Think Cyber
Think Resilience

Building Resilience Together :
Briefing Paper

Resilience in practice:

Practical steps that civic organisations can take to be cyber resilient

CYBERUK STRATEGY

Think Cyber
Think Resilience

iStandUK
BRIDGING THE INFORMATION GAP

ST GEORGE'S HOUSE

Resilience in practice: Practical steps that civic organisations can take to be cyber resilient.

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 some of the practical steps that civic organisations can take to be cyber resilient.

- **Building the right mind set for information assurance: Ian Dyson**, Commissioner of the City of London Police, outlines the key to successfully protecting against loss or vulnerability of data and information is a comprehensive information assurance programme

- **Building cyber risk management capabilities: Mark Brett**, honorary visiting fellow at De Montfort, highlights there is much to learn from existing risk management methodologies when it comes to cyber resilience.

- **Developing the 'Protect and prepare' cyber resilience response : Richard Berry**, Assistant Chief Constable at Gloucestershire, outlines how civic resilience planning needs to be adapted to cope with the cyber age.

- **Civil contingencies, resilience planning and cyber risks: Mick Free** Civil Protection Advisor looks at how too firmly embed cyber into national and local civil protection arrangements.

Building the right mind set for information assurance:

Ian Dyson, Commissioner of the City of London Police, outlines the key to successfully protecting against loss or vulnerability of data and information is a comprehensive information assurance programme

Information management, security and assurance within the cyber debate are often focussed upon the technical challenges and threats. But the key to successfully protecting business against any loss or vulnerability of data and information is through a much more comprehensive information assurance programme.

Very often, responsibility for this can sit within an IT department or with those with technical expertise. While those experts are required to deliver some of the more complex or technical aspects of the business, the most important thing is for any organisation to have a framework against which they can assess their entire business against vulnerability to the loss of information.

There are now a number of models that can be used to do this. There is the ISO 27000:2013 framework, from the Government there is the Information Assurance Maturity Model (IAMM) and 10 Steps to Cyber Security, as well as other products on the market from the private sector that can provide that holistic framework. These look at the security of information across people, process and technology within a number of dimensions such as governance, procurement, training, etc.

In order for this to be effective, it requires leadership from the top of the organisation. In the City of London Police, I have chaired a regular information management board with leadership at the senior level of the organisation. Technical experts from information management and IT are attendees and contributors at the meeting but do not lead it.

We have used the information assurance maturity model to self-assess our performance against all of the dimensions (there are six core elements to the model) and there are five tiers of maturity.

Time to mature

It will take any organisation a significant period of time to reach maturity. Investment has to be made in governance, IT infrastructure, training, health checks, maintenance, patching, and clear and auditable policies around the management of information. As part of our continuous improvement approach to information assurance we are also assessing our compliance with the ISO 27000:2013 standard, and will be enhancing our information security management system with these additional controls.

But once achieved it will create a culture that considers information security as a part of its day-to-day business.

It cannot be done by a few people in a department; it has to be across the organisation. The first step we took was to create an information asset register which showed all of the information assets, including services, in which information is held within my police force. I

can guarantee every organisation that does this will find there are more assets than was first thought.

Once this inventory was drawn up, an information asset owner (IAO) was assigned to each asset. This needs to be somebody in the business who operates and uses the system on a regular basis and therefore understands what purpose the information is stored for, who is entitled to use it, who should have access and how is that access audited.

Strategic risk manager

We recognised a need to create a two-tier system of asset ownership. So, we also have a senior information asset owner (SIAO). They have clear authority to manage the strategic risks for the system and can allocate resources to support the IAO in the operation of their asset. We have established six SIAOs and ensured clear reporting lines to myself as the senior information risk owner.

The National Archives provides training for information asset owners and I use this across my organisation. I found it to be extremely beneficial in developing a mindset and a culture within the organisation of good information management.

So, 18 months on, I now have a robust and accurate information asset register; I have IAOs who understand their business; and I have a regular monthly assessments against red, amber, green made by my information security officer on the vulnerabilities or otherwise of information stored within any system. I have found that by using the IAMM (but it could be any model that looks across all dimensions) one can change the culture of an organisation to one where the biggest vulnerability to information loss, your people, have actually got the right mindset.

Building cyber risk management capabilities:

Mark Brett, honorary visiting fellow at De Montfort, highlights there is much to learn from existing risk management methodologies when it comes to cyber resilience.

Looking at existing risk management methodologies there are various approaches that can help in the cyber resilience space. The key is to understand where the touch points are, what we're trying to mitigate against, and with what, where and when.

The traditional space was around people place and incident. This model has served policing well for a long time.

In the 1970s ICL developed their data dictionary for database entity modelling, which crossed over from the physical tangible world to the intangible work of ICT systems and data models. The model works because most ICT systems aim to facilitate or enable a physical business process.

However, the evolving internet of things (which is going to explode metaphorically) operates the other way round, with physical things interacting with the intangible cyber world.

In order to plan and model this new complex world, we need the language, descriptions, standards and metadata to enable it all. Without understandable frameworks and models, it is not possible to describe, develop and manage risks.

Local public services need a language, metadata and schemas to facilitate the modelling of abstractions that exist in cyber space. Once we can articulate the problems, through conceptual frameworks, we can begin to qualify value and understand the real problems and issues.

This eventually leads to the development of mathematical models and algorithms, which in turn can be used to detect anomalous behaviours in networks and communications systems. This makes is possible to develop risk mitigations for problems that do not yet exist.

Increasing complexities

Technological change will increase the demand, pace and complexities of cyber space. Local public services are already looking at the use of telematics and assistive technologies, but we must also look at the potential risks and implications.

New technologies can help to improve quality of life and drive out savings – but they also open the way for new attack vectors, exploits and harm. Criminals and other adversaries will be quick to exploit these.

For example, we know that when we go on holiday we should not advertise that our homes are empty – but what if criminals could just tap into you heating hive or smart meter or alarm system to detect your house is empty? How many of us post photos on social media advertising the fact that we are on a beach or other exotic location far from home?

Nor is it just criminals that we have to keep out – other adversaries will be equally quick to learn to exploit the new tools and techniques out there.

Therefore, we need to develop new methodologies for risk management and mitigation against those risks.

Disrupt and impede

Yes, technology can help to disrupt and impede attacks. Automated systems monitor networks and detect anomalies, but we should not be over-reliant on automated detection.

We need to raise awareness at all levels within the organisation and across our delivery chains. Awareness raising and training is the best defence we have, coupled with a culture that encourages the reporting of incidents quickly. This will need a change of stance from the information commissioner, especially when accidental human error was the cause.

We may not be able to stop all attacks or incursions into our networks – we may never win the cyber war as the odds are stacked against us – but we can disrupt and impede a lot of it.

Risk management, whether physical or cyber risks, requires leadership; it is about increased understanding of the issues, raising awareness about the impacts, and changing social norms or the expectations of society in how risks are handled.

Developing the 'Protect and prepare' cyber resilience response:

Richard Berry, Assistant Chief Constable at Gloucestershire, outlines how civic resilience planning needs to be adapted to cope with the cyber age.

Although a recent development, civic resilience planning was developed for a non-digital age. Existing planning needs to be adapted to cope with the special considerations required for cyber resilience. Only then can we outline the areas for capability development needed for the Local Resilience Forum (LRF) network.

The Civil Contingencies Act is legislation born out of threats from a predominantly non-digital age. Consequently, it can be argued that we should not seek to shoehorn analogue legislation and practices into cyber and digital challenges.

However, at this time there is very little mature understanding of what can be adapted from the wealth of 'pre-digital' resilience experience which presently exists within the UK and what should be 'genuinely new'. Having been a gold commander in a real cyber incident I am more than aware of the problems which can be faced when responding to a cyber incident.

Cyber presents a number of key challenges for LRFs. These may include all or some of the following features:

- It can thoroughly disrespect any notion of geography and an emergency which can be easily defined to a particular locality.
- Events can be multi-seated between commercial and civil organisations.
- Cyber incidents require different responders, partners, and decision-making processes to the normal multi-agency responses, and civil liabilities can be very different.
- The responders themselves may be affected by the cyber-attack thereby affecting their ability to provide support.
- The velocity of event can require sometimes near real time decision making as threats manifest in different ways with changes in needs.
- Managing responses between the real and virtual worlds can be complex and require refined coordination; i.e. between the technical conversations and the operational decisions.
- The networks required to protect, test, exercise and prepare are under developed.
- There is little locally meaningful threat discovery intelligence available which could inform LRF assessments and their statutory duty to 'prepare' and exercise.

This list is not exhaustive and at first sight it might be a little daunting. The key to success however is to develop a staged model of change:

- The preferred first stage of change being pilot project to 'discover', scope, develop and test resilience planning frameworks.
- The natural second stage is to provide the necessary briefing, development and progression of wider cyber resilience planning on the most suitable basis –regions, cities or nationally managed roll out projects. Once products have been developed these could be easily shared in order to optimise public benefit and value.

- A final third stage is testing and exercising, tying the LRF community into cyber 'prepare' events with industry and other central government bodies.

This three phased approach would requires leadership and organisation; it will need to work across the Department for Communities and Local Government and the LRF network, with strong engagement with policing and other stakeholding agencies. The sustainability of cyber civil resilience will also require learning and training events, incorporating cyber threat related capabilities into normal LRF business.

Civil contingencies, resilience planning and cyber risks:

Mick Free Civil Protection Advisor looks at how too firmly embed cyber into national and local civil protection arrangements.

Structured and consistent planning for civil contingencies is a relatively new concept and one that has rapidly evolved over a short period of time. With the ever developing threat of cyber-attacks, it is now time to firmly embed cyber into national and local civil protection arrangements.

Legislation to define and govern the preparation for civil emergencies in the UK is a 21st century concept (previous civil protection legislative provisions were predicated on 'cold war' planning arrangements).

The Civil Contingencies Act 2004 (CCA) was born out of the series of incidents that started with serious flooding in 1998. This was followed in 2000 by the national fuel crisis; the national foot and mouth outbreak in early 2001; and globalisation of the radical Islamic terrorist threat following the attacks in the United States on 11 September 2001.

Following the events of 9/11 the UK Government established the Civil Contingencies Secretariat (CCS) within the Cabinet Office to co-ordinate resilience planning across all government departments. This included the establishment of both a ministerial and an official level committee to provide national leadership and oversight of UK resilience arrangements. Since 2010 these have been sub-committees of the National Security Council (NSC).

The CCS also developed and continues to maintain the National Risk Assessment (NRA) – a matrix of national threats and hazards – and the UK Capabilities Programme (now National Resilience Capabilities Programme - NRCP). Produced after 9/11 this provides a programme of work, under ministerial leadership, that covers three areas:

- Structural arrangements – to make sure that the frameworks for coordinating and directing an emergency response are in place.
- Central response – Cabinet Office supports central government departments to work together effectively in responding to an emergency.
- Functional workstreams – including mass casualties, mass fatalities and infectious diseases (each with a designated lead department).

The UK now has well established resilience planning arrangements with the focus on local executive leadership through the work of the local resilience forums (LRFs).

Generally mirroring police force areas, their main purpose is to ensure that each Category 1 responder (primarily emergency services, local authority and other key government agencies) within the LRF can deliver its functions as far as necessary or desirable, to prevent or mitigate the effects of an emergency. Each LRF should consider both the NRA and the supporting national resilience planning assumptions (NRPA) in developing a local risk register and contributing to the NRCP.

Omission

However, despite publication of the National Cyber Security Strategy 2016–21 and being listed as a tier 1 threat in the 2016 National Security Strategy, cyber threats are not part of the NRCP. It would appear that the omission of cyber from the NRCP has contributed to it not being included in the resilience arrangements of the majority of LRFs.

The inclusion of cyber resilience as a workstream within the NRCP would have a number of substantial benefits. It would assist in:

- Helping to place this area firmly on the agenda of LRFs.
- Identifying clear ministerial leadership and support for cyber issues within local resilience partnerships.
- Contributing to shaping and assisting the work of the National Cyber Security Centre.
- Supporting the National Cyber Security Strategy, strategic outcome three (under Defend), by which the UK has the capability to manage and respond effectively to cyber incidents to reduce the harm they cause to the UK and counter cyber adversaries.

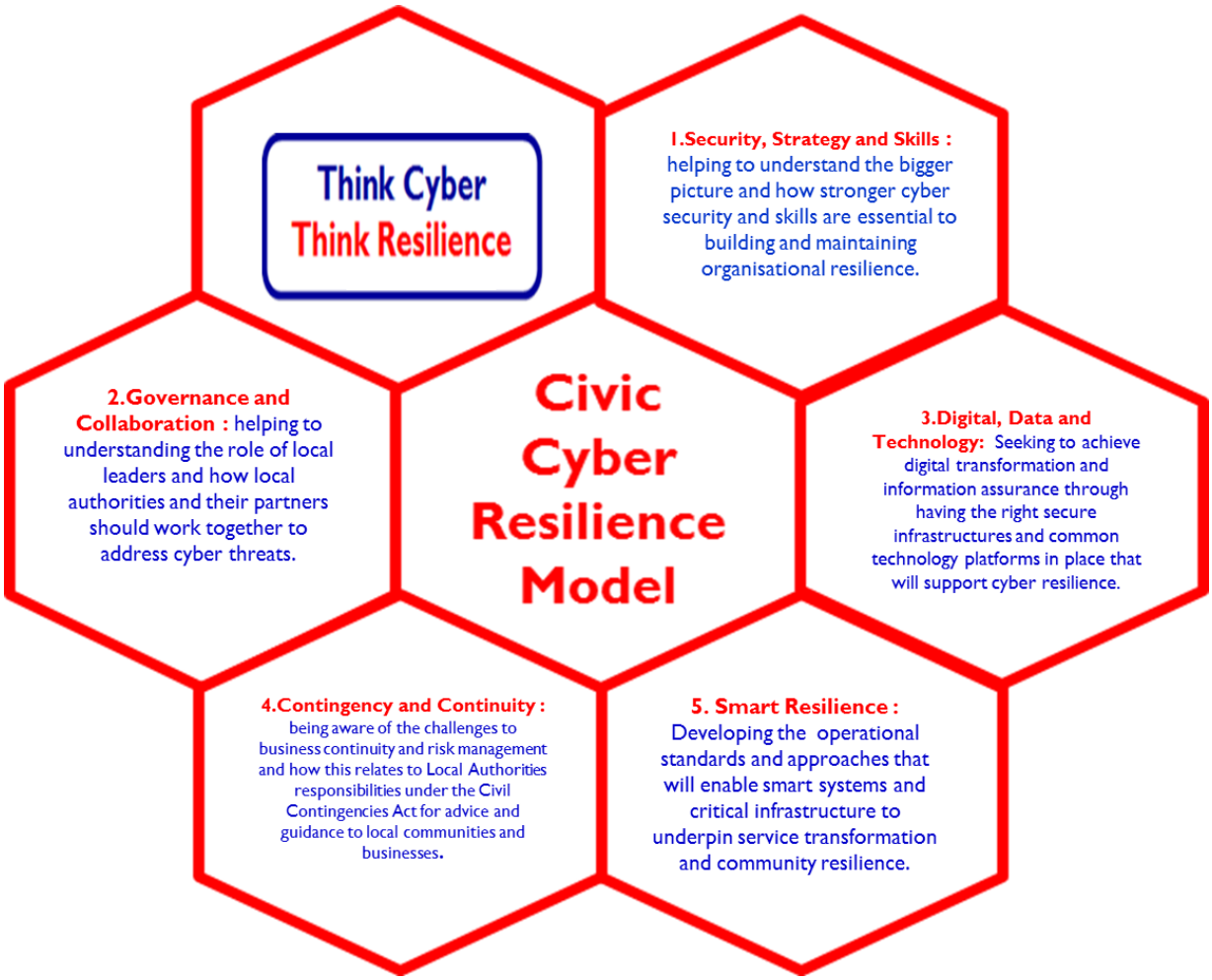
Matters of local resilience (including cyber) can only be effectively dealt with through the LRFs. Anything less undermines the CCA and the concept of joint resilience planning and response where it matters most – in local communities.

Hopefully, the work we have been doing looking at cyber resilience with the Association of Greater Manchester Authorities, the City of London and Gloucestershire will help to formulate a model for other LRFs to imbed this into their local resilience programmes.

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/).

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

OECD Observatory of Public Sector Innovation

iNetwork involve influence inspire

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