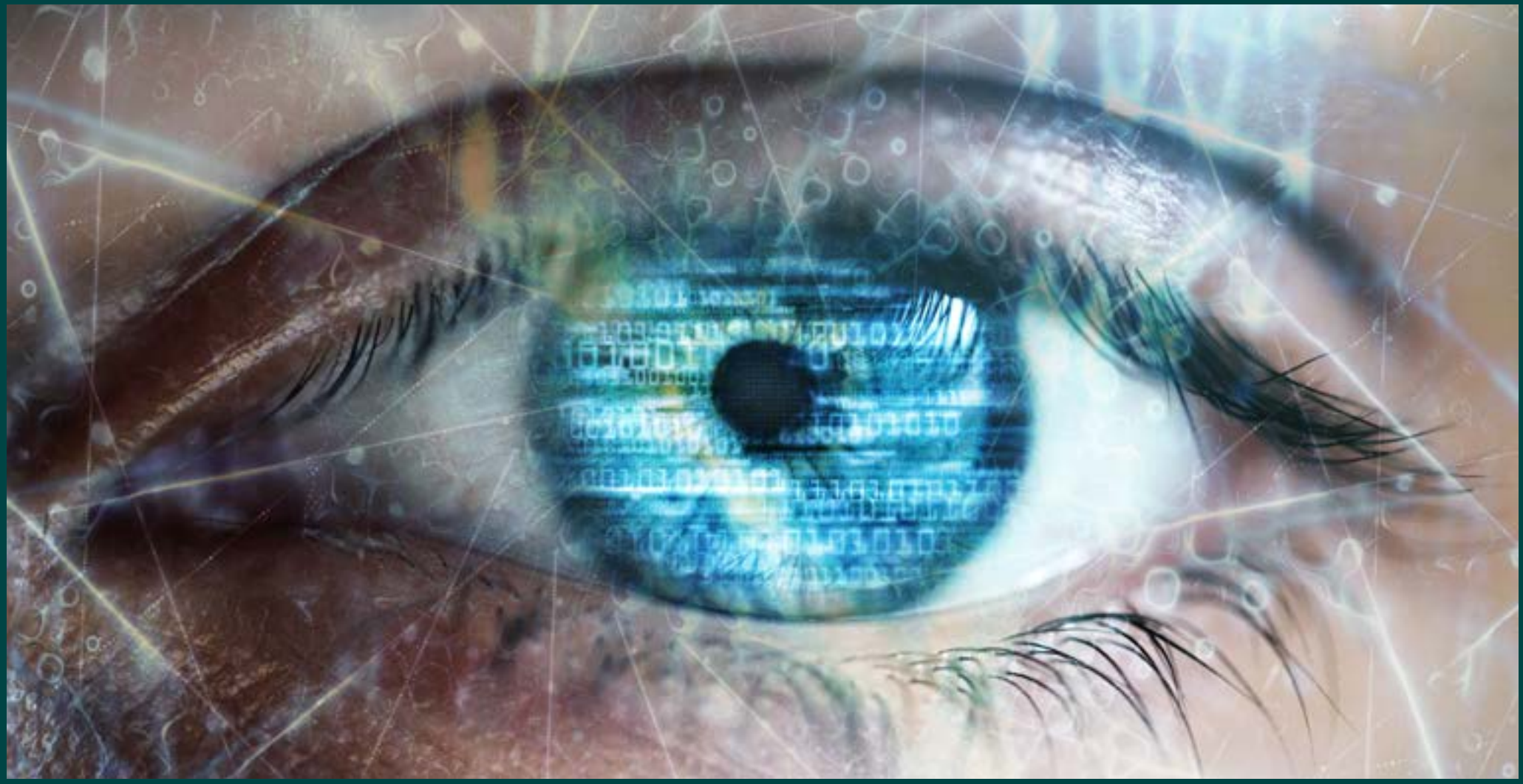
Defending the public sector's cyber attack surface

Perspectives from the UKAuthority Resilience & Cyber4Good 2023 conference



Contents

Event Partner

1. The attack surface widens

As cross-agency working expands in the public sector so does the potential surface for cyber attacks. There are more possible routes through which vulnerabilities can be exploited, affecting not just the initial target but any organisations with which it joins up digitally. And there are possible weak links in supply chains, with the danger that when a supplier is breached it can lead to the compromise of systems and data in sensitive areas of public services.

It was against a strong awareness of these factors that the recent UKAuthority Resilience and Cyber4Good conference took place, bringing together a number of speakers from organisations leading the national effort, along with people from local authorities, NHS bodies and the technology industry to share experiences and perspectives on strengthening resilience.

2. Data aggregation and pathways

One of the core issues was highlighted by Paul Barnes, head of operations and engagement for cyber security at NHS England, who said that it faces a major challenge in the form aggregated risk.

Aggregation of risk

The integration of care necessitates more sharing of information between organisations, which leads to them sharing the risk of a cyber incident. It creates the need for a national body to provide direction in the main steps to strengthen defences and mitigate the risk. While local organisations remain responsible for their security, national bodies have responsibility when the impact of a cyber incident begins to spread.

A similar point was made by a representative of the National Cyber Security Centre (NCSC), who said bulk data is an attractive target for cyber attackers of all kinds.

Focus on outcomes

The issue was highlighted in a healthcare context by event sponsor Cisco, whose cyber security specialist Emma Velle referred to the wider attack surface and emphasised the need to protect all elements of the patient against threats. She said this requires an approach focused on outcomes rather than the capabilities of any individual technology, and held up the experience of the Staffordshire and Shropshire Health Informatics Service (S&SHIS) as an example of how it can be done.

The organisation's head of technology, Richard McCue, described its use of a number of Cisco solutions to preserve resilience, while emphasising that: "The technology should come at the end. We should have the policies and guidance defined so we can align the technology to those business policies." He cited the example of a policy to require multi-factor authentication (MFA) for accessing systems. It was launched at the end of August 2023 and applies to NHS trusts, integrated care boards, arm's length bodies and non-NHS healthcare providers, stating that MFA must be all used for remote access to all systems, with some exceptions. This is aimed at stopping the escalation of any attacks which might have involved the compromise of user names and password credentials.

Supply chain key

The supply chain issue makes things more complex, and can involve a large, and possibly uncomfortable degree of trust in suppliers, as was emphasised by Henry Hughes, chief technology officer for Jisc (the membership organisation for technology services in tertiary education and research). He said this creates a need to work with suppliers on ensuring 'security by design' is prominent throughout the chain, and that it should be an important element of procurement initiatives and contracts in all areas.

This was taken further by Rachel Downs, senior cyber product manager in the Local Digital team of the Department for Levelling Up, Housing and Communities (DLUHC), who said it is an area that needs more consistency among local authorities in how they deal with suppliers. This could involve standardisation of relevant language in contracts, and requirements on suppliers to report any cyber incidents within a specified timeframe. The idea of standard clauses in contracts also drew a positive response from Billy Ruston, cyber security, cyber at the Local Government Association (LGA).

3. Polices, procedures and language

A recurring and familiar theme from the event was that cyber security is about behaviour as much as technology. An organisation has to ensure that its people follow the appropriate policies and procedures and exert what influence it can on its partners to reduce the risks of an incident. If it does not succeed there is a danger that people will design their own workarounds that could create weak links in the chain.

Shifting the organisational mindset

McCue provided the example of the MFA policy at S&SHIS, saying that it ran into opposition from some quarters and needed firm approval from the senior leadership

to ensure it was widely applied. This was accompanied by efforts to explain how important it was to the organisation's operation, aiming to break down a perception that it was an encumbrance and create a mindset in which people took it seriously rather than as 'tick the box' exercise.

It was agreed during the discussions that it is important to make the whole subject of cyber accessible to people so they think of it as a crucial element of what the organisation does and their day-to-day work. For example, in the health service there is a better chance of people cooperating when it is closely related to patient care. But there was also a recognition that the cyber specialists are not always good at doing this and that it needs thought and, in some organisations, a new approach to "making it real" for people. Local authorities face an extra demand in having to do this for elected members as well as employees, which could require a change of emphasis in how it is explained.

Cyber confidence

Another element of policy is to help people feel confident in reporting any apparent cyber incidents, even when they could have come from having made mistakes. Organisations have to build a culture in which their staff can talk at the time about a cyber incident that might be happening, and acknowledging possible missteps with the confidence that this will be seen as a positive move in mitigating any risk.

4. Additional issues

A number of other significant issues were highlighted at the event. Dan Patefield, head of cyber and national security at IT industry association techUK, addressed the need for collaboration between the public and private sectors, especially in the light of an increase in the number of fringe state threat groups that have turned their attention to UK's critical national infrastructure.

Public-private collaboration

He talked of the importance of the Government Cyber Security Strategy[1] , the most recent version of which was published in 2022 and included a new emphasis on 'defend in one piece', with industry playing a larger role and all organisations and individuals recognising their responsibility towards security. He also highlighted the Cyber Growth Partnership, a public-private partnership intended as a conduit to support growth in the sector that is chaired by the digital minister and chief executive of techUK and involves working groups on skills, exports, assurance, strategy, innovation and investment, and regional clusters.

Skills remain a challenge

The skills issue emerged more than once during the conference discussions, with a general recognition that there is a shortage of talent in the sector and public bodies will struggle to keep up with the pay offered by top private sector companies. Patefield said this creates a case for finding ways of sharing expertise across the public sector, along with efforts to develop more training for people interested in a mid-career switch into cyber security. He suggested that the audit sector could be a particularly valuable source of new people.

Growth of PETs

There was also an explanation of the potential of privacy enhancing technologies (PETs) from Calum Inverarity, senior researcher at the Open Data Institute. He defined them as tools and practices that enable greater access to data that may otherwise be kept closed for reasons of privacy, commercial sensitivity or national security, and which have the potential to support more innovation and efficiencies in the use of data while providing some assurance against the fear of breaches. They can be used to train machine learning models, conduct privacy preserving analysis, and increase access to sensitive data for research.

But they could be used in a way that undermines trust, such as in targeted advertising, and Inverarity said there should be an effort to steer them towards use towards the public good. And there is an unwelcome potential for privacy enhanced surveillance, which will demand careful oversight of how they are used.

5. Ongoing work

The event made clear that there are plenty of ongoing initiatives at a national and local level to strengthen cyber defences and included several examples.

Multi-factor authentication

Paul Barnes outlined NHS England's recently published policy on multi-factor authentication (MFA) – which involves using an additional factor to name and password to log into a digital system – saying it should now be regarded as a core element of cyber security in the health and care system. A policy document has been published laying out details of the requirements and exceptions, the latter of which includes unprivileged user account access from within an organisation's trusted network and access to a system to which the same user has previously authenticated with MFA from the same device. It outlines the distinctions between 'basic', 'better' and 'best' strengths for different purposes, and says organisations may use other authentication services, such as NHS Care Identity Service 2 or NHSmail, to provide MFA through federation.

Barnes added that NHS England has developed a five pillared approach in its strategy for cyber resilience in the health and care system. This involves: a focus on the greatest risk and harms; defending as one; developing people and culture; building secure for the future; and exemplary response and recovery.

CAF for local government

Rachel Downs presented the Local Digital team's plan to provide a version of the Cyber Assessment Framework (CAF) specifically for local authorities.

"We are developing CAF Overlay, the collective term for all wraparound stuff we are adding to CAF for councils," she said. "This is things like standalone guidance, templates, and other types of supporting material like video explainers. We are keen to make this as light touch as it can be, with the key information around scope and helping councils through the self-assessment process."

Local Digital was aiming to have the service in place by early 2024, with the possibility of a reporting service on which councils could send back the results of their assessments.

Another initiative for local government was outlined by Jamie Cross, programme manager for bespoke cyber support at the LGA. Its support offer includes the Cyber 360 service, in which the LGA can bring cyber experts together with a council's officers to talk through the issues that affect it and write up a reflective report. This is based on four underlying principles: providing advice not assurance; building capabilities; placing a focus on the security culture; and applying the Cyber 360 Framework.

The organisation also offers cyber reaction exercises to help councils establish how they might react to an incident and to practice their response in a safe environment. Cross said these are aimed at helping councils to better understand what good looks like.

Engaging users

Henry Hughes of Jisc provide a view of the cyber challenge for the higher education sector. Ransomware has become a major threat and there are common weaknesses, such as the reuse of passwords, not using MFA, failing to apply security updates to systems and continuing to use software and hardware beyond the end of its service life.

He said one of the big issues is in trying to get the message out beyond cyber security teams into organisations' wider business, and the complexity and difficulty of establishing and maintaining a strong security posture should not be underestimated. Among the Jisc recommendations to deal with this is the sharing of relevant services and expertise, and regular rehearsals and testing of security measures.

Police CyberAlarm

An update on the response to cyber crime was provided by Detective Superintendent Martin Peters, deputy lead of the National Cybercrime Programme for the National Police Chiefs' Council (NPCC). He outlined the Police CyberAlarm scheme, the role of cyber resilience centres, and the development of a network of these to promote the issue across businesses and the third sector. There are

currently 10,000 businesses signed up to the network and the NPCC wants the number to grow substantially.

6. Tips for best practice

With delegates keen to get the latest on best practice, there was bound to be intense interest in the presentations that offered clear tips on strengthening security.

At the core of these, according to the NCSC representative, are familiar steps such as patching IT systems and ensuring an effective, tested back-up regime is in place. "It is important for organisations to have backups in place to enhance resilience. Testing your back-up regime is equally important to make sure you can restore your data as planned," he said.

This should be accompanied by proportionate, reliable logging[2] to make it possible to "follow the breadcrumbs" as part of an investigation, 'strong enough' passwords as highlighted in the NCSC's 'three random words'[3] guidance, multi-factor authentication where available and access control. All of this should be underpinned by a policy of continuous improvement, with cyber specialists in the organisation up to date on technology developments.

Also important are a shared understanding of the business impact of a cyber incident, with a clear understanding of who is responsible and accountable for different elements of the business, and having an incident management plan[4] in place.

Focus on the cyber basics

Much of this was reinforced by Geoff Connell, director of digital services at Norfolk County Council and chair of the national Cyber Technical Advisory Group (CTAG). He emphasised the importance of basic cyber hygiene measures – such as the systematic use of patching, passwords, permissions and secure back-ups – and shared three recommendations.

First is to engage with national and regional support groups such as local resilience forums and WARPs (warning, advice and reporting points), building the networks for mutual support before an emergency arises. Second is to ensure that cyber resilience involves a team effort inside an organisation, and to report it regularly to the board, in plain English, to assess the appetite for risk. Third is to look out for emerging risks in areas such as smart places technology and data that could be valuable to an attacker.

Rachel Downs added to these by urging organisations to think hard about which of their systems are critical, which functions they need to protect and to make their defence a priority.

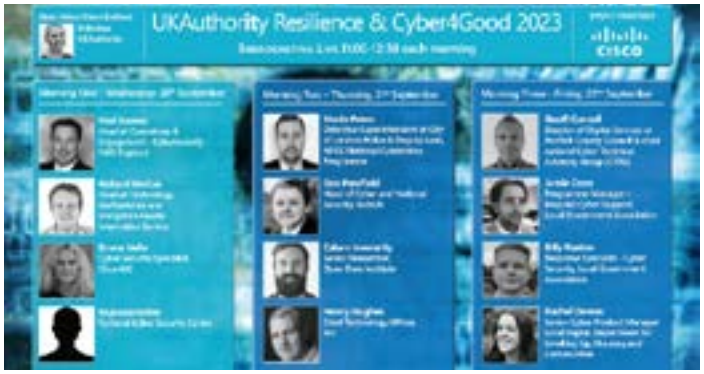
Continuous impovement essential

Underlying all the advice was a recognition that threats are continually changing and that, as Connell put it, cyber security is an arms race. This calls for continuous improvement in the effort to ensure resilience, both in the mindset to keep up with threats and be ready to adopt new approaches, and through plans to provide a structure for the efforts.

In fact, the phrase 'continuous improvement' was something of a refrain during the event, emphasising that best practice in cyber resilience is always valid for a limited time, and that maintaining it involves the capacity to continually learn and change.

7. Resilience & Cyber4Good

Session One - Wednesday 20th September 2023



Watch now

02:14: How can we improve Cyber Security Resilience across the NHS and social care? - Paul Barnes, Head of Operations & Engagement - Cyber Security, NHS England: This presentation covers the complex and changing landscape of cyber security in the health and care system, and the steps we can take to help ensure patient data is used effectively and efficiently across integrated care systems while ensuring good cyber hygiene. (Download slides)

17:15: How cyber security underpins the delivery of patient care - Emma Velle, Cyber Security Specialist, Cisco UKI and Richard McCue, Head of Technology, Staffordshire and Shropshire Health Informatics Service: A discussion about the cyber security vision, how it underpins the delivery of patient care throughout the care system, the challenges we face and the role technologies can play. (Download slides)

Enhancing resilience in the public sector - Representative, National Cyber Security Centre - This presentation is unavailable for viewing

48:46: Q&A and panel discussion - all speakers (excluding NCSC representative)

Helen Olsen Bedford, Publisher, UKAuthority

More than 170 delegates took part in this three day online event on the cyber threat and how public services can keep one step ahead of anticipating the next direction of attack.

Public sector leaders shared examples of what can be achieved and took part in lively discussions and Q&A sessions with delegate participation too. Discussions were hosted by Helen Olsen Bedford, and all sessions can be viewed in full at www.ukauthority.com.

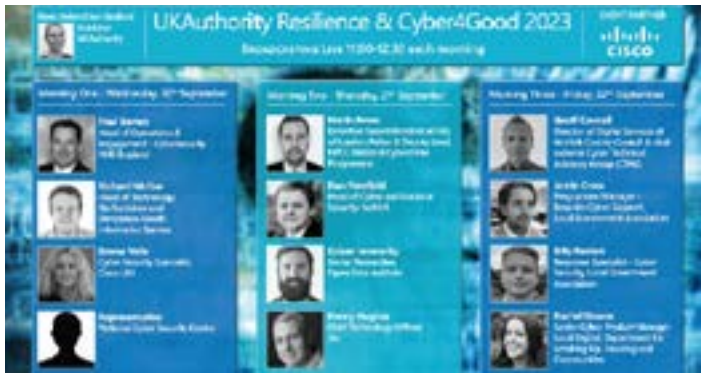
Paul Barnes
Head of Operations & Engagement, Cybersecurity
NHS England

Emma Velle
Cyber Security Specialist
Cisco UKI

Richard McCue
Head of Technology
Staffordshire and Shropshire Health Informatics Service

National Cyber Security Centre representative

Session Two - Thursday 21st September 2023



Watch now

01:50: Defend-as-one: Strengthening resilience through public and private sector collaboration - Dan Patefield, Head of Cyber and techUK: A focus on the strength of the UK cyber eco-system and how the strength of the public-private partnership in cyber can enable transformation across the UK economy. (Download slides)

18:43: Privacy-enhancing technologies: tools for public good? - Calum Inverarity, Senior Researcher, Open Data Institute: Privacy-enhancing technologies are attracting increased attention based on their potential to increase access to data that would otherwise be restricted due to concerns about privacy, sensitivity and security. In this session, Calum Inverarity covers how these technologies might be used to improve systems and processes in the public sector, as well as some of the measures we need to have in place to minimise the potential for their misuse. (Download slides)

32:23: Cyber security threats - Henry Hughes, Chief Technology Officer, Jisc: Cyber security is an ever-present and growing threat to universities and here Henry Hughes looks at the opportunities and challenges faced by the sector – and what advice and support is available. (Download slides)

45:45: UK Cybercrime Policing - Martin Peters, Detective Superintendent, City of London Police and Deputy Lead for the National Cybercrime Programme for the National Police Chiefs' Council: An overview of the Police Cyber Alarm which provides policing with a more comprehensive picture of the cyber threat landscape, informs cyber defence strategy and collects evidence that can be used in the identification, pursuit and prosecution of cyber criminals. His session also covers the cyber resilience centres - a regional network promoting the importance of cyber resilience across the business and third sector communities. (Download slides)

58:48: Q&A and panel discussion - all speakers

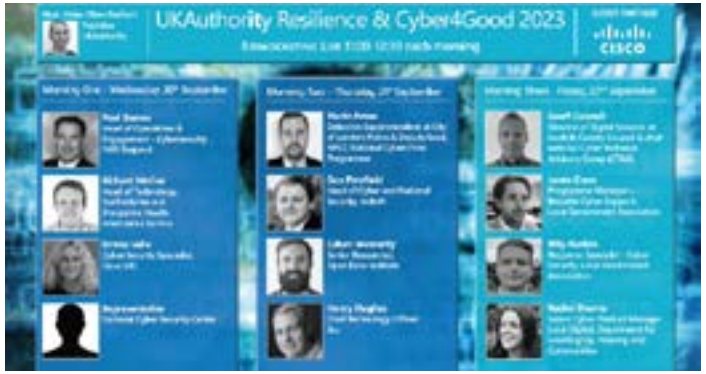
Dan Patefield
Head of Cyber and National Security
techUK

Calum Inverarity
Senior Researcher
Open Data Institute

Henry Hughes
Chief Technology Officer
Jisc

Martin Peters
Detective Superintendent
City of London Police and Deputy Lead for the National Cybercrime Programme for the National Police Chiefs' Council

Session Three - Friday 22nd September 2023



Watch now

01:47: Local Authority Cyber Resilience 2023 - Geoff Connell, Director of Digital Services, Norfolk County Council and chair of the national Cyber Technical Advisory Group (CTAG): Evolving threats including AI, modern backups, shared SOCs , supply chain and partnership working. (Download slides)

11:35: Refine your plans, rehearse your people: how the LGA's Cyber Reaction Exercises can support your council to become more resilient - Jamie Cross, Programme Manager – Bespoke Cyber Support and Billy Ruston, Response Specialist - Cyber Security, Local Government Association: A talk about the LGA's new offer of support for councils, the Cyber Reaction Exercises. This session includes why exercising is so important, how to build momentum for cyber focused exercising across a council and how to get involved to make the most of this free support for councils. (Download slides)

30:07: Testing a Cyber Assessment Framework for Local Government: What We've Learned So Far - Rachel Downs, Senior Cyber Product Manager, Local Digital Team, Department for Levelling Up, Housing & Communities: Lessons learned from DLUHC's in-progress pilot of a Cyber Assessment Framework for Local Government. She shares how this is likely to shape the approach for the sector and what councils can do now to prepare. (Download slides)

43:05: Q&A and panel discussion - all speakers

Geoff Connell
Director of Digital Services
Norfolk County Council and chair of the national Cyber Technical Advisory Group (CTAG)

Jamie Cross
Programme Manager,
Bespoke Cyber Support
Local Government Association

Billy Ruston
Response Specialist, Cyber Security
Local Government Association

Rachel Downs
Senior Cyber Product Manager,
Local Digital Team
Department for Levelling Up, Housing and Communities

7. Event Partner

Cisco

Cisco Secure is Cisco's comprehensive security product portfolio. With a robust line-up of adaptable zero trust, XDR and SASE tools, Cisco Secure makes security both integrated and accessible for organisations of any size, industry, client base and infrastructure. Cisco Secure products offer unmatched efficacy in data protection, providing security that's not only agile and adaptable, but also incredibly easy to use.

Cisco Secure enables companies to achieve security resilience and protect their organisation amidst unpredictable threats or change.

With Cisco, organisations can help ensure the integrity of their financial and data assets, spring back from operational disruptions, better withstand shocks to supply chains and secure a distributed workforce. Cisco Secure's emphasis on resilience, and partnerships with the UK's leading security experts, from the National Crime Agency to the National Cyber Security Centre, helps organisations close security gaps, see more, anticipate what's next and take the right action.

Find out more about Cisco here

Follow them on X (formerly Twitter) | LinkedIn

UKAuthority

This briefing note has been researched, written and published by Mark Say & Helen Olsen Bedford, UKAuthority. UKAuthority champions the use of digital, data and technology (DDaT) by central and local government, police, fire, health and housing, to improve services for the citizens they serve.

8. References

1. https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030
2. https://www.ncsc.gov.uk/collection/10-steps/logging-and-monitoring
3. https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
4. https://www.ncsc.gov.uk/collection/incident-management

Additional Resources

https://digital.nhs.uk/cyber-and-data-security/training/immersive-labs-online-cyber-security-e-learning

https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/multi-factor-authentication-mfa-policy#:~:text=This%20policy%20will%20ensure%20that,have%20privileged%20access%20to%20systems

https://www.isc2.org/certifications/cc

https://digital.nhs.uk/cyber-and-data-security/about-us/cyber-associates-network

https://www.ncsc.gov.uk/section/advice-guidance/all-topics

https://www.ncsc.gov.uk/cyberfirst/overview

https://www.ncsc.gov.uk/cisp/home

https://www.gov.uk/government/publications/national-cyber-strategy-2022

https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf

https://www.jisc.ac.uk/reports/cyber-impact

https://www.ctag.gov.uk/

https://www.local.gov.uk/our-support/cyber-digital-and-technology

9. UKAuthority 2024 Virtual Events

Powering Digital Public Services

Wednesday 6 to Friday 8 March 2024 (11:00-12:30) : As budgets tighten ever further and demand for services rises, can we continue to innovate and deliver at pace to power the digital public services of tomorrow?

Resilience & Cyber4Good

Wednesday 18 to Friday 20 September (11:00-12:30): With the threat of a cyber attack ever present and ever changing, we'll look at how we can build cyber defences and resilience to ensure continuity of service delivery.

Integrating Digital Health & Care

Wednesday 15 to Friday 17 May (11:00-12:30): Focusing on innovation and the complex challenge of integrating health and social care data to improve the patient journey from hospital to home.

AI & Data4Good

Wednesday 16 to Friday 18 October (11:00-12:30): How do we best unlock the power of data to gain valuable, actionable, insights on people, places and organisations and build a foundation for trustworthy AI?

Smart Places & Smart Communities

Wednesday 19 to Friday 21 June (11:00-12:30): Exploring a smart future and how best to harness the right technology and data in a secure way to improve the lives of citizens whilst making sure no one is left behind.

AI, Automation & Bots4Good

Wednesday 27 to Friday 29 November (11:00-12:30): Can AI-powered automation tools and bots deliver a step change in efficiency whilst empowering health and public sector workers?

Would you like to see more expert speakers and take part in more insightful discussions on how technology, digital and data is being used for the public good?
Sign up today to our 2024 virtual conferences using the links above or, to see all of our events, as well as catch up pages for previous events,
by clicking here.