	The different information and levels of i**nformation required by partners and other stakeholders caused frustration among the staff who spent time providing different versions of the same communications.** Future comms plans should mitigate against this, in as far as possible – work is also required to harmonise the requirements of government partners for local government bodies who have experienced attacks.
Equifax	Customer notification was delayed. It lacked timeliness and transparency: **Equifax publicly announced the data breach…six weeks after learning of it and nearly four months after the hackers entered Equifax's networks.** Because Equifax was unaware of all the assets it owned, unable to patch the Apache Struts vulnerability, and unable to detect attacks on key portions of its network, for months **consumers were unaware that criminals had obtained their most sensitive personal and financial information** and that they should take steps to protect themselves from fraud.
British Library	Proactively manage staff and user wellbeing: Cyber-incident management **plans should include provisions for managing staff and user wellbeing. Cyber-attacks are deeply upsetting** for staff whose data is compromised and whose work is disrupted, and for users whose services are interrupted.

Resources:
Did you know that there is an NCSC and UK law enforcement categorisation model for cyber incidents? It was set up in 2018 and is flexible enough to allow the full range of incidents to be categorised, from national crisis through to cyber attacks against individuals. It has **six levels of severity and is applied uniformly across all sectors** including government, critical national infrastructure, charities, universities, schools, as well as small businesses and individuals. The categorisation model can be helpful when considering the potential gravity of effects and impacts in the short and longer term response to an incident.

Theme 4: Challenges in recovery

The fourth learning theme grouped together lessons that impacted recovery from a cyber incident. These were seen in terms of the technical aspects, the human aspects, and the dynamic nature of new and evolved risks following the acute response.

- **Technical:**
  Back-ups and cloud-based services Back ups were not always kept updated or stored on a separate system/location to the original data. In other cases, a register of data assets has not been kept or maintained. This meant that it was very difficult to know what information was there in the first place, what had in fact been exfiltrated, and what the requirements for data restoration entailed.
- **Health and wellbeing:**
  The intensity of the response and its impacts on teams and individuals was also evident in this theme. For example, the NHS noted in response to the WannaCry attack that while the 'traditional nature' of major incidents tends to make them either very intense, but over within a number of hours (such as major traffic incident), or long lasting but slow moving (such as strike action), **Cyber attacks create the potential for a long running, highly intense incident[46].**

46 Lessons Learned Review: WannaCry Ransomware Attack

- **New and evolved risks in recovery:**
  The attack on the British Library highlighted the impact that incident had on organisational risk assessment more generally. This necessitated an updated review of new and specific risks to be managed during the recovery, but also removed some of the prior risk burden due to forced actions like retiring legacy IT infrastructure.

Report	Transferrable lessons
Technical challenges	
Gloucester City Council	**Not all the business applications were cloud- based or backed up to the cloud. This prolonged recovery**. The council's cloud hosted services were able to still function during the cyber attack as they were not on the same infrastructure as the rest of the servers. By distributing the hosting of services with either software-as-a-service suppliers or using specialist hosting, the risks of complete network compromise can be reduced.
Health and wellbeing challenges	
NHS England	'Within local organisations, during the incident, technical, clinical and administrative staff were very stretched in addressing the consequences of the attack. Many of these staff were required to work extended hours, including weekends and a number cancelled annual leave to support recovery'.
Managing dynamic risk	
British Library	**More than half of the risks and actions recorded on the Library's risk registers have been impacted** by the cyber-attack. Some risks have increased, either by the damage caused by the attackers, or by the inability to progress with mitigating actions. Other risks have been reduced or entirely obviated, for example by the forced retirement of ageing systems

47 Network segmentation - An introduction for health and care organisations - NHS England Digital

Theme 5: Infrastructure

This learning theme was the most technical by default. It highlighted the importance of sound IT skills and resources within an organisation. But also the high value, that organisations place on expertise that they had kept available to them on retainer. The support of national cyber security professionals, and indeed other stakeholders and agencies that had lived experience of responding to an attack, was considered invaluable.

The most problematic infrastructure issues were legacy IT systems and software, bespoke and customised applications, and a lack of effective network segmentation.

- The legacy systems were harder to maintain and secure once compatible software updates were no longer available.
- Custom applications were dependent on the varied consultants who had originally built them, but in some cases were then no longer involved.
- Poor network segmentation (see 'Sidelight' below) meant that in essence, cyber criminals who breached the system were not adequately prevented from moving across multiple areas of the wider IT network and could therefore compromise large amounts of data and services.

Sidelight: Network segmentation - NHS Digital

A properly segmented network will improve network security by limiting the 'blast radius' of any cyber-attack. It mitigates the lateral spread and impact of a malicious code across the network by:

- containing traffic within each network segment
- reducing the attack surface
- limiting the adverse impact of a cyber ecurity incident, helping organisations recover with minimal impact on patient outcomes

In addition, network performance may be improved as only authorised traffic is permitted to and from assets on the network whilst unauthorised traffic is blocked.'

Transferable lessons in this thematic area are listed below:

Report	Transferrable lessons
Infrastructure oversight	
NHS England	Recommendation 15: It is recommended that NHS Digital proactively… maintain a clear and consistent view of the technology landscape across local organisations. In the longer term, NHS Digital should have the ability to isolate organisations, parts of the country or particular services in order to contain the spread of a virus during an incident.
Applications	
Gloucester City Council: Managing a Cyber Attack	Customised applications to fit local needs caused ongoing compatibility issues between off-the shelf versions and backed-up files during recovery. Prior to the attack, the setup and configuration of some systems had been extensively customised by external consultants. During the recovery it was not possible to recover this customisation and this hampered restoration of some systems.
Legacy systems	
British Library	Manage systems lifecycles to eliminate legacy technology: 'Legacy' systems are not just hard to maintain and secure, they are extremely hard to restore. Regular investment in the lifecycle of all critical systems – both infrastructure and applications – is essential to guarantee not just security but also organisational resilience.
Gloucester City Council: Managing a Cyber Attack	The nature of the attack meant that the attackers acquired control of the domain security server and were able to move from server to server within the council's systems (lateral movement). It was recommended that network segmentation - an IT network architecture that splits the network into small segments or networks – be employed, which can increase cyber security and help prevent lateral movement within an organisation.
SEPA Internal Audit Report 2020/21 Cyber Attack Lessons Learned	Protection of assets (PA.1) Network Segmentation The network was segmented into Virtual Local Area Networks (VLANs) however there was no access control lists (ACLs) in place to filter traffic and all sites and networks could route to each other irrespective of if there was a need to or not.

Theme 6: Cyber Governance

Cyber governance was a smaller, but vitally important theme across reports. It particularly emphasised the critical role that leadership, and especially Board members have in ensuring their organisation has the understanding, expert oversight and cultural emphasis that underpin effective cyber security. This theme impressed that good cyber governance extends beyond policy review and ownership, to an understanding of the threat, strategic oversight of prevention and preparedness, and the readiness to respond in the event of an attack that may have reputational consequences. Transferable lessons in this theme are detailed below:

Report	Transferrable lessons
British Library	Cyber-risk awareness and expertise at senior level: All senior officers and Board members need to have a clear and holistic understanding of cyber-risk, in order to make optimal strategic investment choices. Current risks and mitigations should be frequently and regularly discussed at senior officer level. The recruitment of a Board member or Board-level adviser with cyber expertise is strongly recommended.
NHS England	Recommendation 5: All NHS organisations are to ensure that every board has an executive director as data security lead, cyber security risks are regularly reviewed by the board, appropriate counter-measures are in place to mitigate and response plans are in place to address service restoration in the event of a successful attack.
NHS England	Recommendation 13: Boards for NHS organisations should undertake annual cyber awareness training Recommendation 11: In addition to local boards assuring themselves that they have sufficient quality and capable IT technical resources to manage and support their local IT infrastructure, systems and services, we recommend that pooled resourcing arrangements are formalised

Make it active:
The NCSC's 'Cyber security briefing packs', which are part of the NCSC's Cyber Security Toolkit for Boards, are an excellent way to introduce the domain of 'cyber security' to non-experts. The latest version of the briefing pack was released in 2024, and includes a case study featuring Sir Roly Keating, CEO of the British Library, who shares insights on the high-profile ransomware attack that targeted his organisation. The toolkit is also available in audio transcript[48].

Conclusion

In conclusion the thematic learning from cyber incidents clearly illustrated that multiple attacks on different organisations has tended to generate similar issues upon post-incident review. In some ways, this can be taken as an encouragement, given that a number of the recurring common issues have very practical implications and opportunities for mitigation.

It is also acknowledged that there is a wealth of free support, advice and guidance available for achieving effective cyber security at home, in charities, businesses and government. Given the extent of the impacts experienced in the chronology of the attacks reviewed, and that some cited are still recovering years later, it seems pertinent to review and take advantage of it.

48 Cyber Security Toolkit for Boards: updated briefing pack... - NCSC.GOV.UK

Learning from lived experience

Personal reflections on cyber incident readiness and response

Adam Bland

Introduction

UK Resilience Academy Associate, Adam Bland, was on call for NHS England in Yorkshire and the Humber when the WannaCry cyber attack struck in 2017. In this interview article with Lianna Roast, Head of Thought Leadership, he shares what he learnt personally and professionally from the experience of responding to and recovering from the incident. He also highlights some of recurring lessons he encounters when helping organisations to develop their own cyber resilience.

Adam, thank you so much for agreeing to share your experience of managing a cyber incident with us. Can you start by telling us how long have you been working in resilience, and what influenced your decision to pursue a career in this area?

My first foray into resilience came when I became involved in the operational response to the Yorkshire floods in 2000 , whilst working for East Riding Council. However, with no real knowledge of the emergency planning and crisis management world beyond that, I pursued a different career, before finding myself in the health service shortly before the London bombings in 2005 .

Conscripted and untrained, I supported the incident response to the bombings. It was during this time that I came to understand the full extent and scope of the resilience the world. Following that experience, I became driven by a desire to never see anyone else respond to their first (or next) emergency 'conscripted and untrained'. This later led me into a full-time resilience role, which began just two weeks before the Swine Flu pandemic started in 2009. I haven't looked back since.

49 Floods leave York on edge of disaster | Environment | The Guardian
50 Report of the 7 July Review Committee
51 The first influenza pandemic of the 21st century - PMC

So, in the space of nine years, you've had first-hand experience of managing emergencies across a range of risk scenarios, including flooding, terrorism, infectious disease. If you didn't know that the world of resilience existed before – you certainly did by then! Yet you weren't a computer coder, and didn't have a background in the IT profession, so how did you end up with a keen interest and specialism in cyber resilience?

As Head of Emergency Preparedness, Resilience and Response (EPRR), I was Strategic Commander on call for NHS England in Yorkshire and the Humber the day of the WannaCry cyber attacks in 2017 . This involved coordinating the area's response to the incident, setting the local objectives, brokering resource priorities and ensuring stakeholders were kept informed of impacts and progress. WannaCry was a global cyber incident which significantly impacted England's health service. I will never forget any of the incidents I've been involved in preparing for, responding to, or recovering from. But there was something about WannaCry that seemed to highlight how ill prepared we were for what at the time was really an emerging threat. That sense of being 'conscripted and untrained' resurfaced. I also perceived there to be such a disconnect between cyber and the planning for other threats and hazards we had encountered previously. This sense of its disintegration with wider resilience endeavours became a key driver for building my interest and knowledge in cyber resilience.

What were the top two lessons that you took away, personally and professionally, from the lived experience of responding to and recovering from the WannaCry attack?

Professionally, the lesson I quickly identified was that I didn't have an off the shelf plan for a scenario like WannaCry. It wasn't an area I had particular knowledge or expertise in. However, what I did have was a good understanding and knowledge of generic incident response

structures and Joint Emergency Services Interoperability Principles (JESIP) resources . This helped enormously, because broadly - even in the context of a global cyber incident - they worked! This made me realise that as resilience professionals, we don't have to reinvent the wheel for cyber. Yes, there are some specific impacts and nuances that require specialist insight and expertise, but the universal principles of Integrated Emergency Management and JESIP can work for a cyber incident, or even a blended incident. I think we just need to integrate them better.

Personally I felt I was too slow to appreciate the human impacts of cyber-attacks, and impacts of decisions taken in response to them, on patients, on staff, on response teams, and on me. For something as intangible as cyber attack, it can be easier than one would think to focus on tangible digital impacts and consequences, rather than the consequences of those impacts. Ultimately, our planning, response and recovery for any incident should always be about people.

Almost 8 years after WannaCry, the cyber threat landscape and associated risks has clearly evolved. In your view, have the lesson we identify from cyber attacks evolved too?

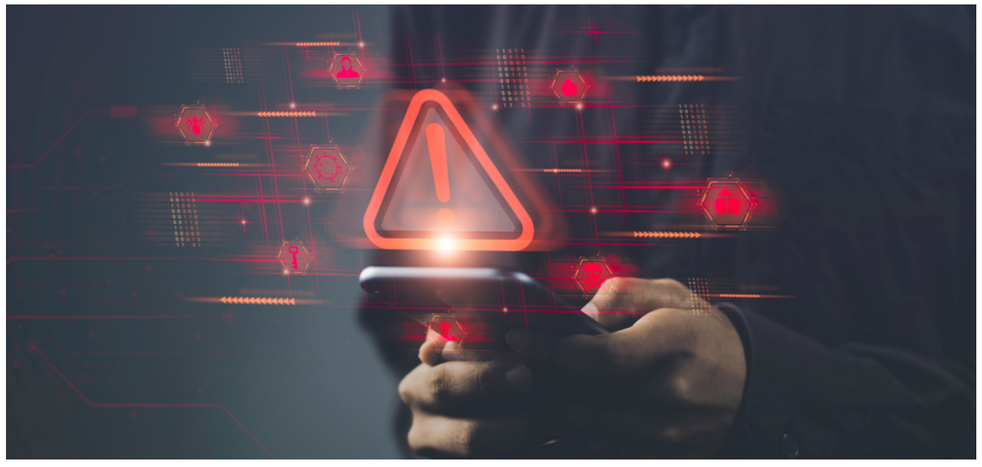
Since WannaCry, I have had the pleasure of working with organisations and teams across the UK and around the world in building their capability to respond to cyber incidents, and other risks besides. Frustratingly, I do still identify many of the same lessons that were highlighted post- WannaCry. One of the most common is one of the simplest to address, and that's continued gaps in the fundamental application of basic cyber hygiene. And I don't think this is limited to my experience. It is something we also see recurring even in recent post incident reviews. Too often, poor cyber hygiene is also coupled with a poor understanding of the consequences of a cyber incident, and a lack of alignment between cyber and 'traditional' emergency response arrangements.

52 NHS England » NHS England business continuity management toolkit case study: WannaCry attack
53 Principles for joint working - JESIP Website
54 Emergency response and recovery - GOV.UK

Why do you think this issue persists, when it's been so commonly identified over such a long period of time?

I see great examples of strong leadership in cyber resilience where teams are encouraged (often directed) to work together to break down the traditional silos of risk, business continuity, IT, cyber, supply chain, communications, and emergency preparedness. I work with boards and senior leaders that give time to teams to candidly share the risks their organisations face and ask the right questions to get an accurate picture of how ready (or not) they are to respond and recover from cyber incidents.

Equally, I see some poor examples, where a culture exists that cyber risk is the cyber team's problem or the view that 'we got through the pandemic, so our emergency planning must be ok'. This intransigence is a significant barrier to cyber resilience generally but importantly also learning the lessons. The lack of effective processes for the collection, acceptance, allocation, implementation, and monitoring of the lessons that are identified can also be an issue. Often action on lessons from cyber incidents sit across organisations, partners, suppliers - there needs to be a robust process and strong leadership to ensure these are learned and embedded.



Adam, thank you so much for sharing your own personal lived experience and professional insights with us.
Is there anything final you would like to add or share with the resilience community?

Thanks for the opportunity to share, it's been very cathartic. I think the recent NCSC annual review sums up my experiences more succinctly than I can:

"the severity of the risk facing the UK is being widely underestimated, and that the cyber security of critical infrastructure, supply chains and the public sector must improve. There is a growing disparity between the resilience of our infrastructure and the threat we face. The gap between the threat and the cyber resilience of the UK needs to close as a matter of urgency[55]."

About the author

Adam is an experienced resilience specialist. Having led organisational response and recovery to a range of incidents including severe weather, business continuity disruption, disease outbreaks, and terrorist attacks, he is passionate about developing and building resilience capability at all levels. With a wealth of knowledge and experience across all areas of crisis management, emergency preparedness, response, and recovery, he regularly helps organisations to identify lessons and embed learning, to maximise opportunities for working differently.

Adam Bland
Senior Associate, UK Resilience Academy

55 NCSC Annual Review 2024

Beyond prevention: minimising cyber impact in local government

Local Government Association

Beyond prevention: minimising cyber impact in local government

Introduction

The Local Government Association (LGA) is the national voice of local government. They are also the membership body for local authorities in England. They work with county and district councils, metropolitan and unitary councils, London boroughs, and Welsh unitary councils (with the Welsh Government Association), to support, promote and improve local government. This includes the commitment to improve the secure use of digital technology by councils and communities.

In this article, **Councillor Alex Coley Deputy Chair of LGA's Improvement and Innovation Board and part of Intelligent Council Services**, sets the cyber threat in the context of local councils and emphasises the importance of impact mitigations. He also draw on one of three cyber incident case studies that the LGA have compiled to help share experiences and learning across their local members.

About Local Government

Local government is responsible for a range of vital services for people and businesses in defined areas. Among them are well known functions such as social care, schools, housing and planning and waste collection. In England, more than one million people work in local government across a range of different types of authorities, providing more than 800 different services to local communities[56].

Targeted cyber attacks in Local Government

It is now broadly understood that cyber-attacks on local government are a matter of 'when' not 'if'. Recent attacks, such as those on Gloucester and Hackney, highlight the urgent need for a greater focus on impact mitigation. Even national institutions for example, Transport for London and the British Library have been targeted, demonstrating the increasing sophistication and frequency of cyber-attacks.

The Local Government Association (LGA) has been championing the secure use of digital technology in councils since 2019. Over the past five years the support has grown in maturity, just as the sector's approach to cyber security has. Initial efforts focused on bolstering cyber defences by addressing procedural, human, and technological vulnerabilities. However, recent incidents emphasise the need to go beyond prevention and prioritise impact mitigation.

Councils hold a treasure trove of sensitive data, from social care records to financial information, making it a prime target for cybercriminals. The critical nature of council services often demands uninterrupted operation, amplifying the potential impact of disruption. For Gloucester, it took four months for the council to fully restore all its systems and services.

The importance of impact mitigation

While preventative controls like firewalls, segregations, and training are vital, eliminating all vulnerabilities is impossible. Councils must prioritise **impact mitigation** to build true cyber resilience. This involves robust crisis management, incident response, disaster recovery, and business continuity planning.

---

56 What is Local Government?

Effective mitigation starts with a comprehensive understanding of assets and their associated risks. This includes identifying all data (including unstructured data), systems, and applications, establishing clear ownership for each asset, and conducting a thorough risk assessment based on its criticality and vulnerability.

Resource constraints are a common challenge for councils. Impact mitigation solutions must be cost-effective, prioritising the most critical assets and services. This may involve focusing resources on protecting the most essential services and data to achieve cost-effective scalability and redundancy.

Responding and recovering from cyber incidents

Formalising response and recovery procedures for an attack is essential. This includes developing strategic crisis management and business continuity plans, detailed cyber incident response and disaster recovery plans for IT teams, and business continuity plans for each service area to ensure the maintenance of essential operations during disruptions. Gloucester's attack impacted a wide range of services, including benefits payments, planning applications, and housing services. The interconnected nature of council systems drives the potential for widespread disruption.

Testing and exercising

Crucially, these plans must be aligned and regularly tested through exercises to identify gaps and ensure coordinated execution. Analysing past incidents, such as the ransomware attack on Gloucester City Council in December 2021 , offers valuable insights into how these attacks work. In Gloucester's case, the attack disrupted critical services by encrypting servers, highlighting the importance of robust data backup and recovery procedures. The council's response, documented in a detailed case study available on the LGA website, provides a valuable learning opportunity for other local authorities. Their experience emphasises the importance of effective communication with the public, staff, and partners during an incident, and the need for strong leadership to guide recovery efforts.

By shifting focus to impact mitigation and learning from real-world incidents like Gloucester's, local governments can build resilience and minimise the disruption caused by inevitable cyber-attacks.

About the author:

Alex is the Deputy Chair of the Improvement and Innovation Board at the LGA. A former civil servant in Cabinet Office and Head of Digital at the Met Police, he has worked in digital for two London councils and an NHS charity. Alex also worked as a Technical Strategist for a digital agency, horizon scanning for new AI technology.

Alex Coley
Deputy Chair of LGA's Improvement and Innovation Board

Resources

For an overview of the LGA's cyber support and assistance to councils, including blueprints and actions that can help you develop and exercise your plans, please visit our Cyber, Digital and Technology Hub.

57 Gloucester City Council – Managing a Cyber Incident

Building resilience against AI - enabled deception

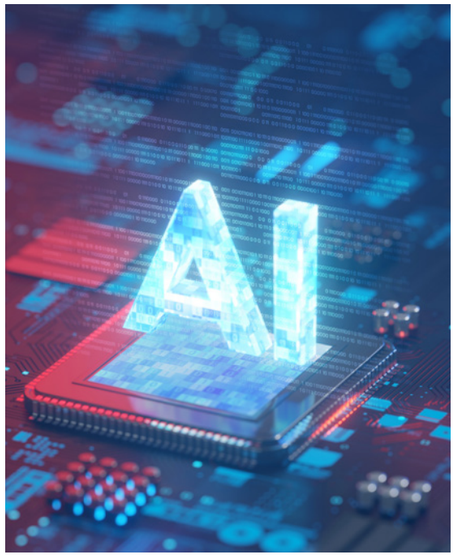
Di Cooke
Kings College London

Introduction

Artificial Intelligence (AI) offers incredible potential and positive, applied opportunities in a range of contexts and settings. However, it has also created new and evolving means for those with malicious intent to exploit cyber infrastructures, and to exacerbate the problem of whether we can trust online content . Whether repurposed to disrupt, deceive, or even manipulate the democratic process, associated cyber security risks require consideration when working to build cyber resilience. In this article Di Cooke, a Fellow at the Center for Strategic and International Studies (CSIS) and researcher at Kings College London, shares her academic insights and expertise on the risks that Artificial Intelligence brings into the cyber security landscape. She also signposts practical tips and helpful resources for managing AI risks in the context of cyber incident planning.

The rise of generative AI

The National Cyber Security Centre defines Artificial Intelligence (AI) as computer systems that can perform tasks usually requiring human intelligence. Generative AI technology is a category of artificial intelligence models used to create synthetic content (popularly known as 'deepfakes'), which are AI-generated or manipulated digital images, audio, video, and text.



This includes deepfake videos, cloned voices, and manipulated images. Popular examples of these tools include ChatGPT for text, Stable Diffusion for images, and Eleven Labs for voice cloning software.

58 Preserving integrity in the age of generative AI - NCSC.GOV.UK

The rise of generative AI technology has dramatically enhanced threat actors' abilities to create sophisticated deceptions that can fool even the most vigilant individuals and organizations. These AI-powered tools can now generate hyper-realistic fake videos, clone voices, manipulate images, and craft convincing text—all at a fraction of the cost and effort previously required. Recent incidents have found threat actors are increasingly leveraging these capabilities to commit highly targeted or large-scale fraud, interfere in political elections, create non-consensual intimate media of adults and children, and more.

The current threat landscape

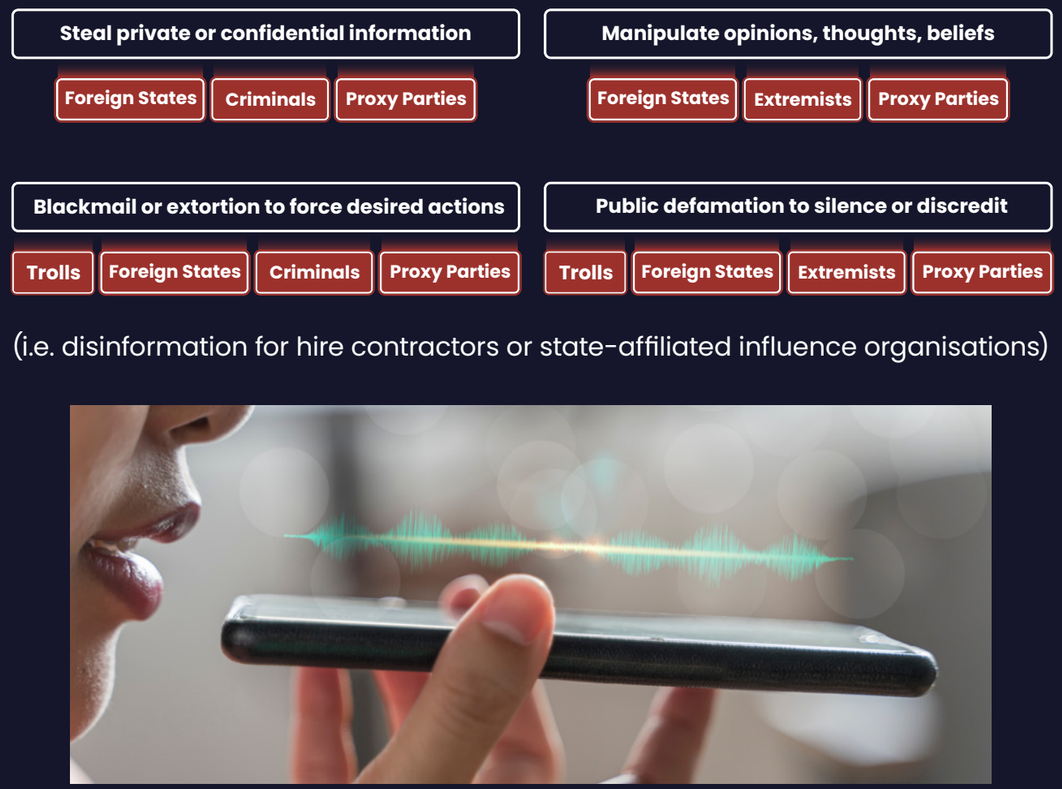
Threat actors increasingly leverage generative AI to enhance their deceptive attacks across multiple fronts. Generative AI-enabled attacks involve varied actors and motivations, as visualised in Figure X. They are becoming a more serious threat due to three key developments:

- Increasing widespread accessibility of commercial or open-source AI tools.
- Less data than ever is required - just seconds of audio and a few photos can create convincing synthetic content.
- Dramatically improved realism of synthetic content, making detection increasingly difficult.

Some of the most prevalent types of generative AI attacks include:

- **Phishing:** AI-generated emails and messages tailored to specific targets
- **Voice Fraud:** Cloned voices used for financial scams or social engineering
- **Video Impersonation:** Deepfake videos of executives or public figures
- **Biometric Spoofing:** Synthetic faces/voices to bypass security systems
- **Financial Scams:** Impersonating trusted figures to authorize transfers
- **Online Personas:** Creating fake identities for espionage/ manipulation
- **Harassment:** Generating harmful synthetic content to humiliate or harm
- **Election Interference:** Using deepfakes to spread disinformation

Figure 7: A visualisation of the varied actors and motivations involved in generative AI-enabled attacks



(i.e. disinformation for hire contractors or state-affiliated influence organisations)

Notable examples of generative AI-enabled attacks include:

- Stealing £20 million using a CEO's cloned voice and video to trick a company employee
- Impersonating Kyiv Mayor Klitschko in a series of video conference meetings with prominent European city Mayors
- Extorting or scamming people over the phone using AI voices of the targets loved ones
- Encrypted messaging apps being used to circulate sexually explicit images of girls and young women.

Planning for and protecting against generative AI risks

Current deepfake detection tools have high failure rates and frequently misidentify both authentic and synthetic content. This makes them unreliable as a primary defence against AI-enabled deception.
A strong defence against AI-enabled deception requires **a multi-layered approach that incorporates threat awareness, cyber hygiene, and escalation protocols.**

Sidelight:
But is it real? Unreliable Human Perception

Research has found that humans can now only correctly identify AI-generated content about 50% of the time - roughly equivalent to a coin flip. This makest it essential to rely on alternative verification processes rather than visual or auditory judgment alone.

Individuals can:

1. Regularly educate themselves on AI threats to remain aware of the rapidly changing landscape. To make it harder to be a target, carefully manage your digital presence by limiting personal information online - ensuring family and colleagues also practice good digital security is also critical.
2. Practice strong cyber hygiene, such as checking sensitive requests through multiple channels of communication, setting up a passphrase with coworkers and family, and using two-factor authentication.

Organisations can support by:

1. Facilitating awareness through regular training on AI threats and how to spot synthetic content. This includes keeping staff updated on new capabilities and attack methods.
2. Identifying useful tools and techniques to help fact-check and cross-reference information to discern better if digital content is real or fake.
3. Ensure there are clear protocols for personnel to report suspicious activity, practice good cyber hygiene, and implement a rapid response plan for handling incidents. Organisations should practice their response plans regularly and learn from each incident to improve in the future.

About the author

Di Cooke is an AI Fellow at the Center for Strategic and International Studies (CSIS) in Washington, D.C and a Researcher at the Center for Science and Security Studies at King's College London. Her research focuses on the AI threat landscape and its implications for national security.

Di Cooke

Make it active

- **Visit:** the NCSC have developed guidance to help managers, board members and senior executives (with a non-technical background) to understand some of the risks - and benefits - of using AI tools
- **Ask:** your IT and security teams whether current cyber hygiene protocols and incident response plans account for AI attacks. If so, how?
- **Request:** briefings on the current threat landscape and protection processes.
- **Read:** more about the Generative AI threat landscape, in Di Cooke's article "Crossing the Deepfake Rubicon".

Resources

Topical reports and resources

Artificial Intelligence: Accelerated Capability Environment (ACE)

ACE is a unit within the Homeland Security Group tackling public safety and security challenges arising from evolving digital and data technology. They create innovative solutions through collaboration with public and private sectors to deliver impact to those on the front line .

On 5th February 2025, ACE published a case study titled 'Innovating to detect deepfakes and protect the public' on gov.uk. Its focus is on finding collaborative ways to mitigate the growing threat from AI-generated deepfakes, as an urgent national priority. To find out more and read about the biggest recent event in this space - the Deepfake Detection Challenge follow this link.

Categorising UK cyber incidents

Cyber incidents can be categorised depending on its severity and potential impact on the UK. The NCSC and UK law enforcement categorisation model for cyber incidents provides descriptions of attacks under: (1) National cyber emergency; (2) Highly significant incident; (3) Significant incident; (4) Substantial incident; (5) Moderate incident; and (6) Localised incident. Full details are available on the NCSC website

59 Cyber Assessment Framework - NCSC.GOV.UK

Cyber Assessment Framework

NCSC's CAF collection is for all organisations that are responsible for securing critical network and information systems that keep our businesses, citizens and public services protected.[59]This includes:

- Organisations subject to the Network and Information (NIS) Regulations
- Organisations within the UK Critical National Infrastructure (CNI)
- Organisations managing cyber-related risks to public safety
- Public sector organisations that support core government functions
- Other organisations / sectors that may find the CAF a useful tool

It is intended to assist organisations to carry out some of their core oversight responsibilities.

Cyber attack case studies

Are range of cyber attack case studies can be found on the National Cyber Security Centre's website

Cyber crime

For more information on the cyber threat and to the UK from serious and organised crime, visit the National Crime Agency's cybercrime pages.

Cyber knowledge

The **Cyber Security Body of Knowledge (CyBOK)**, a comprehensive collection of material collated from a variety of recognised experts and organisations, to inform and underpin education and professional training for the cyber security sector. CyBOK **is detailed at** https://www.cybok.org/

Cyber-security in Defence

For an **extended overview of cyber fundamentals**, threats, functions and operations in the defence context, see the Cyber Primer 3rd Edition, October 2022 from the Ministry of Defence.

Futures toolkit for policymakers and analysts (2024)

The updated 2024 version of the Futures Toolkit from Government Office for Science provides a set of tools to help develop policies and strategies that are robust in the face of an uncertain future. The toolkit can be used in a variety of contexts, including the development of cyber resilience. It sits alongside other GO-Science futures resources, including their Brief Guide to Futures Thinking and Foresight, and Trend Deck.

National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) 2.0

The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce. NIST's Cyber Security Framework (CSF) 2.0 is organised by six Functions — Govern, Identify, Protect, Detect, Respond, and Recover. Together, these Functions provide a comprehensive view for managing cybersecurity risk.

The CSF 2.0 is comprised of: CSF Core - A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks; and CSF Organizational Profiles - A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes. • CSF Tiers - Can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices.

A helpful Resource & Overview Guide provides a good starting point for learning more about the CSF.

Wider learning & reports

- Grenfell Tower Inquiry: A statutory public inquiry, formally established in August 2017, to examine the circumstances leading up to and surrounding the fire at Grenfell Tower on the night of 14 June 2017. The inquiry published its second and final Phase 2 report on 4 September 2024.
- Government published their response to the Grenfell Tower Inquiry's Phase 2 report on 26 February 2025. The response sets out the steps government are taking to implement the report's recommendations at pace, as well as the wider work they are doing to make buildings safer.

  A summary of the government's response is also available in 11 languages.
- UK Covid 19 Inquiry An Inquiry to examine the UK's response to and impact of the Covid-19 pandemic and learn lessons for the future. On 18th July 2024 the Inquiry published its first report, Module 1 – on the United Kingdom's 'Resilience and Preparedness'. The report identifies a range of lessons and makes **10 key recommendations** in response.

  The UK government published their response to the Covid-19 Inquiry Module 1 report on resilience and preparedness, on 16 January 2025.

Accident Investigation Branches

- The Rail Accident Investigation Branch (RAIB) is the independent railway accident investigation organisation for the UK. Amongst other publications, RAIB has produced, and continues to update, a series of summaries of the learning that has come out of our investigations into accidents and incidents in nine topic area
- The Air Accident Investigation Branch (AAIB) provides assistance and expertise to international air accident investigations and organisations. Their purpose is to improve aviation safety by determining the circumstances and causes of air accidents and serious incidents and promoting action to prevent reoccurrence. AAIB monthly bulletins and investigation reports are available online.
- The Marine Accident Investigation Branch (MAIB) investigates marine accidents involving UK vessels worldwide and all vessels in UK territorial waters. This is to help prevent further avoidable accidents from occurring, not to establish blame or liability. MAIB recently published their Annual Report 2023. This includes recommendations issued in 2023 and an update on their status.

Table of Transferable Lessons

Theme 1: Cyber Incident management	
Report	**Transferrable lessons**
GCC	Generalised Business Continuity Plans meant that there was **no specific cyber incident plan** that incorporated a communications plan.
SEPA	Plans such as the Business Continuity Plan, Disaster Recovery Plan and Cyber Incident Response Plan **could not be shared during the incident as there was no offline version or hard copy available.** The plans, along with all the other files on the Storage Access Network (SAN), became unavailable as a result of the incident.
NHS England	One of the key lessons of attack was the **interconnected nature** of health and social care organisations in England, whereby the actions taken by one organisation have a direct impact on others. It is therefore recommended that each [partnership, system, area] **identify a cyber and information security lead** from across the organisations in their locality **to ensure the coordination of cyber security issues.**
St Helens Borough Council	Communications during the incident could have been more coordinated. Local lessons learned **reports highlight the difficulty of managing communications between local organisations** during the incident.
St Helens Borough Council	The different information and levels of **information required by partners and other stakeholders caused frustration among the staff who spent time providing different versions of the same communications.** Future comms plans should mitigate against this, in as far as possible – work is also required to harmonise the requirements of government partners for local government bodies who have experienced attacks.
St Helens Borough Council	The **delineation between the gold (strategic) and silver (tactical)** command levels of the IRT was not clear to all staff so this will need to be reviewed and clarified.
Equifax	Customer notification was delayed. It lacked timeliness and transparency: Equifax publicly announced the data breach…**six weeks after learning of it and nearly four months after the hackers entered Equifax's networks.** Because Equifax was unaware of all the assets it owned, unable to patch the Apache Struts vulnerability, and unable to detect attacks on key portions of its network, for months **consumers were unaware that criminals had obtained their most sensitive personal and financial information** and that they should take steps to protect themselves from fraud.

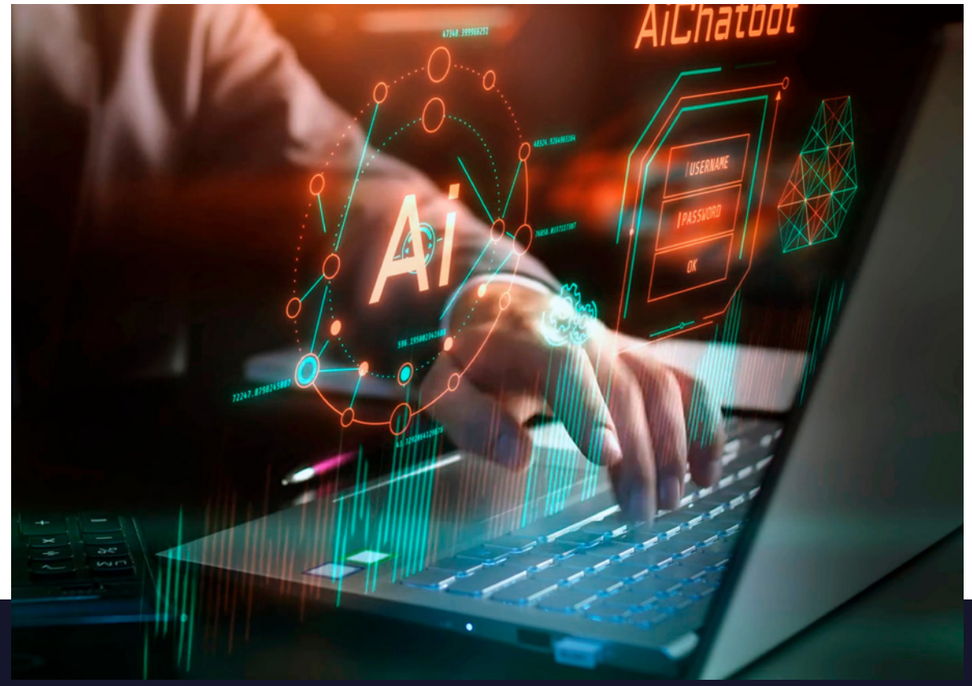
Theme 2: Cyber security and hygiene	
Report	**Transferrable lessons**
Marriott	Marriott used an **outdated version of software, which had known vulnerabilities** that the attackers were able to exploit.
Equifax	Equifax had **no standalone written corporate policy governing the patching of known cyber vulnerabilities** until 2015. After implementing this policy, Equifax conducted an audit of its patch management efforts, which identified a backlog of over 8,500 known vulnerabilities that had not been patched.
SEPA	Many employees had administrative accounts to facilitate their roles. However, **Privileged Account management controls required improvement.** Once compromised, this vulnerability had facilitated lateral movement during the attack, and privilege escalation.
SEPA	Authentication Password policy was not sufficiently secure. **Multifactor authentication (MFA) was not used**, or inconsistently used.
NHS England	All reviews of the WannaCry attack have noted that the **vulnerabilities that were exploited could have been addressed through good IT management control.** …Over half of local NHS organisations reported they **had not patched systems** when required due to concerns about the impact of the necessary downtime on clinical services.

Theme 3: Cyber incident Management	
Report	**Transferrable lessons**
SEPA	Plans such as the **Business Continuity Plan, Disaster Recovery Plan and Cyber Incident Response Plan could not be shared during the incident as there was no offline version or hard copy available.** The plans, along with all the other files on the Storage Access Network (SAN), became unavailable as a result of the incident.
NHS England	It is [therefore] recommended that each [partnership, system, area] **identify a cyber and information security lead** from across the organisations in their locality **to ensure the coordination of cyber security issues.**
St Helens Borough Council	The different information and levels of i**nformation required by partners and other stakeholders caused frustration among the staff who spent time providing different versions of the same communications.** Future comms plans should mitigate against this, in as far as possible – work is also required to harmonise the requirements of government partners for local government bodies who have experienced attacks.
Equifax	Customer notification was delayed. It lacked timeliness and transparency: **Equifax publicly announced the data breach…six weeks after learning of it and nearly four months after the hackers entered Equifax's networks.** Because Equifax was unaware of all the assets it owned, unable to patch the Apache Struts vulnerability, and unable to detect attacks on key portions of its network, for months **consumers were unaware that criminals had obtained their most sensitive personal and financial information** and that they should take steps to protect themselves from fraud.
British Library	Proactively manage staff and user wellbeing: Cyber-incident management **plans should include provisions for managing staff and user wellbeing. Cyber-attacks are deeply upsetting** for staff whose data is compromised and whose work is disrupted, and for users whose services are interrupted.

Theme 4: Challenge in recovery	
Report	**Transferrable lessons**
Technical challenges	
Gloucester City Council	**Not all the business applications were cloud- based or backed up to the cloud. This prolonged recovery.** The council's cloud hosted services were able to still function during the cyber attack as they were not on the same infrastructure as the rest of the servers. By distributing the hosting of services with either software-as-a-service suppliers or using specialist hosting, the risks of complete network compromise can be reduced.
Health and wellbeing challenges	
NHS England	'Within local organisations, during the incident, technical, clinical and administrative staff were very stretched in addressing the consequences of the attack. Many of these staff were required to work extended hours, including weekends and a number cancelled annual leave to support recovery'.
Managing dynamic risk	
British Library	**More than half of the risks and actions recorded on the Library's risk registers have been impacted** by the cyber-attack. Some risks have increased, either by the damage caused by the attackers, or by the inability to progress with mitigating actions. Other risks have been reduced or entirely obviated, for example by the forced retirement of ageing systems

Theme 5: It Infrastrcuture	
Report	**Transferrable lessons**
Infrastructure oversight	
NHS England	Recommendation 15: It is recommended that NHS Digital proactively… maintain a clear and consistent view of the technology landscape across local organisations. In the longer term, NHS Digital should have the ability to isolate organisations, parts of the country or particular services in order to contain the spread of a virus during an incident.
Applications	
Gloucester City Council: Managing a Cyber Attack	Customised applications to fit local needs caused ongoing compatibility issues between off-the shelf versions and backed-up files during recovery. Prior to the attack, the setup and configuration of some systems had been extensively customised by external consultants. During the recovery it was not possible to recover this customisation and this hampered restoration of some systems.
Legacy systems	
British Library	Manage systems lifecycles to eliminate legacy technology: 'Legacy' systems are not just hard to maintain and secure, they are extremely hard to restore. Regular investment in the lifecycle of all critical systems – both infrastructure and applications – is essential to guarantee not just security but also organisational resilience.
Gloucester City Council: Managing a Cyber Attack	The nature of the attack meant that the attackers acquired control of the domain security server and were able to move from server to server within the council's systems (lateral movement). It was recommended that network segmentation - an IT network architecture that splits the network into small segments or networks – be employed, which can increase cyber security and help prevent lateral movement within an organisation.
SEPA Internal Audit Report 2020/21 Cyber At-tack Lessons Learned	Protection of assets (PA.1) Network Segmentation The network was segmented into Virtual Local Area Networks (VLANs) however there was no access control lists (ACLs) in place to filter traffic and all sites and networks could route to each other irrespective of if there was a need to or not.

Theme 6: Cyber Governance	
Report	**Transferrable lessons**
British Library	Cyber-risk awareness and expertise at senior level: All senior officers and Board members need to have a clear and holistic understanding of cyber-risk, in order to make optimal strategic investment choices. Current risks and mitigations should be frequently and regularly discussed at senior officer level. The recruitment of a Board member or Board-level adviser with cyber expertise is strongly recommended.
NHS England	Recommendation 5: All NHS organisations are to ensure that every board has an executive director as data security lead, cyber security risks are regularly reviewed by the board, appropriate counter-measures are in place to mitigate and response plans are in place to address service restoration in the event of a successful attack.
NHS England	Recommendation 13: Boards for NHS organisations should undertake annual cyber awareness training Recommendation 11: In addition to local boards assuring themselves that they have sufficient quality and capable IT technical resources to manage and support their local IT infrastructure, systems and services, we recommend that pooled resourcing arrangements are formalised

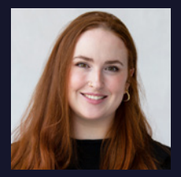


Acknowledgements

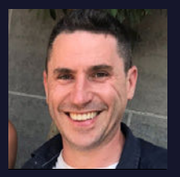
Acknowledgements

The UK Resilience Lessons Digest has been commissioned by government, and researched and designed by the UK Resilience Academy, in collaboration with the Cabinet Office Resilience Directorate, JESIP's Joint Organisational Learning Team, central Government Departments and local practitioners.

The Digest team would like to thank Lianna Roast, colleagues working in Critical National Infrastructure, the National Cyber Security Centre, and our contributing authors:



Di Cooke



Alex Coley

Adam Bland

Jonathon Ellison

Lianna Roast

UK Resilience Academy