UK Resilience Academy

UK Resilience Lessons Digest

Learning from Cyber Incidents

Issue 6 | April 2025

UK Resilience Academy

Welcome

Please put any questions in the chat

This session is being recorded

Operated by

serco

National Cyber Security Centre
a part of GCHQ

Opening Keynote

Jonathon Ellison OBE

Director, National Resilience

National Cyber Security Centre (NCSC)

UK Resilience Academy

UK Resilience Lessons Digest

Introduction

Lianna Roast

Head of Thought Leadership, UK Resilience Academy

UK Resilience Academy

Purpose

The UK Resilience Lessons Digest is part of the Government's commitment to strengthen societal resilience. 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.

Objectives

- **Summarise** transferable lessons and themes from a range of relevant sources
- **Share** lessons across responder organisations and wider resilience partners
- **Coordinate** knowledge to drive continual improvements in doctrine, standards, good practice, training and exercising

Practice

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.

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.

https://ukresilienceacademy.org/resources/uk-resilience-academy-launch-event/

Welcome to the UK Resilience Academy (UKRA), formerly the Emergency Planning College (EPC)

Introduction to resilience | About UKRA | Contact UKRA | View courses

UK Resilience Academy

Learn | Validate | Develop | Collaborate | Share

Share

Knowledge, resources & tools to help you, your team or your organisation to become more resilient

Find out more about Share

Resources

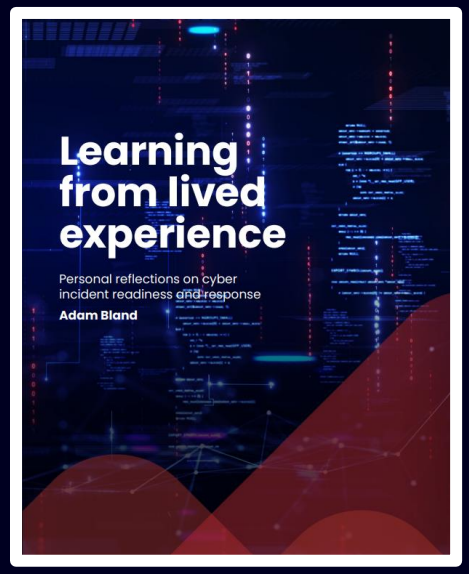
Exercising hub

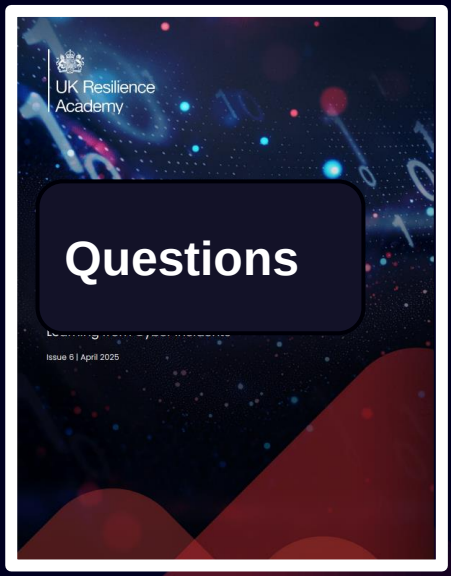
News & Insights

Lessons Digest

Session overview

1 2 3 4 5

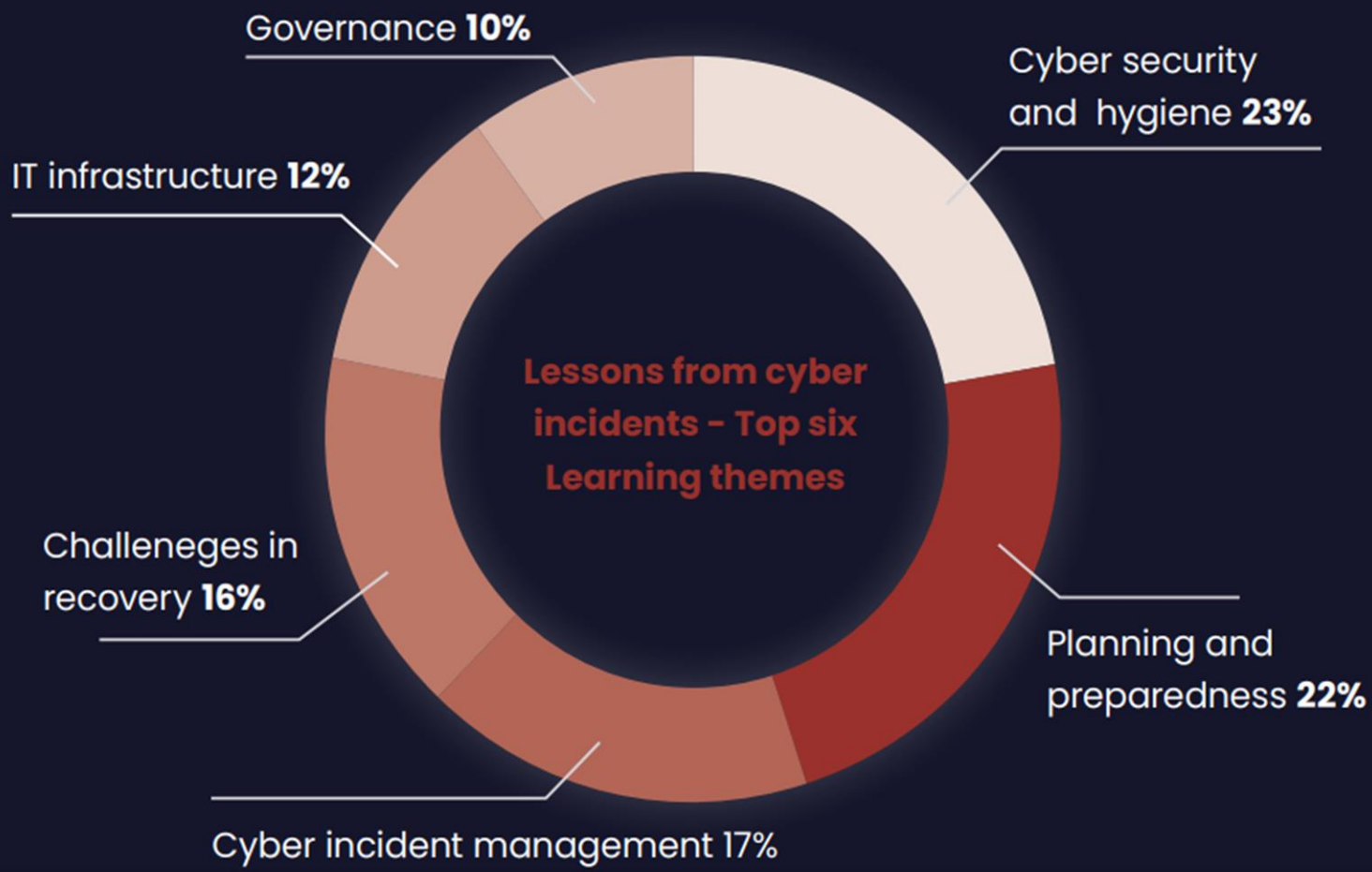




Lessons from cyber incidents

- A total of seven documents selected for the analysis.
- Each detailed learning from a significant, high-profile, cyber incident. Attacks were sectorially diverse and employed different methods
- All incidents occurred within the last six years (2017 – 2023), with direct or indirect impacts for UK citizens, services and/or business franchises.
- Combined total of 100 findings, lessons and recommendations were reviewed

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



Theme 1:
Cyber security hygiene

- Basic, routine practices that help to maintain the ‘health’ and security of an IT system
- The measures that might have reduced the severity of an incident’s impacts, or perhaps mitigated an attack altogether, were often recognised as routine or readily available
- Patching, Multifactor authentication (MFA), outdated software

Theme 2:
Planning & preparedness

- Basic training - evolved scale and nature of threat had been insufficiently appreciated
- Inadequate planning - breadth, depth, and longevity of incident impacts, which repeatedly exceeded the organisation’s expectations and assumptions
- Over reliance on generalised Business Continuity and/or Disaster Recovery plans
- All impacted the extent and effectiveness of cyber incident exercising

Theme 3:
Cyber incident management

- Cyber-incident specific - plans stored electronically on the system that was attacked
- Cyber-incident specific - Internal and external communication challenges, impairing the situational awareness required to deliver effective response communications
- Exacerbated by the fact that cyber attacks often occurred just before(or in) a holiday period, or at a weekend

Theme 4:
Challenges in recovery

- Technical: back-ups stored on the system affected, rather than alternative and lack of data asset register
- Traditional major incidents either very intense, but over within a number of hours, or long lasting but slow moving, but cyber attacks have potential to be long running and highly intense

Theme 5:
Infrastructure

- Legacy systems were harder to maintain and secure
- Custom application dependent on the varied consultants who had originally built them
- Poor network segmentation meant that criminals were not adequately prevented from moving across multiple areas of the wider IT network

Theme 6:
Cyber Governance

- Leadership, and especially Board members, have critical role in ensuring their organisation has the understanding, expert oversight and cultural emphasis that underpin effective cyber security.

Beyond Prevention:

Minimising cyber impact in government

Councillor Alex Coley

Deputy Chair, Improvement and Innovation Board

Local Government Association

UK Resilience Academy

The Inevitability of Cyber-Attacks

Cyber-attacks are no longer a matter of "if" or "when", but “how often” for local government.

- Gloucester and Hackney highlight the urgent need for a greater focus on impact mitigation.

- **Gloucester case**
  - Gloucester City Council hit by a sophisticated ransomware attack in December 2021, initiated through a spear-phishing email that led to malware deployment and data exfiltration.
  - The attack significantly disrupted critical council services, including benefit payments and planning, with some systems taking up to a year for full restoration.
  - The incident incurred over £1.1 million in costs and involved the potential exfiltration of approximately 240,000 files, though law enforcement indicated a low risk of publication
  - The council chose a complete system rebuild and migration to cloud-hosted solutions rather than paying the ransom, aiming for enhanced security and resilience.

- **Key lessons:**
  - necessity of a specific cyber incident plan,
  - enhanced staff training on cyber threats, and careful engagement with external suppliers.

Local Government as a Prime Target for Cybercriminals

- Councils hold a "**treasure trove**" of sensitive data, ranging from social care records to financial information.
- The **critical nature of council services** demands uninterrupted operation, amplifying the potential impact of disruption from an attack.
- The Gloucester incident, where full system and service restoration took **four months**, exemplifies the potential for significant disruption.

The Critical Importance of Impact Mitigation in addition to Prevention

• While preventative controls (firewalls, segregation, training) are vital, eliminating all vulnerabilities is impossible. **Councils must prioritise impact mitigation to build true cyber resilience.**

• Involves robust crisis management, incident response, disaster recovery, and business continuity planning.

• Involves architectural design. Gloucester chose a complete system rebuild and migration to cloud-hosted solutions.

Standardised vs. Bespoke IT: The Recovery Challenge

Learning from Cyber Incidents: A Shared Experience Approach

- The Local Government Association (LGA) has championed the **secure use of digital technology** in councils since 2019.

- The LGA has compiled **cyber incident case studies**, such as the one discussed in this article, to share experiences and learning amongst local government.

- This approach helps councils understand and implement **effective mitigation** measures based on real-world scenarios.

- Effective mitigation requires understanding **and assessing assets, identifying critical data, and implementing clear ownership for security**.

Learning from lived experience

Personal reflections on cyber incident readiness and response

Adam Bland

Senior Associate, UK Resilience Academy

UK Resilience Academy

WannaCry ransomware attack (2017)

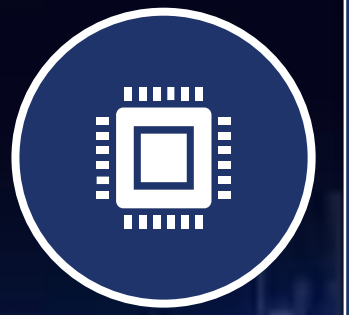
Strategic Commander on call for NHS England in Yorkshire and the Humber

- This was a **known risk** but no plans or training in place for emergency response
- The potential **scale and impact** was not well assessed or documented
- The vulnerability was known, and a **patch was available**

Personal reflections - readiness

This threat needs urgency - plan for it happening now, not when or if.	**The response needs urgency** - don't wait, go big and fast. Scale back if not needed.	Put the **human impacts front and centre** - recovery is long

Personal reflections - response



It helps to **know 'enough' about cyber resilience** and IT but ensure you've got access to **Subject Matter Experts (SMEs)**	It helps for **SMEs to know 'enough' about emergency response** to work within tried and tested processes and structures	In the absence of specific plans and playbooks, **fall back on universal approaches: JESIP Principles for joint working**

Building resilience against AI - enabled deception

Di Cooke

AI Fellow, Center for Strategic and International Studies (CSIS)
Researcher, Kings College London (KCL)

UK Resilience Academy

Weaponised Synthetic Content

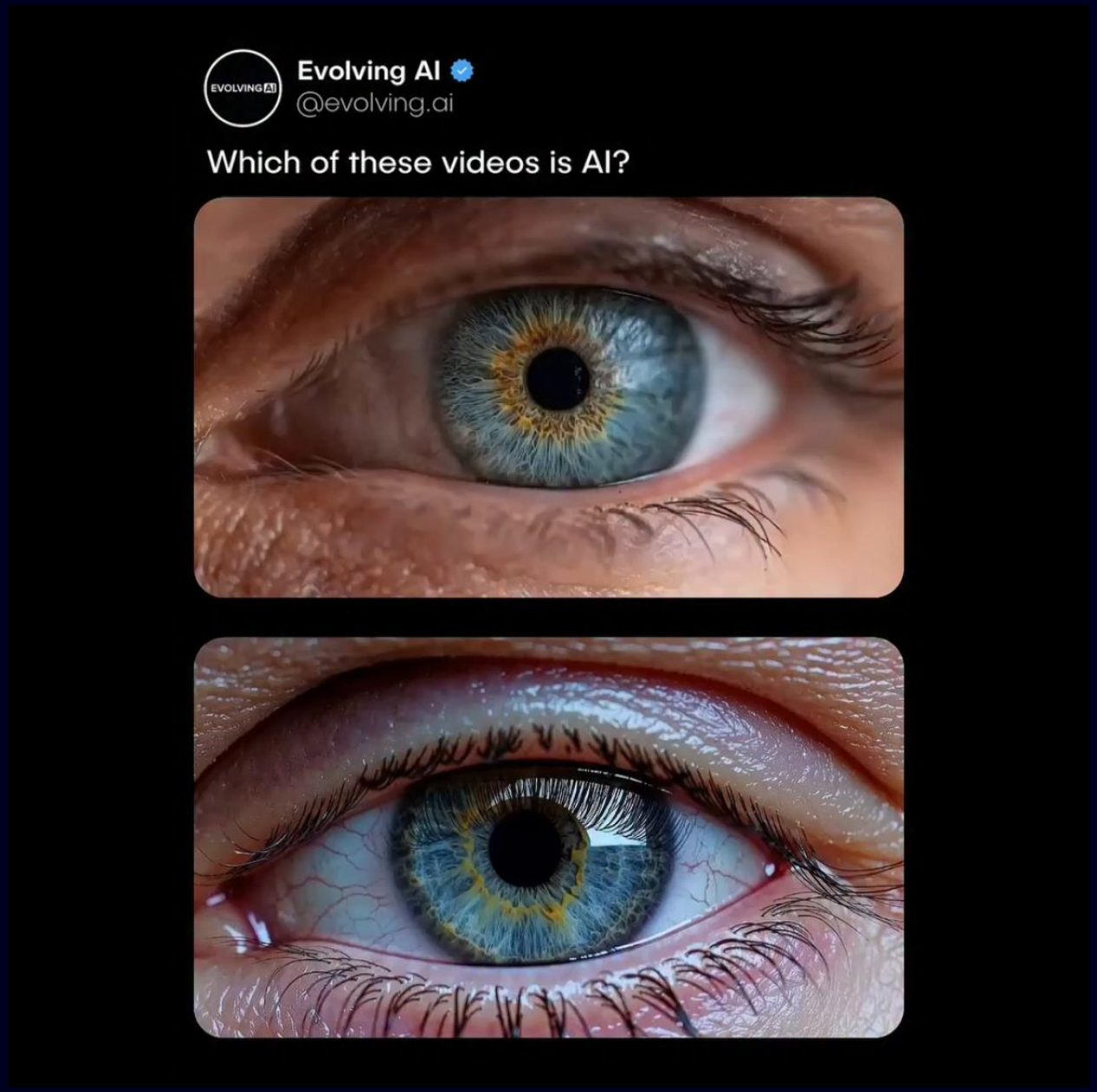
A Clear and Present Danger

A rapidly expanding threat landscape

- Synthetic content has been weaponised for a growing number of malicious purposes, including for election interference, financial fraud, CASM and non-consensual intimate media creation, grey zone warfare, espionage and surveillance, military deception, sextortion & blackmail, and more.

AI-enabled cyberattacks

- Generative AI technology enables threat actors to conduct more sophisticated and large-scale cyber attacks at an increasingly accelerated pace than ever before
- Proliferation of AI-enabled cyberattacks in recent years has been widely attributed to threat actors' employment of this technology


Evolving AI
@evolving.ai
Which of these videos is AI?

Cyber Attack Incidents

- **Voice-phishing**

AI voice cloning technology used to impersonate individuals to scam financial institutions and individuals

442% increase in voice-phishing in 2024 has been driven by generative AI technology

- **Insider threats**

Espionage campaigns, such as in 2024 when North Korea where state-affiliated agents created synthetic identities for remote job interviews

One successfully hired actor was later caught loading malware onto company equipment

- **Malware**

Using generative AI to create sophisticated malware such or dissemination of generative AI tools offering sophisticated attack capabilities

AsyncRAT, ranked 10th most prevalent malware globally, was created using the support of generative AI tools

Popular generative AI cybercrime tools include WormGPT and FraudGPT

Building Resilience Against AI-Enabled Attacks

An Integrated Defence Framework

Security Hygiene

Authentication, Verification, and Digital Identity Protection

Planning and Preparedness

Threat Awareness, Training, and Proactive Defence

Incident Management

Crisis Command, Communication, and Multi-Agency Coordination

Overcoming Recovery Challenges

Sustained Response, Wellbeing, and Adaptive Response

IT Infrastructure

Technical Architecture, Expert Capabilities, and System Robustness

Governance

Strategic Leadership and Cultural Transformation

UK Resilience Academy

Q & A Panel

UK Resilience Academy

Resilience in the Round

PODCAST

Episode 1

‘Resilience is Everyone’s Business’

Thank you for joining us

UK Resilience Academy

UK Resilience Academy

UK Resilience Lessons Digest

Learning from Cyber Incidents

Issue 6 | April 2025