April 2016

Socitm
Policy

Briefing

Role of local government in National Cybersecurity Strategy:

A policy perspective from Socitm

Purpose of this Briefing

This briefing sets out a high level view from Socitm about the part that local government could and should play in implementing the National Cybersecurity Strategy announced in HM Government's Autumn Statement (2015).

In particular, it sets out the case for a stronger local cyber resilience, in order to protect the UK as a whole, as well as to ensure security and protection of local public service delivery.

The national – local context

In his Autumn Statement, the Chancellor of the Exchequer announced an investment of £1.9bn over five years to protect Britain from cyber attacks and to develop its capabilities in cyberspace. Together with existing spending on core cybersecurity capabilities and the more recent announcement of an additional £1bn for cybersecurity in Health, the Government's total cybersecurity spending is now set to reach more than £4.2bn over the next five years.

To date, most UK government cybersecurity policy, strategy and measures have focused on central government's response to the threat – through the big government departments and specialist agencies such as GCHQ. Whilst this remains a priority, a new local focus is needed if the UK is to manage and respond to changing threats.

Over 60% of citizen interactions with government take place between citizens and local authorities and devolution will only increase this proportion. In addition, local public services are being redesigned universally to become 'digital' and joined up at, and across, local and national levels. This not only increases cyber risks, but also opens up new avenues for national cyber-attacks via local digital 'backdoors' of inter-connecting systems and IT networks.

It follows that local government and its partner delivery organisations must play a bigger part in the UK cybersecurity 'ecosystem' in future. Local government holds essential intelligence about local communities and cyber risks. This data needs to be better managed, joined up, shared and used to support UK-wide threat mitigation.

The steps outlined in this briefing would help ensure that local government's cybersecurity contribution and its requirements are treated as part of the overall UK system of preventative measures to protect all government services. We argue that local government needs to be engaged in the emerging national strategy and plans, and properly resourced to locally address cybersecurity and resilience.

Local government's track record

The shutdown of systems and services following the malware attack on Lincolnshire County Council during in January 2016 is a rare example of a successful cyber-attack on a local council. Local government has a strong track record of investing in effective information security and of engaging service managers in business continuity planning. Whilst most councils do experience daily cyber-attacks, these are mostly repelled successfully and there have been few serious incidents to compare with the Lincolnshire attack.

However, there is no room for complacency. Historically, local government has not been a target for cyber-attacks in the same way as some central government departments, except for the usual risks such as attempted fraud or attempts to damage reputation through websites. But this is changing. As local government plays a bigger role in public service delivery and as IT networks such as the PSN join together across the public sector, the risks are changing and growing. The imminent expansion of the Internet of Things (IoT) will only further increase the range of devices, systems and locations where a national cyber-attack could be initiated locally, or where local services could be penetrated and crippled, requiring a national response.

Socitm has been working with DCLG to share best practice in cybersecurity with discussions in train to explore the national benefits of using central funding for local government to help further cybersecurity best practice among councils.

A recent two-day DCLG consultation event considered the risks and the need for greater local cyber resilience. This brought together police chiefs, local authority leaders, the LGA, GCHQ, Socitm, SOLACE, Cabinet Office and other subject specialists. A full report on the outcome of the consultation is available here. Its conclusions support the view that better coordination is needed across the full spectrum of public services – local and national - in recognition of changing cybersecurity threats, along with clarity of local and national accountability and the targeting of resources.

> "Historically, local government has not been a target for cyber-attacks in the same way as some central government departments, except for the usual risks such as attempted fraud or attempts to damage reputation through websites. But this is changing."

> "The nature of the cyber threat is changing and growing. It requires a new and sustained approach locally, not just nationally."

A robust foundation of compliance already exists in the form of cybersecurity accreditation for Public Services Network (PSN), Payment Card Industry (PCI) and related technology and data handling requirements. This includes Socitm's research, assessment and benchmarking, and advisory services. (This is because the crowdfunded PSN Solutions service has just been closed down). Professional research, advice and guidance and peer networks such as WARPS all assist local authorities and their partners in risk management, preventative action and, ultimately, preparedness to handle cybersecurity threats. There is also a growing list of UK Local Resilience Forums (LRF) involving Councils and Local Economic Partnerships (LEPs) that are also beginning to take an interest in cyber threats as part of local commercial and enterprise development.

Yet most of these groups do not work in a unified and collaborative fashion – sharing learning or adopting common principles, standards and accountability. For example, only a little over half of local authorities belong to the government-founded Cyber Security Information Sharing Partnership (CiSP), and whilst many councils have a Senior Information Risk Officer (SIRO), broader cyber resilience is not typically part of their remit. Cyber resilience is generally seen as an 'IT security' matter in local government, not often treated as a major business and service threat, with top executive and political ownership. This needs to change.

What is needed is a single set of government cyber guidance, responsibility, accountability, testing and governance, defined both locally and nationally, as part of the National Cyber Security Strategy (NCSS) currently being updated. Lincolnshire County Council's experience is the exception rather than the norm. However, the nature of the cyber threat is changing and growing. It requires a new and sustained approach locally, not just nationally.

Our proposals

The following proposals are the result of consultation with key stakeholders and the Socitm membership.

- **Local government must play an active role in the planned National Cybersecurity Centre (NCC) and the development of the National Cyber Security Strategy (NCSS). This includes its governance and the co-design of solutions, advice, support, etc., grounded in an awareness of local communities, business priorities and ways of working. What is needed is single set of government cyber guidance, responsibility, accountability, testing and governance, defined both locally and nationally**
- **Central and local government should be in a symbiotic relationship, to resource and develop local capacity to ensure secure operation of joined-up services (e.g. those involving DCLG, DWP, DVLA, etc.). This implies a holistic assessment of how national resources should be targeted – money, skills and effort. All local authorities should be members of the Cyber-Security Information Sharing Partnership (CiSP) (www.cert.gov.uk/cisp), agreeing common priorities and actions, applied appropriately at a local level to reflect local risks, issues and threats reflected in the NCSS.**
- **Local government should be given a specific remit for cyber resilience, including both executive and political accountability. This would include local risk assessment, audit, testing, awareness, public engagement, training and information sharing. Work should be undertaken to build a common and shared picture of risk, establishing clear political and executive responsibilities in local government, with key partners such as the police.**

These are all significant but achievable ambitions. Local cyber resilience is now high on the list of top threats to business and government and needs to replace old-thinking about past risks.

An effective future response to cyber-attack nationally will depend critically on local cyber maturity and investment. Doing this together with a stronger local focus reduces risk, improves cyber response and arguably gives the National Cybersecurity Centre greater influence over local risks. Failure to act now places the UK in a weakened and vulnerable position, especially with the growing dependence on open government, digital public services and UK ecommerce.

What Socitm is doing now

Socitm is well placed to take a strong leadership role on cyber resilience and is currently focused on several key areas:

- **Expanding its information governance work with stakeholder partners to 'mainstream' cybersecurity into local government e.g. adults' and children's social care, devolution, infrastructure services and smart cities.**
- **Working with suppliers to ensure that procurement mechanisms (e.g. Digital Services Marketplace and Crown Commissioning Services) embrace relevant cybersecurity accreditation and understanding.**
- **Collaborating in campaigning and briefing materials for local government, police forces and other stakeholders, to target different audiences and raise awareness of both IT and non-IT aspect of cyber resilience.**

Socitm continues to develop and share good practice and dialogue on sensitive issues such as cyber, including peer reviews, regional workshops and collaboration with existing groups such as LGA, SOLACE, and others. We continue to lobby for greater involvement, openness and influence in groups such as CiSP, NCC and the NCSS.

Our work recognises that cyber resilience must be much more than managing the technology and the way in which systems are designed, implemented and managed. No matter how good the malware prevention and detection systems, there is always a risk. Culture, staff training, process and business continuity planning are essential parts of cyber resilience, which is why we encourage top management and political awareness and support.

Our recent Socitm Insight Briefing *Push for local cyber security and resilience* sets out the steps that local CIOs can take by working in partnership with senior local public service leaders and securing the right level of focus on the topic.

Nevertheless, there is a recurring theme of local government being involved too late in national strategy development, despite the risk this brings, as described in this Special Briefing. Socitm, working with others such as DCLG, LGA, SOLACE, the Local CIO Council (facilitated by Socitm) and the Local Government Delivery Council, will continue to lobby central government on behalf of local public services for a new approach.

The sums of money and time needed to support local government input into wider public sector co-ordination would not be significant in terms of the overall cyber resources earmarked but, with the exception of the Local e-Government Programme (2000-05), provision for local public services engagement in co-ordination of national technology policy and implementation is absent or very limited indeed. Cyber resilience depends on better collaboration across the whole 'ecosystem' of public services and that must include local government and its partners in the places where they operate.

Appendix 1
Source Materials

Some current background references and relevant information are listed here:

Socitm Insight Briefing: *Push for local cyber security and resilience* sets out the steps that local CIOs can take by working in partnership with senior local public service leaders to ensure the right level of focus on the topic. Insight briefings are available to subscribers here.

The CPNI 10 steps to Cyber Security:
CESG Security Design Principles for Digital Services

CiSP is a joint industry/government initiative that aims to increase overall levels of situational awareness of cyber threats and therefore reduce or otherwise mitigate their potential impact: www.cert.gov.uk/cisp. CiSP helps partnership members from across sectors and organisations to exchange cyber threat information in real-time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information. It is free to join and there is a dedicated forum for local authorities on the online platform.

Warning, Advice and Reporting Point (WARP) is a cost-effective, trusted environment where members of can enhance their information security by sharing cyber threat and vulnerability information.

DCLG, supported by iNetwork, City of London Corporation and the British Computer Society, convened a consultation group of senior leaders from local government, the wider resilience community, central government and professional associations, including Socitm and SOLACE, to examine the forthcoming 2016-2021 National Cyber Security Strategy (NCSS) and the revised National Cyber Security Programme (NCSP#2) can best reflect the ongoing role of local government and their partners in supporting wider cyber-resilience. A full report from this St Georges House Consultation (Windsor Castle, January 2016) is available:

Local Leadership in a Cyber Society: Towards a model for civic cyber resilience

Socitm is the professional body for digital leaders in local public services. We offer networking and peer support, professional development, and access to research and consultancy on a wide range of digital policy and technology issues to 1500 members and their employing organisations.

Socitm works with the Local Government Association, SOLACE, CIPFA, ADASS-IN, the Local CIO Council, the Local Government Delivery Board, iStand (formerly Local e-Government Standards Body) and LocalGov Digital in areas such as digital leadership, strategy, skills and inclusion, data quality, interoperability standards, transparency and open data; and with Central Government, including Cabinet Office, CESG, HM Treasury, the Department of Communities and Local government, the Department of Work and Pensions, and the Department of Health on pan-government digital transformation. Socitm also has strong links with its partner associations in Europe and around the world.

Have your say

We welcome comments and discussion on the ideas presented in this Policy Briefing.

Socitm Member group: www.khub.net/socitm

Martin Ferguson
Director of Policy & Research
E-mail: martin.ferguson@socitm.net
Phone: +44 (0) 7931 456 238

Socitm
Delivering digital leadership

8a Basset Court
Grange Park
Northampton
NN4 5EZ

Telephone: 01604 709456

www.socitm.net