Think Cyber
Think Resilience

Building Resilience Together :
Briefing Paper

Partnering for Resilience:
The role of inter-agency collaboration in supporting civic cyber resilience

CYBERUK STRATEGY

Think Cyber
Think Resilience

iStandUK
BRIDGING THE INFORMATION GAP

ST GEORGE'S HOUSE

Partnering for Resilience: The role of inter-agency collaboration in supporting 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 inter-agency collaboration in supporting civic cyber resilience.

- **Cyber strength in partnership: Stephen Baker**, Chief Executive of Suffolk Coastal and Waveney District Councils, argues that working in partnership can strengthen the sector's overall resilience to cyber-attack.

- **Collaboration is a key component to cyber protection: Phil Swan**, Chief Information Officer for Greater Manchester Combined Authority, outlines that ransomware attacks on public services are the tip of the cyber threat iceberg.

- **Cyber, community resilience and place based well-being: Noelle Godfrey**, Head of Digital Infrastructure at Cambridgeshire County Council and programme director, Connecting Cambridgeshire, says that digital technology underpins almost every aspect of modern living including work, travel, leisure and health.

- **Planning for a Cyber Resilient Future: Mark Brett**, honorary visiting fellow at De Montfort University, the cyber collaboration agenda has recently been brought to the fore through the continuance of high visibility attacks and the increased reporting of cyber-crime.

Cyber strength in partnership

Stephen Baker, Chief Executive of Suffolk Coastal and Waveney District Councils, outlines how working in partnership can strengthen the sector's overall resilience to cyber-attack.

Is there anyone who doesn't work 'in partnership' these days? The increasing breadth of service delivery, the reduction in resources and capacity, and the need to access a wider range of skills more effectively has prompted the vast majority of us to work in partnership in many forms.

This has many benefits, but also generates a new series of demands. New relationships have to be created and shaped between the partners.

Revised roles and responsibilities must be understood so that all those involved understand who is responsible for what. Also we must be aware of any new risks that may develop from working in partnership.

To achieve effective cyber resilience everyone must play their part, and for everyone to play their part roles and responsibilities must be understood. By working in partnership we can certainly strengthen our resilience, sharing challenges and skills, and recognising the need to collectively resist the shared enemy of a cyber-attack.

Shared understanding and awareness of the risk

It is essential that all those in a partnership have a shared understanding of the risk faced from a cyber threat. If this is disjointed or inconsistent then the partnership is weakened. That shared understanding will be underpinned by effective communications and solid commitment from all partners to recognising the importance of cyber resilience.

Access to tools to maintain resilience

Partners need consistent and relevant reference points to ensure that they are working to the same standards and information. A shared information assurance policy, and access to and use of data handling guidance underpins the partnership and ensures that all have a shared responsibility for how data is handled and managed.

Duty of cyber care

We are familiar with the term 'duty of care'. Between partners we need to establish a 'duty of cyber care'. This will recognise the responsibility that each partner has for the other, and emphasises within the partnership an understanding of the impact that a weakness in their systems will have on their partners.

Maintain skills and training

An inconsistency in the level of skills and training between partners will create an imbalance in the understanding of and awareness of the potential of a cyber threat. This in turn will lead to an adverse impact on the level of cyber resilience within the partnership.

This can be avoided by sharing training and skills development, recognising that it is a mutually held objective that all partners wish to avoid an attack, or at least be able to resist one should it happen.

Supportive leadership and culture

The effectiveness of any training, or of sharing information, will be diminished if there is a lack of leadership, or if the culture of the partnership, or individual partners, is such that the cyber resilience is not recognised as a priority. It is essential that the leadership is present within the partnership, that values the time taken to prepare for and maintain cyber resilience, and that culturally there is an expectation that everyone has a role to play.

The need to work in partnership within organisations, and beyond organisational boundaries, will never go away, and sadly neither will the threat posed by those who wish to cause damage to organisations through a cyber-attack.

Maintaining cyber resilience is a challenge for partnerships, but also a means of strengthening the way that partnerships work together.

Collaboration is a key component to cyber protection

Phil Swan, Chief Information Officer for Greater Manchester Combined Authority, outlines that ransomware attacks on public services are the tip of the cyber threat iceberg

Every silver lining has a cloud and this could be said of the growing frequency and sophistication of cyber-attacks.

Damaging cyber-attacks which disrupt operations, compromise data and impact people, are increasing in local public services as colleagues from GCHQ can testify. The Wanna-cry ransomware incident highlighted in May 2017 showed these are still only the tip of the cyber threat iceberg – many types of council and NHS organisations are seeing unprecedented volumes of malicious emails and brute force attacks on their websites.

Support from the national cyber security programme has been welcomed, not only because of the range of capabilities on offer but because it is pushing awareness of this agenda towards the corporate leadership. As Richard Knowlton, group security director at Vodafone, said on the BBC Radio 4 programme The Bottom Line: "The more successful I am (at fighting cyber-attacks) the less investment I get. I'm seen purely as a cost centre".

Good leadership recognises this and understands that prevention is better than cure, particularly as the average cost of a security breach is now estimated at £2.7 million (source: IBM), with big attacks much more. The US retailer Target estimated the cost of its recent breach at $148 million and Talk Talk's at over £50 million. These costs often exclude the reputational damage and career limiting implications of, for example, the leader's Twitter account being hacked and used to publish indecent images.

A key complicating factor is the increased reliance on digital information across public services. I would like to highlight two ways in which councils can mitigate this – by maximising productivity and through mutual support arrangements.

Safe space

Regards the former, with an acknowledged cyber skills shortage, it is increasingly important that knowledge is shared and useful capabilities exploited. In our regional iNetwork group we have a quarterly information security and assurance group meeting which typically brings a large group of individuals together in a 'safe space' to share practical tips, near miss experiences and content they do not want on an electronic forum.

We regularly raise issues anonymously, and a busy online forum provides continuity between meetings - as does the partnership office which sources answers to problems.
Mutual support arrangements should be looked into as they can be drawn on when a significant breach occurs. These come into their own when responding and, for example, the corporate network and communications needs to be taken down for a week or more with consequent knock-on impacts. The pressure placed on ICT staff to fix the problem is enormous, and risks burning people out such that after 72 hours they become ineffective.
Taking a leaf out of the civil contingencies book we would encourage groups of organisations with similar ICT architectures to agree to help each other. There are a variety of ways to do so but the common factor has to be to do it before you have a problem, not when one is already occurring.

Cyber, community resilience and place based well-being

Noelle Godfrey, Head of Digital Infrastructure at Cambridgeshire County Council says that collaborative digital technology underpins almost every aspect of modern living including work, travel, leisure and health.

It's a truism now to say that digital technology underpins almost every aspect of modern living including work, travel, leisure and health.

Increasingly access to digital infrastructure and services has become a barometer of the economic strength, sustainability and quality of life for rural and urban communities. With the largest internet economy across the G20 the UK has been catapulted into the digital age with far reaching social and economic consequences.

As our working lives, personal lives, our entertainment and communications are increasingly happening in the virtual world of digital technology the way in which that world operates becomes integral to the fabric of our lives as well as to the health, well-being and prosperity of our communities. The speed with which digital technology has radically transformed so many activities in the early 21st century means that we risk being unprepared for the consequences of the new dependency on digital technology.

Our communities, businesses and public services need to learn new ways of behaviour if we are to continue to thrive in the lawless 'wild west' of the internet where the stakes are high, and the risks as well as the rewards are myriad. Trust in the integrity and confidence in the delivery of digital services amongst customers, members of the public and the wider community are essential to the ongoing success of the digital economy.

This makes an appreciation of good 'cyber hygiene' a matter of public policy and a precondition for resilient communities which are able to thrive and to benefit from the social and economic opportunities of digital technology.

Lifeblood

If collaborative digital infrastructure and services are the lifeblood of future economic success and thriving communities, then cyber resilience becomes paramount. Furthermore, a whole place approach recognises the inter-relationship between the business imperative for cyber resilience and the links to strong local public services.

Local public service organisations have the opportunity to act as conveners, to draw out the unifying thread of cyber security across place, which equally impacts businesses and communities, using intergenerational links and existing community ties to develop and share good cyber practice. This extends into the business community by helping to foster shared learning and best practice and threat analysis across an area.

A place based approach can use local business and community networks to raise awareness and understanding of the risks to cyber resilience and the best way to combat them.

Planning for a Cyber Resilient Future

Mark Brett, honorary visiting fellow at De Montfort University, the cyber collaboration agenda has recently been brought to the fore through the continuance of high visibility attacks and the increased reporting of cyber-crime.

The cyber agenda has recently been brought to the fore in peoples' thinking, partly through the continuance of high visibility cyber-attacks and partly through the increased reporting of cyber-crime.

The fact remains that local public services need to be able to continue through the impact of a direct cyber-attack or the consequences of a close partner or delivery organisations being affected by an attack.

One of the key aspects of cyber is the fact it is intangible: cyber-attacks are not restricted by physicality and the can be instant, travelling at light speed through electronic signals. The cost of sophisticated technology is always decreasing, and the provision of commercial public cloud infrastructure has brought the power of multi-million pound data centres to people's laptops.

The challenges faced by local public services to counter these unwelcome visitors can partly be addressed by traditional resilience planning and guidance. However, the traditional approaches to threat and risk management are predicated on historical trends and occurrences. A number of factors suggest that a new approach is required:

- Local public services are often outsourced and can be inversely affected if an outsourced supplier is attacked.
- Re-organisation and moves towards service integration between authorities and organisations, significantly alters the threat profile and attack surface of those organisations.
- Criminal activity increasingly favours the cyber world where risks are seen as smaller and the gains greater. It is possible to steal data without removing the originals or leaving any traces.
- New technology or service developments create new opportunities. Electronic currencies like bitcoin enable digital transactions, but they can also be stolen and used to buy tangible goods or services.

We have for some time concentrated on business impact models to determine the level of resilience and integrity we build into systems, traditionally based on the need for confidentiality, integrity and availability. We need to learn from past experience, but at the same time think differently about the future. Different risk modelling methodologies, possibly based around services as well as people or places, are needed to reflect the realities of cyber risks, and we need to reconsider the deleterious consequences either delivered or affecting the cyber aspects of local public services.

Experience in planning

There is a lot of experience to call on – we planned for and managed events like the Year 2000 bug or the 2012 Olympics. We also plan for, and learn from, major incidents like the 7/7 attacks in London. All of these events had detailed and meticulous planning behind them, coordination protocols and resources of people and investment to make them safe.

However, in future there will be numerous smaller but nevertheless very damaging events that, whilst localised, will be debilitating to the services impacted and the communities they serve.

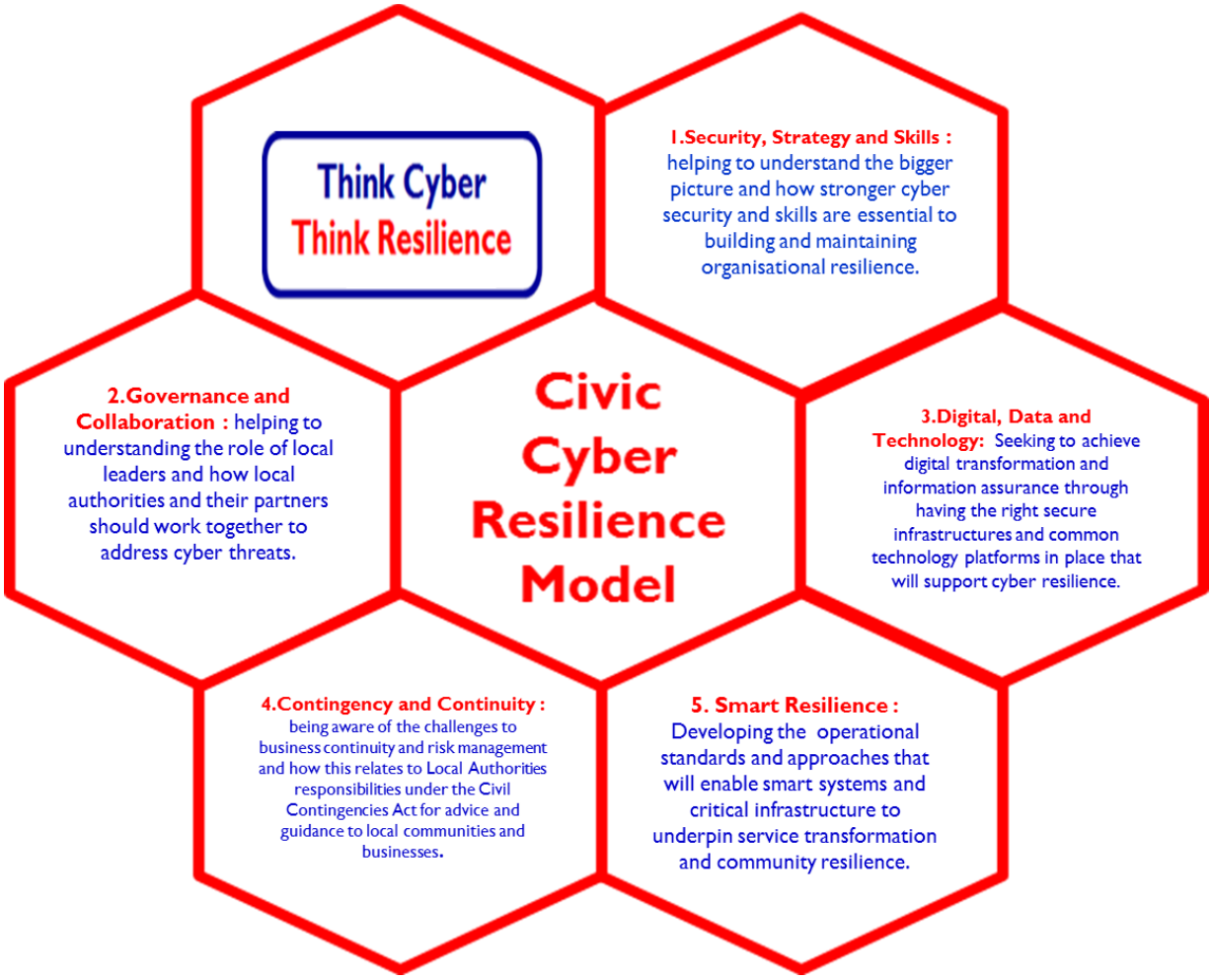
Perhaps the most profound issue is the need to think forward as to how we will continue to embrace digital services and maintain resilience. At the local level, digital leadership needs to re-focus some of these issues – they may seem to be abstract today but in the not too distant future they will be very tangible. More must be done to consider risk management based on potential harm and not just business impact, with greater use of modelling, planning and exercising consequence management.

Too often the cry is "That would never happen", but what if it did? What would the consequences look like? What would it cost? What would the harm be?

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