BYTES | Smarter together

The Front Line of the Future

Reducing Cyber Vulnerabilities in Local Government

Table of Contents

Introduction

There is increasing potential for hackers and cyber criminals to attack local councils as public services become digitalised.

Cyber-attacks are a primary threat to local authorities as ransomware attacks have the power to capture vulnerable citizens data and hold it to ransom. In fact, Socitm recently placed cyber resilience at the core of their 12 digital priorities for 2023.[1]

More than 7,000 people have recently been affected by a hack on Colchester City Council. It was reported that the hack targeted the city council's "outsourcing contractor Capita".[2] The contractor had been "running the council's benefits system and audited its council tax and benefits services for six years".[3] This was vital data that was exposed to criminals looking to exploit even the smallest vulnerability in the public sector. Unfortunately, this is not an isolated issue. In 2022, it was estimated that Hackney Council spent "£12.2m in the last financial year" on recovering from a targeted hack.[4] This included "more than £444,000 spent on IT consultancy, £152,000 on recovery of the Mosaic systems used for social care data, and £572,000 on the housing register in the last financial year."[5] Through hacks such as these, not only is extremely vulnerable citizen's data put at risk, but an enormous amount of money and time is spent recovering services to a normal state of play.

It has never been more essential that local government reinforces its cyber resilience and cyber security protocols. With the war in Ukraine, the National Cyber Security Centre (NCSC) has seen a dramatic uptake in international actors targeting the public services. Malevolent forces from countries such as China and Russia, are continually producing "ever more sophisticated" hacking technologies.[6] They utilise complex phishing and ransomware operations to directly target the most vulnerable aspects of a state's infrastructure. When seen in combination with the recent attacks on local councils, the potential for harm is vast, daunting, and immediate. Local government is at the forefront of providing vital services to our most vulnerable and cyber threats are the singular biggest threat to the public.

The Situation Today

During 2022, the NCSC co-ordinated "the national response to 18 ransomware attacks including the attacks on a supplier to NHS 111, and South Staffordshire Water."[7] The true numbers of ransomware attacks in the UK each year are far higher, as "organisations often do not report the compromises."[8] This demonstrates the sheer scale of the threat that is faced on a national level, especially when organisations and departments are not reporting attacks due to fear of exposing vulnerabilities.

Ransomware attacks specifically pose such a threat that the NCSC joined forces with the FBI, CISA, the National Security Agency (NSA) and the ACSC in 2022 "to highlight that there had been an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organisations globally. Given its potential impact on critical national infrastructure and essential services, ransomware is considered a national security risk."[9] Cyber-attacks such as these are defining themselves as targeted, efficient, and prolific.

For Local government, Ransomware remains the most significant cyber threat. Ransomware attacks "threaten both a council's ability to deliver essential services to communities, and their financial resilience. Despite extensive work undertaken to ensure local government is as resilient as possible to cyber-attacks, the risks posed by ransomware attacks are still increasing."[10] As mentioned above, in 2020 criminal hackers deployed ransomware that severely crippled Hackney Council's systems, limiting the council's ability to look after vulnerable people. The Pysa ransomware gang "later claimed responsibility for the attack and, weeks later, claimed to be publishing data it stole from the council."[11] This exposure of vital data is at the core of these attacks as the information is held hostage with the threat of exploitation hanging over the councils – the pressure increasing as the attack goes on. In 2022, Hackney Council was still dealing with the aftermath of this attack. For approximately a year, "many council services weren't available. Crucial council systems—including housing benefit payments and social care services—weren't functioning properly."[12] This highlights the human cost of this attack regardless of the £12.2M cost previously stated. In placing security at the heart of workflows local council organisations can effectively defend against highly sophisticated cyber-attacks.

With the modernisation of local government also comes an increase in vulnerabilities. There are several issues within local government that broaden the range of opportunities for cyber-attacks: the exposing of supply chain when working with 3rd party organisations, the use of legacy software and hardware, the growing technical skills gap within workforces, and the on-going creation of smart cities.

Since HM Government's declaration of the objective to spend 33% of procurement spend with SME's, supply chain has become fertile ground for cyber criminals of all kinds.[13] Councils often rely on external suppliers to provide devices and services, and "have an annual spend of over £70 billion in procurement in England alone."[14] Local governments' ability to reduce the risk of a cyber-attack and maintain cyber resilience also "depends on the cyber security of the organisations in their supply chains."[15] As the Local Government Association (LGA) states, "embedding cyber-resilient practices into the council's supply chain structure is integral to creating a solid foundation to prevent and mitigate the effects of cyber threats".[16] Local authorities are autonomous organisations, independent from one another. As cyber-attacks tend to be isolated, "there is resilience associated with the diversity of technology and discrete systems within the local government sector."[17] This does not account for how often "councils share data and access to systems with various agencies to deliver essential services."[18] This multitude of linkages between organisations present "multiple intrusion points" that increase vulnerability, especially if these linkages are not monitored.[19] In order to provide modern services, it is essential that vital data and information is shared, that's why ensuring that modern security solutions are adopted and placed within the heart of workflows is so important.

The adoption of these modern solutions is another area that presents an ever-growing opportunity for cyber criminals. Many councils are running legacy IT estates that cannot keep up with modern threats. Cyber security demands investment to address "vulnerabilities associated with legacy IT and manage and mitigate new vulnerabilities that may arise from increasing digitalization."[20] If Councils don't make the necessary investments "there are concerns that councils will fall under the 'cyber poverty line', and no longer invest in what should be regarded as essential security measures."[21] This "digital poverty line" is also pointed to in HM Government's 'Organising for Digital Delivery' report. It states that legacy IT estates create a 'technical debt' as huge swathes of funds ("50% of current Government IT spend") is spent on simply "keeping the lights on".[22] This presents a wide range of issues for local government as vital funds are not only spent on recovering from attacks, but also spent on simply trying to keep this legacy IT infrastructure afloat and operational. This is extremely fertile ground for hackers as vulnerable people's data is under-protected and vulnerable.

This legacy hardware and outsourcing to third parties has also led to a significant technical skills gap. HM Government's 'Cyber security skills in the UK labour market 2023' identifies that "Half (50%) of all private sector businesses identify a basic technical cyber security skills gap, i.e. a lack of confidence in performing a range of basic cyber security skills tasks or functions."[23] This demonstrates the vast issue facing the UK's workforce. The paper also looks at local authorities' ability to attract talent to cyber jobs as pay scales cannot align with the private sector. This shows just how drastic the situation is as the few qualified staff available cannot be tempted away from the positions they hold. In not having upskilled staff, local authorities are particularly vulnerable to cyber-attacks as they hold huge amounts of vulnerable data and funds. Cyber-attackers do not fear an instant and thorough response when attacking a local authority.

This vulnerability takes on a physical aspect when we look to the creation of smart cities and 'connected places'. Connected places utilise a combination of sensors, hardware, applications, and networks to analyse and improve services and places. These places collect data to improve:

Transport and new mobility solutions

such as the instalment of smart traffic light systems to reduce congestion on busy roads or future air mobility solutions.

Environmental monitoring

such as the use of sensors to monitor water levels in areas at risk of flooding or air quality to provide citizens with clean air walking routes.

Social care, health and wellbeing

such as the deployment of temperature and moisture sensors in houses to monitor and improve living conditions, or the use of sensors that help facilitate assisted living and improve accident response times.

Critical infrastructure and utilities

such as crowd monitoring to determine town centre business and provide citizens with information on best times to shop, or the use of smart local energy systems to reduce pressure on the grid.[24]

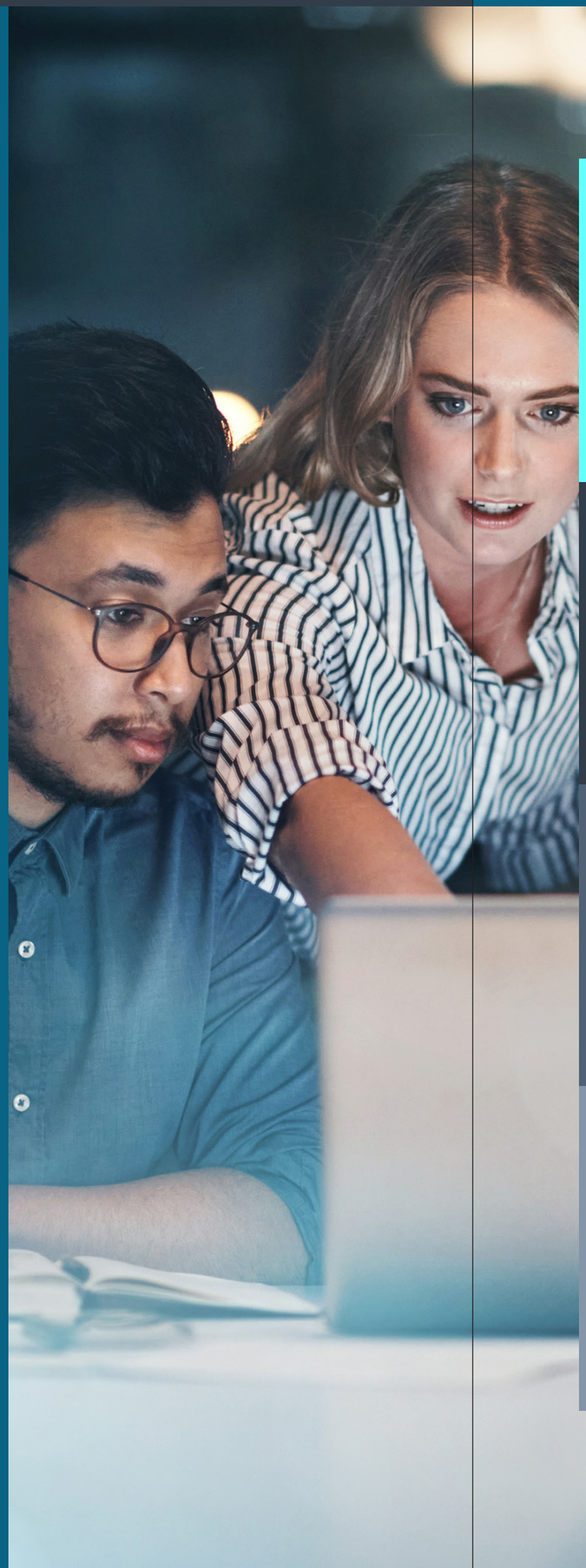
Whilst these improvements grant local authorities transformative power, they are also, however, vulnerable targets. Rather than vulnerable service users' data, cyber attackers in this instance can directly hack and hold to ransom the physical infrastructure of a local authority. This would mean a significant disruption in service users' lives as well as a significant spend of crucial funds and time. Without a robust and continual focus on cyber resilience, attacks on the ever-evolving smart cities will only become more common. The interconnected nature of these places, whilst their strength, is also their biggest weakness in terms of cyber resilience.

Fostering a Culture of Security

The areas for hackers to seek out vulnerabilities and exploit are only growing. As the public sector and local authorities continue modernising workflows and digitising services this is set to continue exponentially. The solution is a mentality of ongoing revision towards cyber security - constantly placing secure protocols at the heart of workflows whilst remaining vigilant to the progress of your organisation's cyber resilience. Local government is being supported in adopting this mentality.

In September 2022, the Department for Levelling Up, Housing and Communities (DLUHC) Local Digital team initiated a pilot with a number of councils, exploring how the NCSC's Cyber Assessment Framework (CAF) could be "used to help assess and manage cyber risks across local government in England."[25] The first phase of the pilot saw an undertaking of more than "50 hours of workshops with 10 councils from across England" working through the four objectives outlined in the CAF.[26]

The NCSC framework is made up of a set of 14 cyber security principles, together with guidance on applying the principles. It helps organisations achieve an appropriate level of cyber resilience. The principles define "a set of top-level outcomes that, collectively, describes good cyber security for organisations performing essential functions."[27] Each principle is accompanied by guidance for achieving the outcome and recommends routes to tackling common cyber security challenges. The 14 cyber security principles fall under 4 main objectives. They are:



Objective A: Managing security risk

Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.

Objective B: Protecting against cyber-attack

Proportionate security measures are in place to protect the network and information systems supporting essential functions from cyber attack.

Objective C: Detecting cyber security events

Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.

Objective D: Minimising the impact of cyber security incidents

Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.[28]

These objectives will directly focus local authorities on the core remit of their cyber reliance. Helping them to create a culture of vigilance within their workforce.

In a recent update, some core 'pain points' have been identified by the councils taking part. The primary being. "The need for improved efficiency and security against cyber attacks within councils. Significant progress can be made through collaboration, innovation, and better technological measures."[29] This demonstrates what we already know of how far councils are behind in both legacy systems and the skills gap. Addressing this gap, another 'pain point' was "siloed approaches and gaps in skills and data, as well as difficulties shifting cultural mindset, have reduced the ability for innovation within councils".[30] This shows how beneficial the scheme has already been in identifying the need to think beyond simply implementing new tech. There needs to be a definite and consistent approach to both training and cultural shift. This will implant security practices such as this framework directly into day to day practices.

Local Digital has also launched the Local Digital Fund. The Local Digital Fund "aims to help local authorities implement the Local Digital Declaration by funding digital skills training and projects that address common local service challenges in common, reusable ways."[31] It funds both collaborative projects, which receive funds as well as dedicated support from the DLUHC Local Digital team, and digital skills training, which seeks to meet the need for digital leadership and agile project delivery training.

Local Digital has also launched the Continuous Digital Planning Fund. Under this model, "funding is not limited to specific time-bound rounds or dates; the model aims to complement the delivery pace of individual projects to support project momentum and the cohesion of project teams".[32] Both funds provide access to the capital needed to negotiate the CAF framework and implement a culture of cyber vigilance within the workplace. The continual nature of this opportunity, in particular, means that the on-going growth of cyber security can be kept up to date.

Solutions

Bytes offers a wide range of solutions to help public sector organisations successfully defend against sophisticated cyber attacks. With over £490 million worth of security projects delivered annually, Bytes is well equipped to help place security at the heart of local government working practices. Our solutions mean that information silos can be overcome and modern, flexible ways of working can be adopted. Bytes offers four main sections of cyber solutions:

Cyber Consulting

Listening to customer needs and helping to deliver effective change.

Cyber Solutions

Working with more than 100 top tier vendors to ensure that customers get the exact solution that they need.

Cyber Services

Offering tech support as well as fully managed security services to effectively neutralise security risks.

Cyber Insights

Providing customers with cutting-edge research into cyber security to help them stay ahead of cyber threats.

Each of these main sections of solutions directly relate to the main objectives of the CAF. Cyber Consulting offers audit advisory, strategy, and assurance services. Services such as digital risk assessment, project and third-party security reviews, and penetration testing, all directly serve objectives A, B, C, and D. These place security at the heart of your working operations by effectively instilling a cyber strategy into your local authority organisation.

Bytes Cyber solutions come from a diverse range of 100+ top tier vendor partnerships. Our vendor agnostic approach means that our experts listen to your organisation's individual needs. We highlight the pros and cons of each solution that we think would be suitable. We also can directly relate which solution would work to meet its corresponding objective in the CAF. A solution that helps create a secure, yet flexible working environment through a virtual desktop, for example, would directly address objective B.

Bytes offers support, delivery, and fully managed services under its 'Cyber Services' section of solutions. Our support lines are open 24/7 with engineers that hold a minimum of 5 years experience. This support is a fantastic way to mitigate the risks of a cyber-attack and directly addresses objective D in the CAF. Within our delivery support, our expert engineers design, deploy and migrate bespoke working solutions for your government organisation. They can then provide expert training to staff, ensuring that objectives A, C, and D are met.

Finally, our cyber insights solutions provide ongoing content for your staff to keep on top of the most recent developments in cyber security. With over 35 expert led videos, podcasts, and annual reports year on year and over 25 thought leadership events, Bytes is an expert in the newest cyber threats. Our industry insights and expert research means all objectives in the CAF can be approached and met confidently.

Supporting Technology Partners

proofpoint.

Proofpoint is a leading cybersecurity company that helps protect local and central governments from rising cyber threats. Our people-centric approach to cyber defence focuses on protecting the individuals most likely to be targeted within an organisation. From essential services, to election systems, and other critical infrastructure like water and utilities, no government agency is safe from alarmingly frequent cyber attacks. Unfortunately today's attackers have more digital avenues to attack, and they know they can take advantage of an agency's most vulnerable asset: their people. Our cloud-based suite of people-centric compliance and security solutions enable rapid response to threats, minimise the risk of financial fraud, and let local and central governments manage legal and compliance risk across email, the cloud, social media, and the web.

tenable

Tenable® is the Exposure Management company. Approximately 43,000 organisations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform.

Tenable is the leading cyber exposure organisation within the public sector, helping customers comply with the DSPT, Cyber Essentials, PSN compliance and more. Tenable work with local and central government, healthcare, housing, police and fire and rescue to ensure those organisations are in control of their cyber exposure.

cisco SECURE

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 helps organisations close security gaps, see more, anticipate what's next and take the right action.

Microsoft

At Microsoft we are dedicated to advancing human and organisational achievement. Our mission is to empower every person and every organisation on the planet to achieve more and by collaborating with policymakers around the world in addressing online security challenges, Microsoft supports global efforts to make the future of computing more secure.

Microsoft's solutions help address security issues and use AI and automation to detect and stop attacks automatically without human intervention. Get a holistic view into your environment and eliminate gaps in coverage with comprehensive cyber security solutions that work together and with your ecosystem to safeguard your identities, endpoints, apps, and clouds.

Today's world is more connected than ever before. Microsoft enables productivity and innovation by giving people the right solutions and processes to allow governments to take advantage of technology to improve how they communicate and deliver services without increasing the risk of attack.

About Bytes & Its Assessment

For over 40 years, Bytes have built trusted relationships with a vast partnership network of innovative vendors. With our expertise, favourable pricing, and our strong links and accreditation levels, we make effective use of technology to implement digital change and protect infrastructures. Bytes Public Sector have made our solutions and services available on a range of frameworks, making it simple and straightforward to work with us.

Bytes CAF Gap Analysis provides organisations with a security focused gap analysis based on the National Cyber Security Centre Cyber Assessment Framework. First, bytes collects and collates information on your current security solutions, processes and procedures. Then, a session is delivered to discuss and clarify the information collected and to gather any additional information needed to create your report. After which Bytes reference your answers against the 14 principles of the NCSC. Finally, a bespoke, detailed report is produced, which includes a high-level score against each of the 14 principles, as well as detailed explanations to justify the score and recommendations for next steps to improve the overall result.

The Bytes CAF Gap Analysis provides expert analysis of your security solutions, processes, and procedures to provide tangible recommendations on how best to improve your organisation's security posture.

References

1

Socitm. “Public sector digital trends.” Socitm, 23 January 2023

socitm.net/resource-hub/collections/public-sector-digital-trends/

2, 3

BBC. “Colchester City Council contacts 7000 people after data hack.” BBC, 21 June 2023

www.bbc.co.uk/news/articles/c97992yg5weo

4, 5

Gregory, Julia. “Cyber attack recovery effort cost Hackney Council over £12m last year.” Hackney Citizen, 13 October 2022

www.hackneycitizen.co.uk/2022/10/13/cyber-attack-recovery-hackney-council-12m/

6, 7, 8, 9

National Cyber Security Centre. “NCSC Annual Review 2022.” National Cyber Security Centre

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

10, 14, 15, 16, 17, 18, 19 20, 21

Local Government Association. “Ransomware: LGA response to the Joint Committee on the Nation-al Security Strategy inquiry - December 2022.” Local Government Association

www.local.gov.uk/our-support/cyber-digital-and-technology/cyber-digital-and-technology-policy-team/consultation-responses/ransomware

11, 12

Burgess, Matt. “The Untold Story of a Crippling Ransomware Attack

www.wired.co.uk/article/ransomware-attack-recovery-hackney

13

HM Government. “Central Government Direct and Indirect Spend with Small and Medium-sized Enterprises 2016/17.” GOV.UK, 8 February 2021

www.gov.uk/government/publications/central-government-spend-with-smes-2016-to-2017/central-government-direct-and-indirect-spend-with-small-and-medium-sized-enterprises-201617

22

HM Government. “Organising for Digital Delivery.” GOV.UK, 22 July 2021

www.gov.uk/government/publications/organising-for-digital-delivery/organising-for-digital-delivery

23

HM Government. “Ipsos report.” GOV.UK

assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1173325/Cyber_security_skills_in_the_UK_labour_market_2023.pdf

24

HM Government. “Secure connected places playbook.” GOV.UK, 16 May 2023

www.gov.uk/guidance/secure-connected-places-playbook

25, 26

HM GOV. “Insights from the Cyber Assessment Framework for Local Government pilot - DLUHC Digital.” DLUHC Digital, 14 December 2022

dluhcdigital.blog.gov.uk/2022/12/14/insights-from-the-local-government-caf-pilot/

27

Local Government Association. “Cyber Assessment Framework - Policy Brief.” Local Government Association

www.local.gov.uk/our-support/cyber-digital-and-technology/cyber-digital-and-technology-policy-team/cyber-assessment

28

National Cyber Security Centre. “CAF - Principles and guidance - NCSC.GOV.UK.” National Cyber Security Centre

www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance

29, 30

Medium. “Future Councils update #3. It’s been a busy month for the... | by Local Digital | Local Digital | Aug, 2023.” Medium, 9 August 2023

medium.com/ldcu/future-councils-update-3-2f863883b985

31, 32

HM GOV. “The DLUHC Digital Planning Programme.” Local Digital

www.localdigital.gov.uk/digital-planning

BYTES Smarter together | GOV NEWS DIRECT

About us

Bytes is a leading provider of world-class IT solutions. Our growing portfolio of services includes cloud, security, licensing, SAM, storage, virtualisation and managed services.

Since being established in 1982, Bytes has grown rapidly and now employs over 450 people in the UK and Ireland. Thanks to our passionate people and close partnerships, we’ve helped hundreds of top brands to transform, grow and adapt to the changing technology landscape.

www.bytes.co.uk

GovNewsDirect

This paper was built in partnership with GovNewsDirect. GovNewsDirect specialise in facilitating innovative and engaging partnerships between the private and public sector.