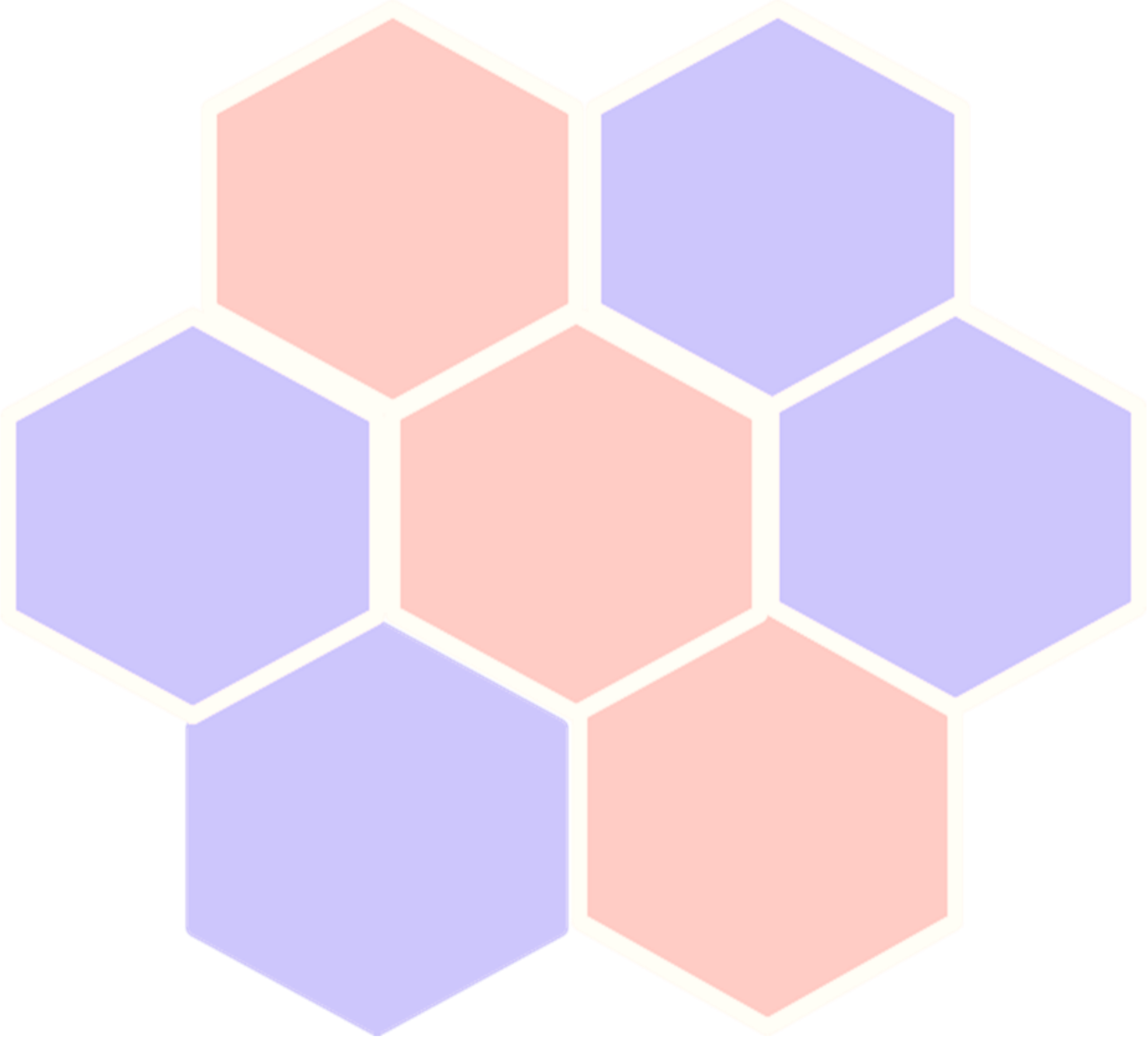
Think Cyber
Think Resilience

Building Resilience Together :
Briefing Paper

Leadership in practice: The role of strategic leadership in civic cyber resilience



CYBER UK STRATEGY

Think Cyber Think Resilience

iStandUK BRIDGING THE INFORMATION GAP

ST GEORGE'S HOUSE

Leadership in practice: The role of strategic leadership in civic cyber resilience.

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 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 and 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 though leadership round tables in association with **St George's House Windsor** to look at various aspects of Local Leadership in a Cyber Society. At these events senior leaders from local and central government, academia and civil resilience planners met to discuss emerging thinking around strengthening wider 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 need for taking a strategic approach to leadership issues arising from the civic cyber resilience agenda.

- ❑ **Understanding the cyber challenges: John Barradell**, Chief Executive, City of London Corporation, highlights three aspects of cyber risk and how they can be managed.

- ❑ **Cyber: the strategic response: Jos Creese**, former President of the British Computer Society and chief executive of CCL, highlights the role of governments to protect society from a 'less tangible' threat.

- ❑ **Set the cyber agenda and lead from the front: Graeme McDonald** Director SOLACE outlines how cyber security is rising rapidly up our consciousness and our organisations' risk registers.

- ❑ **Cyber, community resilience, localities and the digital divide : Stephen Baker**, chief executive of Suffolk Coastal and Waveney district councils, outline the cyber leadership dimensions of how digital services are now the 'default setting' for many in our communities.

Understanding the cyber challenges

John Barradell, Chief Executive, City of London Corporation, highlights three aspects of cyber risk and how they can be managed.

Cyber-attacks and online data theft are a daily reality for organisations across the UK. Most local authorities now experience multiple cyber-attacks every month. Cyber infrastructure is a vital and flexible tool for storing and collating data as part of our work providing services to our local communities.

But the very openness and flexibility of this tool can leave us vulnerable to attacks, compromising or harming our organisations with potentially profound reverberations for our communities.

There are three important, inter-linked aspects of the cyber risk. First, the risk is systemic, i.e. it affects every part of an organisation as we increasingly rely on cyber infrastructure to deliver services. Second, the risk is unconstrained by geography or sector – it is pervasive. Third, the risk is often invisible; experts say that cyber-attacks are increasingly going undetected.

This is why local authority leaders need to put cyber awareness at the heart of their work to make their organisations resilient.

What can leaders do to tackle this threat? In my view, a good place to start is to understand what 'cyber' really means in an organisational context. The term is often daunting to people and needs to be explained to non-technical colleagues - that it is short-hand for the use of technology to access information.

Moreover, cyber needs to be understood not just as an IT issue but as a form of risk management which should be embedded across all business plans and at all levels of the organisation. This means that appropriate governance structures need to be created to oversee and monitor risk mitigation programmes.

Training and awareness

There should also be regular training in and awareness-raising of cyber issues so that senior managers can remain up-to-speed on the overall risk picture and better understand risk mitigation. Information sharing partnerships such as CiSP (Cyber Information Sharing Partnership) are a useful way to seek advice, gain awareness of the current risks and learn from the experiences of others.

Part of the solution here has to be a shared analysis of how the cyber risk manifests itself. The City Corporation has worked with Deloitte to identify a few of these. Firstly, multiple system issues – ranging from slowdown, to part closure, to total failure. Secondly, regulatory and legal issues – failure to comply with regulatory requirements may lead to fines, while the spillage of private data could compromise long-term relations with key stakeholders. Thirdly, costs – the potential financial impacts of remedying problems such as data corruption might hinder service delivery or compromise supply chains.

The City's work with Deloitte demonstrated that these risks can be mitigated in various ways. This includes sharing sector-specific best practice, implementing trusted supplier mechanisms, creating well-resourced contingency infrastructure, eliminating single points of failure within systems, minimising insider threats through acceptable use policies, and regular stress-testing and table-top exercises.

The cyber threat now forms an indelible but invisible part of our working lives; understanding this threat must now form part of every leaders' toolkit. After all, when it comes to cyber risk an organisation is only as strong as its weakest link.

Cyber: the strategic response

Jos Creese, former President of the British Computer Society and chief executive of CCL, highlights the role of governments to protect society from a 'less tangible' threat.

It is a role of governments to protect. In the past that safeguarding has typically been against the so called 'four horsemen of the apocalypse' – war, famine, pestilence, and death. But today we have a fifth rider: cyber. Many criminals and malicious governments are turning to digital means to disrupt or to attack the business of industry and government, creating a whole new era of risks to our way of life and to our safety.

With the growing dependency in modern societies on digital infrastructure, traditional protection agencies need to be modernised to be able to deal with cyber threats. This includes the armed forces, police, fire, health and local emergency planning – all now need to have the capacity, capability and coordinated approach to handle cyber resilience risk, particularly at a local level.

The UK has always been served well by cyber security experts in government, with world class expertise in GCHQ in particular. Indeed, the UK has set a world lead, ever since the code breakers of WW2.

But the nature of the threat is diversifying, as digital networks and infrastructures are joined together. It is also not widely understood, because it's new, complex and less tangible than other more common risks such as flood, fire, disease, nuclear incident or failure of our energy or food supplies.

Integration vulnerability

For example, supply chains (business to business and business to government) are becoming automated and more integrated. Government digital infrastructure is increasingly homogeneous – such as the Public Services Network (PSN). These digital trends bring huge benefits, but also bring a need to ensure greater rigour in the design of security systems, in the routine detection and monitoring of threats, and in sophisticated mitigation response to minimise damage when risks materialise.

To be effective, it also requires closer working between all players in the digital services chain to balance ease of use with digital safety.

Consider the impact of the internet of things (IoT) – the growing network of physical objects which contain electronics, software, sensors, and network connectivity. These objects will soon be in every home, office, public space, our vehicles and in a variety of appliances we use and own. The cyber threat is not just to our privacy, but the extent to which these embedded objects can hold latent and undetected vulnerabilities that become a 'back door' to our networks and our data – nationally and locally.

We live in a world where a cyber-attack is easier, cheaper, faster, less detectable and potentially more damaging than any traditional form of malicious attack. The UK needs to build a new and strategic response to this, which integrates traditional services and is coordinated nationally and regionally, across public and private sectors.

For the UK to be prepared, that strategic level response must include:

- A pan-government approach, coordinated locally and nationally, with local civic leadership of integrated public protection planning.
- An assessment of which agencies need to work together to coordinate risk monitoring, alerts, sharing information and detection systems, as well as sharing best practice.
- A widespread public awareness campaign, to ensure the risks as well as the benefits of 'digital society' are better understood and communities and individuals can better protect themselves and their families from cyber threats.

Emergency planning

Current emergency planning services should in future be expected take on an obligation to prevent, detect and respond to cyber threats locally, running scenario tests and recognising that this is a complex and technically challenging topic, requiring specialist skills and experience.

The UK is a global leader in digital – advanced in ecommerce, open government, and cyber expertise. But a serious cyber security incident could seriously undermine digital government and digital business, let alone threaten our national security.

That makes cyber resilience one of the highest strategic priorities for local and national leaders alike.

Set the cyber agenda and lead from the front

Graeme McDonald Director SOLACE outlines how cyber security is rising rapidly up our consciousness and our organisations' risk registers.

In Judith Rodin's excellent book 'The Resilience Dividend', she outlines not just that resilience is important in terms of survival, but that whatever crises might come our way we can emerge from them stronger: "We can create and lead lives less shadowed by threat, develop communities and organisations that are more productive and innovative, and strengthen societies such that they are brimming with greater opportunities and prosperity."

When I think of resilience my thoughts turn immediately to accidents, terrorism and most prominently perhaps, the impact of climate change. But it is cyber security that is rapidly rising up our consciousness, our organisations' risk registers and feeding into major £1.9bn announcements by the Government.

Only recently local government was reminded by the case in Lincolnshire of the impact that malicious attacks on our IT systems can have on frontline services. Indeed, I can remember only too acutely the impact of a wayward memory stick at my own council which had a number of important service systems out of action for a number of days. It not only impacted on service provision – it also rocked the reputation of the organisation and our ability to modernise safely.

These examples have led to cyber security becoming an increasing concern, but it still remains shrouded in a little mystery with many of us non-experts unsure of what role to play and whether we form part of the problem, let alone solution. Impenetrable problems often leave us persuading ourselves that they are rightly the preserve of the expert, and ignoring the critical role we all play.

Need for action

There is no doubt that cyber security requires action right across an organisation. In a local authority where information comes in and out in so many channels and from a variety of partners, and where we seek to be as open and transparent as possible, this presents a real challenge.

We do rely on our specialists in some areas. We need them to build digital infrastructure that creates secure environments in which we can work, and applications that enable us to work with efficiency and effectively. But we won't escape the cyber threat by only relying on those experts.

The business as a whole needs to set the agenda on cyber security by identifying the risks which are the most important. Choices should be made so that we balance the risks identified, and the cost and business impact of mitigation. And finally, perhaps most importantly, non-specialists play a key role in driving behaviour change.

The whole organisation needs to use data thoughtfully, and to ensure that security is integrated into our business processes. For example, our procurement teams need to ensure our contracts are secure with intelligence terms and conditions that strengthen our cyber resilience. Security should be designed in at the outset.

However, as is so often the case, this type of cultural change is driven and modelled at the top. And it is important that the senior managers and their chief executives regularly give sufficient time to cyber security and its potential impact on the business of local government.

Key questions

It is tempting to ask the specialists to go away and develop a plan – and to see the top team's role as simply monitoring the progress of that plan and pushing when required. But there are a number of key questions that senior management teams can start to ask which ensure that the plan is real, measured and grounded:

- Which are our most important risks, and which are less important?
- What is the current level of capability focused on these important risks?
- How are trade-offs between risk and business need being made, and are they the right ones?
- Is the organisation engaged across all of its functions?
- Have we got the resource allocation right?

Asking these simple questions can help ensure that your organisation's response is both adequate and balanced. We have learnt that finance should not be just the preserve of the accountants, or communications the preserve of the communications team.

Similarly, our response to cyber threats should not be the preserve of IT. It requires a range of responses from across organisations – not least a change in all our behaviour to ensure that our data is used safely and is protected.

Top teams need to set this agenda, balance the risks and lead.

Cyber, community resilience, localities and the digital divide

Stephen Baker, chief executive of Suffolk Coastal and Waveney district councils, outline the cyber leadership dimensions of how digital services are now the 'default setting' for many in our communities.

Digital services are now the 'default setting' for many in our communities. The use of online services, whether for shopping, banking, entertainment or advice is now a natural choice for many of our residents.

We have also played our part in encouraging this; not only have the retail and finance sectors recognised how services can be more efficient and accessible if provided online, but so have the public sector. Providers such as the DVLA have surged ahead with online services whilst others, such as local councils, have also provided a myriad of local services through digital applications and online access, driven by an ambition to improve accessibility to, and responsiveness of, services and to reduce costs.

However, with this new innovative, digitised, approach comes a range of new challenges and responsibilities. As communities and residents become more reliant on such services, and as the new level of instant access becomes the norm, we need to ensure that these services are resilient. This aspect of 'community resilience' is a new issue to address, and needs new thinking.

The term 'digital divide' is heard less often these days. Previously it referred to the gulf between the users and non-users of digital services. There is no doubt that such a gap still remains, but now the term can be applied to a new, extended, definition: namely the difference, in terms of access, between those with superfast broadband and 4G mobile, and those who still measure their broadband speed in kilobytes per second and are plagued by 'not spots' in their mobile signal. To deliver community resilience these issues concerning the access to adequate networks and minimising the fragility of those networks, must be addressed.

Skills aspect

For some residents and communities the speed of the network is irrelevant because they lack the skills to exploit its potential. This is another aspect of community resilience that must be addressed. Digital services can be life changing for some of the most vulnerable in our communities, those who rely on more support than others, yet a lack of skills constrains their engagement, and reduces the potential benefit considerably. Beyond skills lies the issue of 'confidence'.

Users of digital services, especially of those services that are critical to their well-being and involve personal data, must be confident that the online service will be delivered, and that their data is secure. Too often users still prefer to submit a claim form as hard copy, as this provides them with a degree of comfort that an online submission does not. However, if that claim is for a benefit that puts food on the table then one can understand why that is more important than, perhaps, a DVD being delivered by an online retailer.

What is the role of government in ensuring community resilience? Perhaps we need to act as advocates for local communities, such as when a broadband service is lost and a repair is expected to take weeks, rather than days (or better still, hours).

Certainly we should provide leadership to local communities, giving them the confidence they need to become resilient, providing the support they need to address local issues, and offering the encouragement that may be the difference between collaborative and networked communities, and those that are disconnected and not recognising the full potential of digital services.

Local focus

With some support communities can develop the skills base, and level of confidence, for themselves. Indeed, a local approach will have the advantages of providing a local focus, with local reference points within the community. With support, local community leadership can help to address the issue of community resilience, and a community that is self sustaining will always be more resilient.

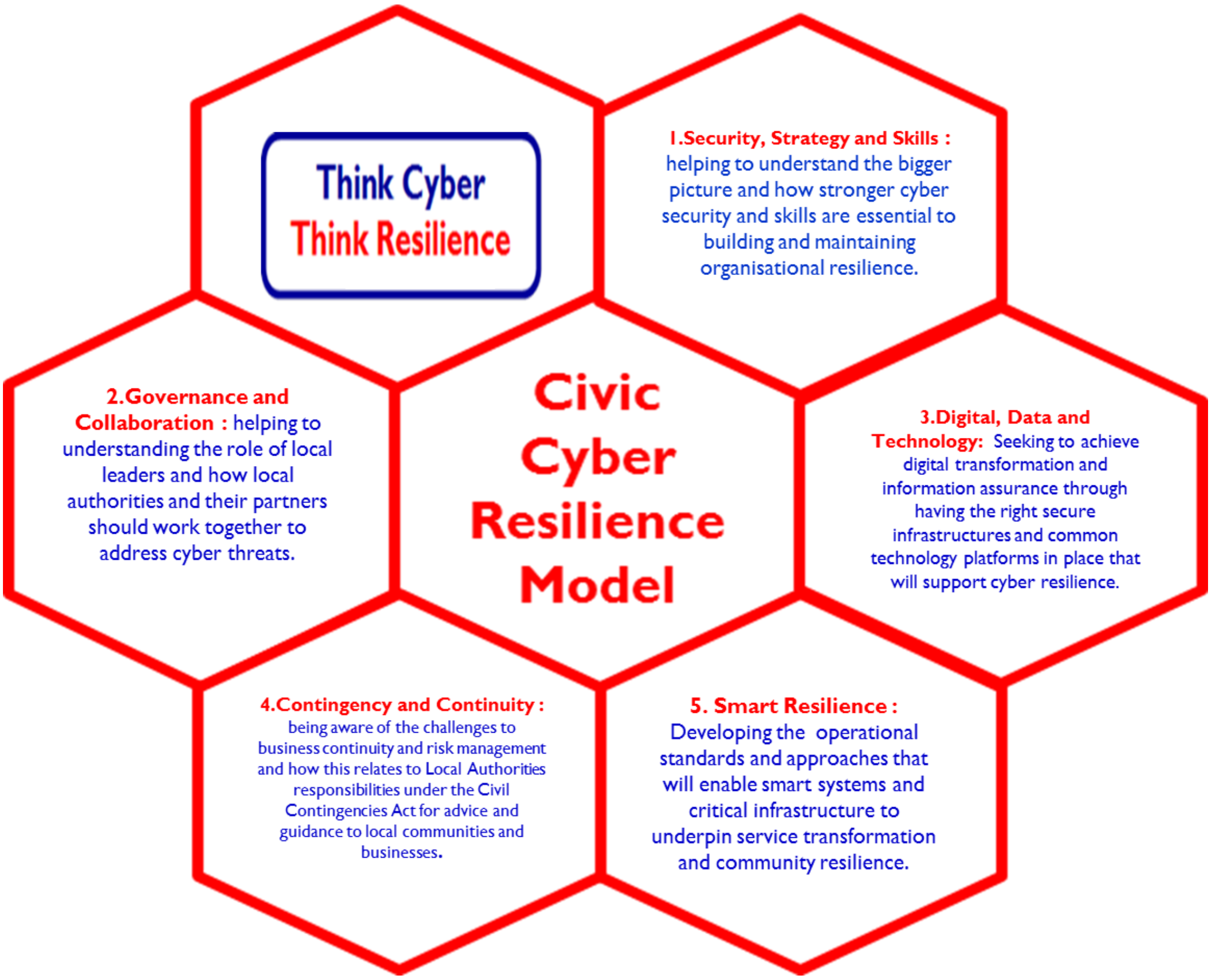
However, where communities are likely to require support and guidance is with addressing the issue of cyber security. A reliable source of advice and guidance on how to safeguard against cyber threats will become more and more critical. Whether it's a local community group trying to provide information online or a local resident trying to access services, cyber security is important to both the continuity of service provision, and confidence in ongoing service use and access.

Government, whether national or local, is ideally placed to provide a source of trusted and reliable support for communities as they become more aware of, and respond to, the need for greater cyber security.

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



1.Security, Strategy and Skills : helping to understand the bigger picture and how stronger cyber security and skills are essential to building and maintaining organisational resilience.

2.Governance and Collaboration : helping to understanding the role of local leaders and how local authorities and their partners should work together to address cyber threats.

3.Digital, Data and Technology: Seeking to achieve digital transformation and information assurance through having the right secure infrastructures and common technology platforms in place that will support cyber resilience.

4.Contingency and Continuity : being aware of the challenges to business continuity and risk management and how this relates to Local Authorities responsibilities under the Civil Contingencies Act for advice and guidance to local communities and businesses.

5. Smart Resilience : Developing the operational standards and approaches that will enable smart systems and critical infrastructure to underpin service transformation and community resilience.

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/).

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)

❑ **OECD Public Sector Innovation Observatory –** for the **Think Cyber Think Resilience** international exemplar case study**.** (https://www.oecd-opsi.org/)

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

Think Cyber Think Resilience: Awarded OECD Public Sector Innovation Exemplar Status April 2017

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