Think Cyber
Think Resilience

Building Resilience Together :
Briefing Paper

Strengthening Technical Resilience:
The role of technology leadership in helping to strengthen local civic cyber resilience

CYBERUK STRATEGY

Think Cyber
Think Resilience

iStandUK
BRIDGING THE INFORMATION GAP

ST GEORGE'S HOUSE

Strengthening Technical Resilience: The role of technology in helping to strengthen local civic cyber resilience

The **Think Cyber Think Resilience** initiative is a National Cyber Security Programme (NCSP) funded collaboration between the Ministry for Housing, Communities and Local Government and IStandUK (the Local e-Government Standards Body) that brings strategic leaders, policy makers and practitioners together from across the local public and resilience sectors to work with NCSP partners to develop shared cyber resilience learning and mentoring resources to support wider awareness across civic sector organisations.

Since its launch in 2015 **Think Cyber Think Resilience** has run a wide scale programme of "*Building Resilience Together*" briefing seminars, conferences and exercises across English local authorities and local resilience forums to help induct over 2000 local public sector leaders and practitioners in the wider National Cyber Security Strategy. The initiative works closely with the National Cyber Security Centre, Cabinet Office Civil Contingencies Secretariat and the Local Government Association.

Think Cyber Think Resilience has hosted a series of Local Leadership in Cyber Society strategic round table events at **St George's House Windsor** to support wider thought leadership across government, local public service, private and academic sectors. **Think Cyber Think Resilience** was awarded international exemplar status by the **OECD Observatory of Public Sector Innovation** in April 2017 for its innovative approach to shared learning in support of civic cyber resilience.

A number of the participants, recognising the need for peer-to-peer leadership from within and across the sector, agreed to write short articles relating to the themes discussed. These articles are personal reflections on some of the issues relating to civic cyber resilience and locality or place based service delivery. They do not represent government policy but do reflect some of the issues around civic cyber agenda that are increasingly common to all local authorities and the wider local public sector. In this booklet the following senior local leaders write on the role of technology leadership in helping to strengthen local civic cyber resilience

- **In our digital world it is vital to be cyber resilient: Geoff Connell**, Chief Information Officer for Norfolk County Council (former Socitm President) addresses the need for technology leaders to be ever vigilant.

- **Towards a more cyber resilient infrastructure: Darren Scates** from the Metropolitan Police Technology leadership looks at how Cloud computing and platforms can support the development of a cyber resilient infrastructure.

- **Security doesn't stop at the PSN: build your own plan: Mark Smith**, Head of the Public Services Network, sees an evolution in councils' cyber security practice that helps us all.

- **Use the cyber resources available to you: Martin Ferguson** Socitm director of policy and research urges public sector organisations to use the cyber resources already available to them to meet the responsibility to be cyber resilient.

In our digital world it is vital to be cyber resilient:

Geoff Connell, Chief Information Officer for Norfolk County Council (Socitm President 2016/18) addresses the need for technology leaders to be ever vigilant

At a time when the news suggests the criminals are ahead in the cyber security race, we cannot afford to be complacent in our approach to protecting our information assets.

This is particularly when budgetary pressures and modern service delivery methods see us move more of our transactions online, interact with our residents and local business over the internet, exploit cloud services and work in increasingly complex partnership arrangements.

The cyber threat opportunities are increasing and we need to understand the changes and take appropriate action.

Whilst we continue to invest in technology, it is our people that are our greatest asset, and ironically our greatest vulnerability. We must be proactive with our awareness raising and training. Throughout our organisations we need to encourage a culture which recognises the importance of protecting information and an understanding of the risks and mitigating actions they can take.

In order to protect our vital and sensitive information we should maintain a detailed information asset register, implement good information governance with an appointed lead for information risk management. We need to define and understand the organisation's risk appetite and use this understanding to determine the areas where investments in technology, policy changes and training will deliver the highest value to protect the organisation.

No guarantees

Being resilient to cyber-attacks and incidents will become an increasing priority as there are no guarantees that our defences will not be breached at some point. We can prepare by conducting regular cyber exercises that need not be technically sophisticated, but do need to focus on working together to solve problems and respond to incidents.

Good incident response and management will improve organisations' reaction time to deal with incidents, saving time and money in providing an efficient and effective recovery from cyber-attacks and breaches of information security.

The General Data Protection Regulation (GDPR), will come into effect from May 2018. Organisations need to prepare now, by strengthening their governance, ensuring they have appropriately qualified expertise available and by reviewing internal processes. Staff training and testing will be even more important, as will effective incident management and response.

Hygiene impact

Cyber hygiene - getting the basics right - will have the biggest immediate impact. Keep the approach to cyber resilience simple, understandable and measurable: the local public services mantra of 'simplify, standardise and share' applies to cyber resilience. Good awareness raising, training and response will take an organisation a long way.

There must be board level leadership and scrutiny. This is a corporate issue, to protect the information and personal data we hold. Criminals need not keep the upper hand, if we all work towards simple cyber hygiene, work together and support each other.

On that note, I welcome the focus in the National Cyber Security Strategy 2016-21 and the creation of the National Cyber Security Centre as reflecting the importance of the topic, the need for funding, and the capacity to help the public sector keep safe and secure in this increasingly digital, connected, online world.

Towards a more cyber resilient infrastructure:

Darren Scates from the Metropolitan Police Technology leadership looks at how Cloud computing and platforms can support the development of a cyber resilient infrastructure.

"If it's good enough for…" is a much used term in technology. And while we should never rely totally upon someone else's risk based decisions about their infrastructure, connectivity and hosting solution, (designed inevitably to address their own risk profile and appetite) we must learn from each other.

In local government today we have early adopters and market leaders embracing public cloud services and sharing systems as well as those who are realising the advantages of moving away from our traditional software vendors and systems integrators. We also have local authorities who insist on being able to drive in less than 30 minutes to their local datacentre and rolling forward quite traditional monolithic delivery models. So which end of that scale is correct? In truth neither can be 100% right or wrong and at least in the short to medium term a best of breed hybrid is likely to be the answer. Some of our oldest legacy systems do need 'feeing and watering' but have we all got a migration strategy away from such architecture?

Central government has tried to assist with advice and guidance, also by opening up the supply market with a Digital Market Place for the whole of the public sector. This provides access to literally hundreds of ready-made services and also to specialists in small, medium and large companies.

Cabinet Office guidance on the right approach to assurance around cloud services significantly moves us on from having to see and touch our servers and the often false level of security we used to think this provides. Where are we more likely to suffer a network failure, power outage or flood – in a public cloud provider's purpose built multi-million pound resilient datacentre or in our basement? A rhetorical question but one that I hope gets you thinking about what we mean by cyber resilience.

We can extend the comparison to denial of service attacks, hardware failures and firewall intrusions – all of which can be provided in a cheap and resilient way by a public cloud provider. "Oh but can we conduct intrusion tests?", well yes you can – and you should involve your accreditor in the design of cloud solutions before undertaking the same level of intrusion testing on 'your' new cloud service as you would on a system in your own datacentre.

Finally, the platforms and service being developed by central government are all equally applicable to local government. From crown hosting and the Verify and Payments platforms to the designs emerging from Common Technology Services in areas like shared networks and securing cloud email one has to ask, So, if it's good enough for them…

Security doesn't stop at the PSN: build your own plan:

Mark Smith, Head of the Public Services Network, sees an evolution in councils' cyber security practice that helps us all.

In recent years, the number of data breaches and threats to public sector data has focused local authority attention on effective security regimes. In our role of overseeing the Public Services Network (PSN) compliance process, it's been great to see this evolution in practice – a smarter and more thorough response to security helps us all.

There are, however, still some organisations that don't see the bigger picture and continue to think that, because they are PSN compliant, they must by default be completely secure and resilient.

PSN compliance is just one component of any organisation's security landscape, but we often see PSN compliance misused as a delivery mechanism for security across an entire organisation. It means they make their security decisions based on just meeting the demands of PSN compliance – not on meeting their organisation's specific needs.

In our experience, any organisation that uses PSN compliance as a checklist of the things they need to do to be 'secure' seems to have little understanding of security issues or their needs. And that often means they're going to fall down when it comes to being properly secure or resilient.

Compliance not the same as 'secure'

It's important to recognise that risk management and security responsibilities cannot be deferred by virtue of simply using a particular network. PSN compliance – by its very nature – only reports on some parts of what you need to do because it only looks at risks that are important to the PSN network and those connected to it.

Organisations need to go further than simply meeting the security outcomes of PSN compliance – they need to focus on ALL their security needs. That means they need to have a complete understanding of their organisation, the information they hold, use and share as well as their network and everything connected to it.

Getting the balance right

Local government in particular holds significant amounts of sensitive data, which makes the cost of a potential breach even greater. However, security and resilience certainly isn't about locking everything down – it's about being armed with the latest research, guidance and information to help you decide the best course of action for your organisation.

Investment in an effective security regime is essential and it's important to grasp your responsibilities. A good way to start is to understand these principles:

- Cyber security is constantly changing and evolving. You can never be 100% secure.
- Solutions should be implemented in a way that balances risk with cost and usability.
- Solutions should be outcome based and regularly reviewed to keep pace with the changing security landscape.

When you choose solutions bear in mind that something that carries an accreditation or a certificate of compliance is a good start – but it won't guarantee it's right for the needs of your business. Carry out your own due diligence to make sure it's right for you.
Make sure the solutions are appropriate for protecting the things that are important to your business and the way it works. Also – because you can never be 100% secure – have strong incident and response processes to reduce the impact of a potential attack.
You can also help make sure these processes are deeply rooted in your business by making them a compulsory module in new starter training, which you can then build on by continually training your staff. We've seen this method work well across a number of organisations.

Security is about helping your organisation and your staff to do what they need to do as safely as possible. If you understand your responsibilities and the needs of your business, accept that the cyber security landscape is constantly changing, implement well-configured commodity solutions and build a strong incident response system, you'll have the tools to do it.

Use the cyber resources available to you:

Martin Ferguson Socitm director of policy and research urges public sector organisations to use the cyber resources already available to them to meet the responsibility to be cyber resilient.

Accelerating digital ways of working and sharing data and information between agencies and actors places an ever growing responsibility on all those involved to be cyber resilient. This responsibility impacts all users of information systems and those supporting them.

Citizens, businesses, staff working for community, third sector and private sector delivery organisations, local authority staff and IT teams all need to understand the importance of guarding against cyber threats, and the behaviours and steps that, individually and collectively, they need to adopt.

Cyber threats are not just technical in nature. The human factor and insider threat is just as important and, no matter how good the malware prevention and detection systems are, there is always a risk that hackers will be one step ahead. We need to ensure that operational staff will always be diligent and follow relevant advice.

For local authorities, cyber security awareness and skills are required at the following levels:

- Senior leadership and management – business requirements and cyber practices.
- IT, digital and web teams – infrastructure and technical cyber skills.
- Staff in all service delivery organisations – user and operational cyber skills.
- Citizens, community groups, businesses, voluntary organisations – awareness and skills to protect themselves, their organisations and services.

10 steps

Senior leadership needs to ensure that appropriate steps are in place to secure data handling procedures and to train all staff. Their organisations should retain a 'senior information risk owner' capability to implement good cyber security practice in each of the areas addressed by the NCSC 10 steps to Cyber Security including user security policies, information assurance awareness, and cyber skills guidance and training.

In line with local authorities' responsibility for economic, social and environmental wellbeing, these activities should encompass partner organisations delivering public services, as well as citizens, local businesses and voluntary organisations in their area.

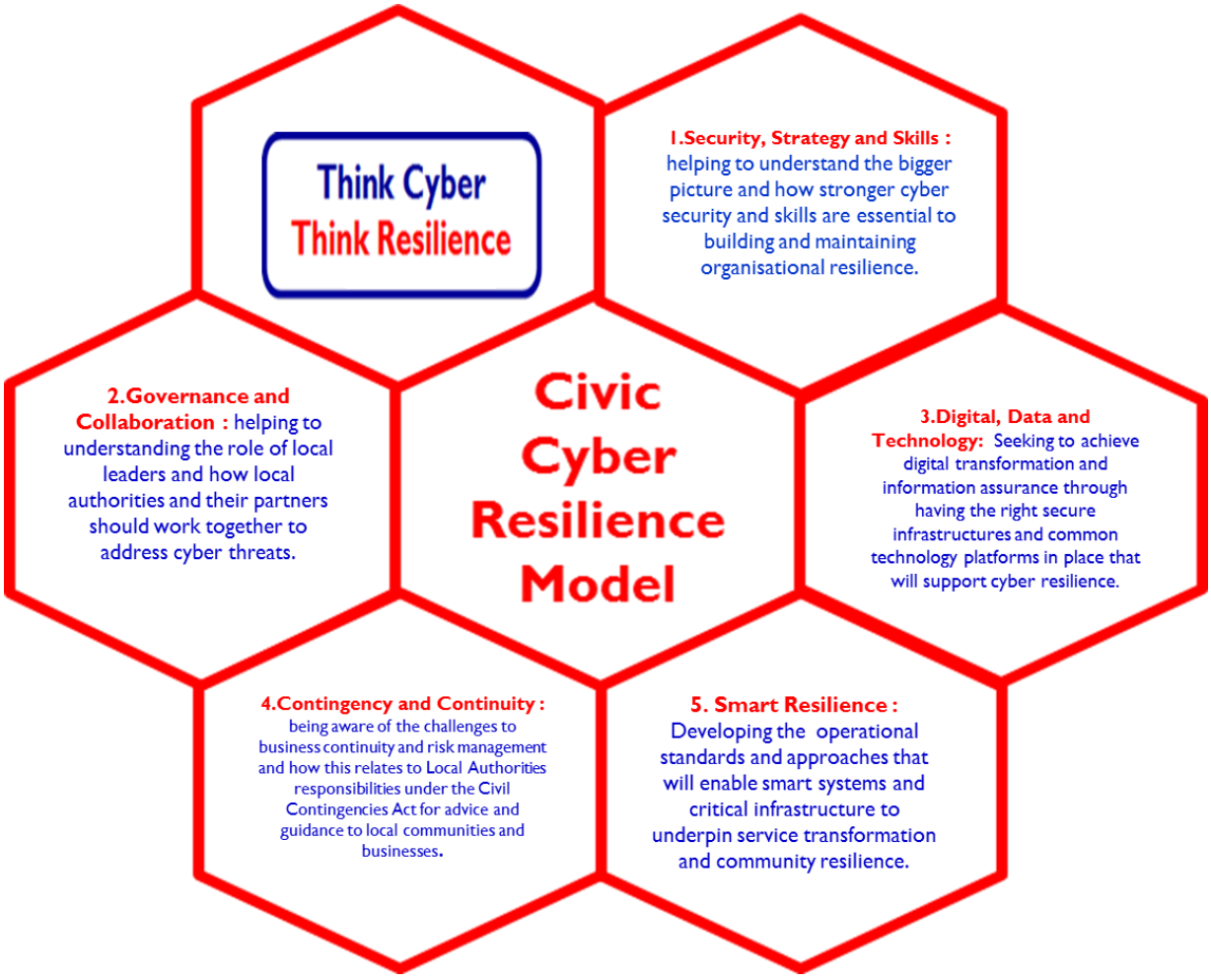
Given the national cyber security skills shortage, local authorities - especially those at the smaller end of the spectrum - will be unable to retain all the necessary and relevant cyber security capabilities in-house. They should take advantage of external resources and shared capabilities wherever possible. These include:

- Free membership of cyber security information sharing partnership (CiSP).
- Participation and sharing between authorities through regional warning, advance and reporting points (WARPs).
- Professional support, guidance and services of associations like Socitm – for example, maturity assessment tool, briefings, research and advisory services.

Think Cyber Think Resilience: Civic Cyber Resilience Model supporting strategy into practice

The **Civic Cyber Resilience Model** (see Fig 1 below) developed by the **Think Cyber Think Resilience** initiative in conjunction with the wider National Cyber Security Programme through a series of workshops with over 1000 local public sector leaders, policymakers, practitioners and a subsequent senior leadership roundtable at **St George's House Windsor** (see below) . It covers five broad themes and is sub-divided by a set of key design principles. It sets out the strategic headlines and provides relevant prompts for the actions you need to consider in devising your own cyber resilience strategy. It can help organisations to identify, assess and mitigate the threats to your organisation.

Fig 1- Civil Cyber Resilience Model



To find out more about the themes outlined in this booklet and the supporting design principles contained in the **Civic Cyber Resilience Model** visit http://istanduk.org/cyber-resilience/).

Think Cyber Think Resilience is particularly grateful to the following organisations for their help and support in developing this booklet:-

St George's House http://www.stgeorgeshouse.org/

St George's House was founded in 1966 by HRH The Duke of Edinburgh and the then Dean of Windsor, Robin Woods, as a place where people of influence and responsibility can gather to grapple with significant issues facing contemporary society.

The House offers a safe physical and intellectual space, rooted in history but focused firmly on the future. The emphasis throughout our carefully crafted consultations is on dialogue and discussion to encourage creative thinking, informed debate and sustained engagement. This is a place where participants can make a real contribution to society, where personal enrichment and social progress are mutually compatible, and where
Wisdom is nurtured.

iNetwork http://i-network.org.uk/

iNetwork's vision is to help local public service organisations to "collaborate to innovate" and thereby provide effective support for their users, patients and communities.
A large number of councils, police, fire, health, housing and voluntary sector organisations across the North and Midlands are members of iNetwork. In addition we run national programmes for Government and host the local government information standards organisation, iStandUK.

Society of IT Managers https://www.socitm.net/

Socitm is the professional body for people involved in the leadership and management of IT and digitally enabled services delivered for public benefit. Their role includes helping to: maximise the effectiveness of IT and digital in delivering services for public benefit; develop members professionally to deliver their organisation's IT and digitally-enabled transformation objectives; and help public service organisations and citizens get maximum value from IT and digital services.

Socitm have identified four main benefit areas to provide services to support members and their organisations – professional development, peer support, policy & influence, and research & improvement.

Society of Local Authority Chief Executives http://www.solace.org.uk/

Solace is the representative body for Chief Executives and senior managers working in the public sector in the UK; committed to promoting public sector excellence.

Solace provides its members with opportunities for professional development and seeks to influence debate around the future of public services to ensure that policy and legislation are informed by the experience and expertise of its members. Whilst the vast majority of their members work in local government, some occupy senior positions in health and social care organisations, police and fire authorities and central government departments.

Think Cyber Think Resilience

Building Resilience Together :
Briefing Paper

The **Think Cyber Think Resilience** initiative is a National Cyber Security Programme (NCSP) funded collaboration between Ministry for Housing, Communities and Local Government and IStandUK (Local e-government standards body) that brings strategic leaders, policy makers and practitioners together from across the local public service and resilience sectors to work with NCSP partners to develop shared cyber resilience learning and mentoring resources to support wider awareness across civic sector organisations.

To find out more see http://istanduk.org/cyber-resilience/ or contact: **cyber-resilience@communities.gsi.gov.uk**

In addition we would recommend that you accessing the following National Cyber Security Programme partners web pages as a way of keeping your organisation up to date with the latest wider cyber resilience guidance :-

- **National Cyber Security Centre** – national technical authority for cyber security see (https://www.ncsc.gov.uk/)
- **Cyber Essentials and Cyber Essentials Plus** - national schemes that offers a sound foundation of basic cyber hygiene measures (https://www.ncsc.gov.uk/scheme/cyber-essentials)
- **Cyber Aware** - national campaign to improve the online safety, behaviour and confidence (https://www.cyberaware.gov.uk/)
- **Local Government Association** – cyber security information pages for local authorities (www.local.gov.uk)
- **St George's House** – for the Local Leadership in a Cyber Society Report (http://www.stgeorgeshouse.org/wp-content/uploads/2016/04/Local-Leadership-in-Cyber-Society-Report.pdf)
- See also **OECD Public Sector Innovation Observatory –** for the **Think Cyber Think Resilience** international exemplar case study**.** https://www.oecd-opsi.org/

OECD Observatory of Public Sector Innovation

iNetwork involve influence inspire

Published by INetwork in support of the National Cyber Security Programme 2016/2021