UKAuthority Inform

2022

New cyber threats, new approaches to security

Perspectives from the UKAuthority Resilience & Cyber4Good 2022 conference

Resilience & Cyber4Good 2022

Event Partner

cisco SECURE

Contents

1. Contant Vigilance

Over the past couple of years the cyber risks facing the public sector have evolved and intensified. There is a sense of the threat from nation state attacks and ransomware exploits having grown, attackers have become more sophisticated in their approaches, and the vulnerability surface has increased with the wider adoption of apps and connected devices. Along with this are limitations on resources as public sector finances are squeezed and organisations struggle with the recruitment and retention of cyber specialists. It creates a disturbing outlook, with a need for constant vigilance and the capacity to add new layers and take new approaches to defence.

Ideas on how to respond, and examples of how organisations have done so, came under the spotlight at UKAuthority's Resilience & Cyber4Good 2022 online conference, with a range of speakers from the public sector and the IT industry providing valuable perspectives on the outlook.

2. Changing threats

Key points for the sector following the Covid-19 pandemic were raised by Paul Barnes, head of operations and engagement for cyber security at NHS England. There has been an increase in remote working, which brings its own threats, and a rise in the volume of phishing attacks to obtain sensitive data. There is more cross-agency working with integration between different networks, over which no single cyber team has complete control; and attackers are collaborating with each other through trends such as selling ransomware as a service.

There is also a growing appreciation of the fact that a large supply network with a lot of partners creates a massive risk surface, with an array of potentially weak points through which attackers could enter a system. This creates challenges in the growing need for cyber assurance along the organisational supply chain.

The point was reiterated by Geoff Connell, chief digital officer at Norfolk County Council and chair of the Cyber Technical Advisory Group (CTAG), who commented: "It is a very big ask to make sure the whole supply chain is secure. But we've seen suppliers to local government and the NHS get hit with ransomware and the operational impacts. There's a lot of work to do there."

He said there are two types of supply chain risk: in which a supplier is hit and cannot provide crucial goods or services; and in which their systems are compromised and there is a knock-on effect to those of the client organisation.

Connell also highlighted the need for assurance as the public sector moves away from using the Public Services Network towards secure routes for communication through the internet. "It will be more secure but does mean we will be losing something that has been painfully implemented but quite beneficial, that is independent assurance around PSN," Connell said.

3. Sources of support

Responding to such issues can be a daunting challenge for individual organisations, but there are sources of support. Connell pointed to the work of CTAG on activities such as developing strategies for supply chain security, promoting the application of basic cyber hygiene, training and skills development, and on exploring the possibilities for post-PSN assurance. The latter, on which the Local Digital team in the Department for Levelling Up, Housing and Communities (DLUHC) is also working, could involve a local government version of the Cyber Assessment Framework (CAF).

Another source is the Local Government Association (LGA), whose programme manager for cyber security support Jamie Cross outlined two significant offers. One is the Cyber 360 programme, managed and facilitated by the LGS, which supports councils in improving key areas against established frameworks. "It's about bringing peers and sector experts together to form a team and work with a council on its cyber security culture," they said. It involves the LGA team spending two or three days spread over two or three weeks with key people in a council, including senior leaders, to help them understand their roles and responsibilities; then following up on a reflective report focused on areas for improvement. "It's about advice, not assurance," they said. "It's trying to build capabilities, having supportive conversations, helping individuals and councils as a whole understand what good looks like."

The other LGA offering is a programme of cyber reaction exercises to help councils understand how they might react to an incident and practice in a safe environment. It involves incident response – knowing what a team should do and whether plans have been practised – and business continuity, with an opportunity to test the response, rehearse the roles of individuals, identify where existing plans need refinement, and improve awareness of cyber security.

The organisation also offers audits on cyber activities and pushes the message that there is always a need for continuous improvement, and is aiming to increase its support for councils through to 2025.

From an industry perspective, Emma Velle, cyber security specialist for NHS and local government at Cisco, highlighted the potential of cyber tools to deal with the risks from more devices being plugged into systems – while also contributing to better productivity.

"Cyber tools can tell you how people are putting information into the system, so you know who's logged on, who is going into the system, what time they are going into the system," she said, adding: "This can be shared so you are able to redirect patients to where they can be seen. You can see where kit has not been used and ask why not. The real value to the business from security tools is not just in the defence aspect but in showing how the business is working."

4. Possibilities for progress

Ideas on how cyber defences and risk management could evolve were also prominent at the event – although these often came with a cold eye on the difficulties involved.

Geoff Connell said a list of accredited suppliers would be highly useful in strengthening supply chain security, and credited the Crown Commercial Service for ensuring its procurement frameworks take basic cyber factors into account when accrediting suppliers. But he also warned that public authorities should always understand what they are buying, stop buying products and services that are not to scratch, and join together in demanding that improvements are made.

The point was reinforced by Henry Hughes, security director for non-profit education technology services provider Jisc, who stressed the need for a documented process for suppliers to demonstrate their security posture, and said it is necessary to closely examine not just software but the whole technology stack.

There was support for the idea of a shared CAF, possibly tailoring versions to different sectors such as local government, healthcare and education. Lawrence Hopper, deputy director for digital at DLUHC, said this would require the spine of a universal standard with the flexibility for different sectors to mould it to their demands. "The more we can embrace that the better," he said.

One of the questions to emerge – prompted by the limits on resources of many organisations – was whether it would be realistic to attempt to create a single national body as a security operations centre (SOC) for the public sector. NHS Digital has been able to take this route for organisations within NHS England, and there is sentiment in favour of extending its role or creating equivalents for other service sectors. David Willis, senior information security officer at the Lancashire and South Cumbria Health and Social Care Partnership, said that budgets and politics currently prevent the NHS SOC becoming available for councils, and that there would be complications in whether it extends to private sector operations providing public services, such as care homes. This will be a lingering issue with the increasing connections between NHS and local authority systems in the drive to integrated care.

The idea of a national approach won support from a police perspective with Detective Chief Superintendent Andrew Gould, cyber crime programme lead for the National Police Chiefs' Council (NPCC), saying that common standards and the National Management Centre run by the Police Digital Service have helped to stop a lot of incidents escalating. But he also acknowledged its limitations in extending into the chain of private organisations such as law firms. This prompted a suggestion among delegates' questions that it might be easier for relevant suppliers to have their own national body.

Delegates also asked about the outlook for cyber security insurance, leading Gould to comment that the increase in cyber threats is making it more difficult for the insurance industry to provide affordable solutions. The idea of a central provider of insurance for the public sector met with little enthusiasm, and the point that it would require standardised investments – which plenty of organisations would struggle to afford – in infrastructure, skills and collaboration to improve resilience.

5. Experience on the ground

A number of examples were put forward of how organisations are responding to the threats and strengthen their resilience.

NHS England has set up a Cyber Associates Network as a secure mechanism for sharing threat intelligence, asking questions, raising concerns and alerting. It also runs webinars and master classes on specific issues, holds an annual conference and stages campaigns that have extended into areas such as developing future talent and providing a diversity of people in the field.

Paul Barnes said there has been a recognition of the need to step up collaborative working in cyber in response to the integration of health and social care, and that the big challenge is to develop assurance at a local level while also obtaining a national view of the threat landscape.

Another NHS initiative has been from the Lancashire and South Cumbria Health and Social Care Partnership, which has worked with Cisco on an approach for resilience involving four key steps. First is to get full visibility of the cyber risk at the local organisational level, and second to develop a solution for responding to incidents in real time. Third is to understand the capacity, capability and sustainability of the teams involved, and fourth to stage a series of regional events for digital emergency planning, resilience and response.

Willis said a programme was underway to create a response solution that is granular and automatic, and that technology tools had been deployed in three of the five NHS trusts attached to the partnership's network, applied not just to computers but internet of things devices and clinical equipment.

These tools provide a picture of which staff are logging into the systems at which times, the information they are adding and which clinical equipment is being used, not just by one organisation but others in the partnership. The latter point can provide additional benefits: one in making it possible to spot spare capacity and when necessary redirect patients to another of the partners; another in providing information that can be used in a safe 'playpen' environment for staff training.

Efforts to support local government were to the fore. Lawrence Hopper reported that the DLUHC has been working on a CAF for the sector and has its eyes on post-PSN assurance, and worked with the LGA and National Cyber Security Centre (NCSC) in helping councils with issues such as supply chain vulnerabilities and an understanding of where cyber risk originates.

The Local Digital team in DLUHC has outlined plans for a CAF pilot, which will involve testing a local government profile through an assessment of the councils' networks with reference to the 39 CAF outcomes and supporting indicators of good practice.

The results will be reviewed through one-to-one workshops with a DLUHC cyber assessor, with questions on whether one profile will be appropriate for all councils in England, what guidance they will need and what barriers emerge during an assessment.

Jamie Cross described the LGA's Cyber 360 offer to local authorities – outlined above – supporting them in improving their performance against established frameworks. They emphasised the importance of a council agreeing on a risk assessment framework so the response to cyber risks can be escalated as appropriate, and that this should be part of a corporate risk register. The LGA has also been developing a guide on how to run an effective cyber continuity exercise.

An example of what happens when an organisation falls foul of a serious attack came from David Cowan, head of ICT at Copeland Borough Council, which suffered major disruption in 2018 – before he joined – from a brute force remote desktop attack, which led to a zero day ransomware delivery. In a short time the council effectively lost control of its technology along with all of its files, some of which it has still not been able to recover. Its first stage in recovery was invoking a business continuity plan, paper copies of which were held by key managers, although it was soon discovered that this did not make provision for 100% loss of IT.

Copeland has gradually renewed its operations, but Cowan urged others to learn from its experience and put forward five key learning points:

- Senior leaders have to set the tone for cyber controls.
- Be prepared to protect systems, with a cyber incident plan that is regularly reviewed and tested.
- Know your assets, being clear about which systems you would need to recover first. Not all are equally important.

- Have a back-up strategy, with the NCSC '3-2-1' rule as a minimum (three copies on two devices and one off-site back-up).
- Do not underestimate how long a recovery would take. It is likely to be a minimum of months and in Copeland's case has taken years.

Tertiary education has been a target for cyber criminals, with 42 significant incidents and around 1,000 distributed denial of service attacks on the sector over the past two years. Henry Hughes of Jisc said it has seen different approaches to assurance and is a big supporter of the Cyber Essentials scheme as a baseline standard, although it only covers four of the top 10 areas of security controls, and there is a need to address further areas such as supply chain risk and incident management. He strongly supported the 'defend as one' policy within the UK Cyber Security Strategy – which promotes collaboration at all levels – and emphasised that cyber is not just an IT team risk but one that has to be addressed at board level.

He added: "Where we see organisations have done rehearsals, exercises and tests, they recover in a much shorter time. The figures we see are roughly a 10-day recovery period for those that are well prepared, and for those where people are not sure of their roles and responsibilities it can be up to 20 days for recovery from major incidents."

The police response to cyber crime was also on the agenda, with Andrew Gould describing how the long established cyber crime units have been joined by the Police Cyber Alarm tool, which can be downloaded by small organisations including those in the public sector. It monitors traffic seen in an organisation's connection to the internet and can detect and provide regular reports on malicious activity.

Regional cyber resilience centres are also providing support across England and Wales, run by a not-for-profit company backed by the Home Office and including a number of major companies from the technology industry. Gould said there is an aim to increase the number of member organisations from around 10,000 to 100,000 over the next three years.

6. The positives

While nobody denied the immensity of the risks and the need for perpetual vigilance and planning, a few positive points emerged from the conference.

Emma Velle of Cisco pointed out there is a growing number of tools in the marketplace – while warning that is not enough in itself – and Lawrence Hopper of DLUHC commented: "Over time we're definitely seeing cyber literacy and capabilities improve, albeit from a low base. We're seeing that in councils cyber support has fixed specific things, and meant that senior leadership is seeing the need for reform, cultural change and to invest in skills. We've had over 100 councils come to our cyber clinics and we've heard stories from people of how they are now starting to win the business cases so they can invest in cyber on an ongoing basis."

Paul Barnes of NHS England suggested there is a growing appreciation that "cyber security is a team sport" that requires extensive collaboration, and that there are good signs of an ongoing dialogue through organisations such the NHS Cyber Associates Network (which is open to local authorities) and WARPS (warning, advice and reporting points). He emphasised the importance of beginning to network and reiterated a point made by David Cowan:

"Make friends before you need them, because if you try to make friends in a crisis they will have a focus on other things. It's about networking, building that level of trust before you need to trust someone in a crisis."

7. DAY ONE - Wednesday, 5th October

Day One, Wednesday 5th October, 11:00 - 12:45

Helen Olsen Bedford
Publisher
UKAuthority

Event Partners

CISCO SECURE

UKAuthority

Paul Barnes
Head of Operations and Engagement - Cyber Security, NHS England

Jamie Cross
Programme Manager - Cyber Security Support, Local Government Association

Henry Hughes
Security Director
JISC

Lawrence Hopper
Deputy Director for Digital
Department for Levelling Up, Housing and Communities

Geoff Connell
Director of IMT & CDO, Norfolk County Council and chair of the national Cyber Technical Advisory Group (CTAG)

01:00: Cybersecurity Is Everyone's Business - Paul Barnes, Head of Operations and Engagement - Cyber Security, NHS England

An overview of cyber security in NHS England - looking at the ever changing threat landscape and the importance of collaboration, staff engagement and Cyber Associates Network. Cybersecurity is a team sport! (Download slides)

16:10: Local government cyber and digital reform - Lawrence Hopper, Deputy Director for Digital, Department for Levelling Up, Housing and Communities

An outline of the Local Digital's plans for the next three years and what this means for local government including lessons learnt so far and what's next on their journey to drive cyber and digital reform in the sector (Download slides)

28:25: What can we learn from the Cyber 360s? - Jamie Cross, Programme Manager - Cyber Security Support, Local Government Association

An introduction to the Cyber 360 programme, common themes and learning across the five pilots, how the programme will be developed and calls to action (Download slides)

46:25: CTAG & Post PSN Assurance - Geoff Connell, Director of IMT & CDO, Norfolk County Council and chair of the national Cyber Technical Advisory Group (CTAG)

A look at how local government cyber security will be assessed once the PSN is no longer in use (next year); how CTAG is working with relevant government departments to help ensure the new regime is appropriate and not overly onerous; plus an update on CTAG & WARPS to help the audience know how to get the most out of them (Download slides)

1:01:00: The ongoing cyber security challenge - Henry Hughes, Security Director, JISC

Cyber crime costs the UK economy £27,000,000,000. Here Henry Hughes discusses how the UK education sector is facing the challenge - and how rehearsals, exercises and tests are key (Download slides)

1:16:01: Q&A / panel discussion

8. DAY TWO- Thursday, 6th October

Day Two, Thursday 6th October, 11:00 - 12:45

Helen Olsen Bedford
Publisher
UKAuthority

Andrew Gould
Detective Chief Superintendent, National Cybercrime Programme Lead, National Police Chiefs' Council

Emma Velle
Cyber Security Specialist for NHS and Local Government, Cisco

Davi
Actin nior
Infor ation
Security Officer, Lancashire & South Cumbria Health & Social Care Partnership

David Cowan
Head of ICT
Copeland Borough Council

Event Partners

cisco SECURE

UKAuthority

00:55: The Police Response - Andrew Gould, Detective Chief Superintendent, National Cybercrime Programme Lead, National Police Chiefs' Council
An update on the current threat and what policing offers organisations to help protect themselves (Download slides)

14:15: David Willis, Senior Information Security Officer, Lancashire & South Cumbria Health & Social Care Partnership and Emma Velle, Cyber Security Specialist for NHS and Local Government, Cisco
Working with Cisco, Lancashire and South Cumbria Health and Social Care Partnership has developed an approach for resilience involving four key steps. Here they discuss the work underway and how resilience depends as much on organisations and people as it does on technology (Download slides)

38:51: Covid Cyber Security Challenges at Copeland -David Cowan, Head of ICT, Copeland Borough Council
An overview of some of the cyber security challenges and responses in Copeland Borough Council and how these activities impact beyond the Covid experience (Download slides)

1:07:10: Q&A / panel discussion

11. 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 here | Twitter | LinkedIn

12. UKAuthority Events

Support from our event partners enables UKAuthority to produce free events for the public sector to share success stories, best practice and experience

Click here to find out more and register to attend future UKAuthority events

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 public they serve.

Visit UKAuthority.com to keep up with news and developments in the use of DDaT for the public good. We host regular virtual round tables and events exploring best practice and innovation in the public sector. Visit the UKAuthority 2022 events schedule here