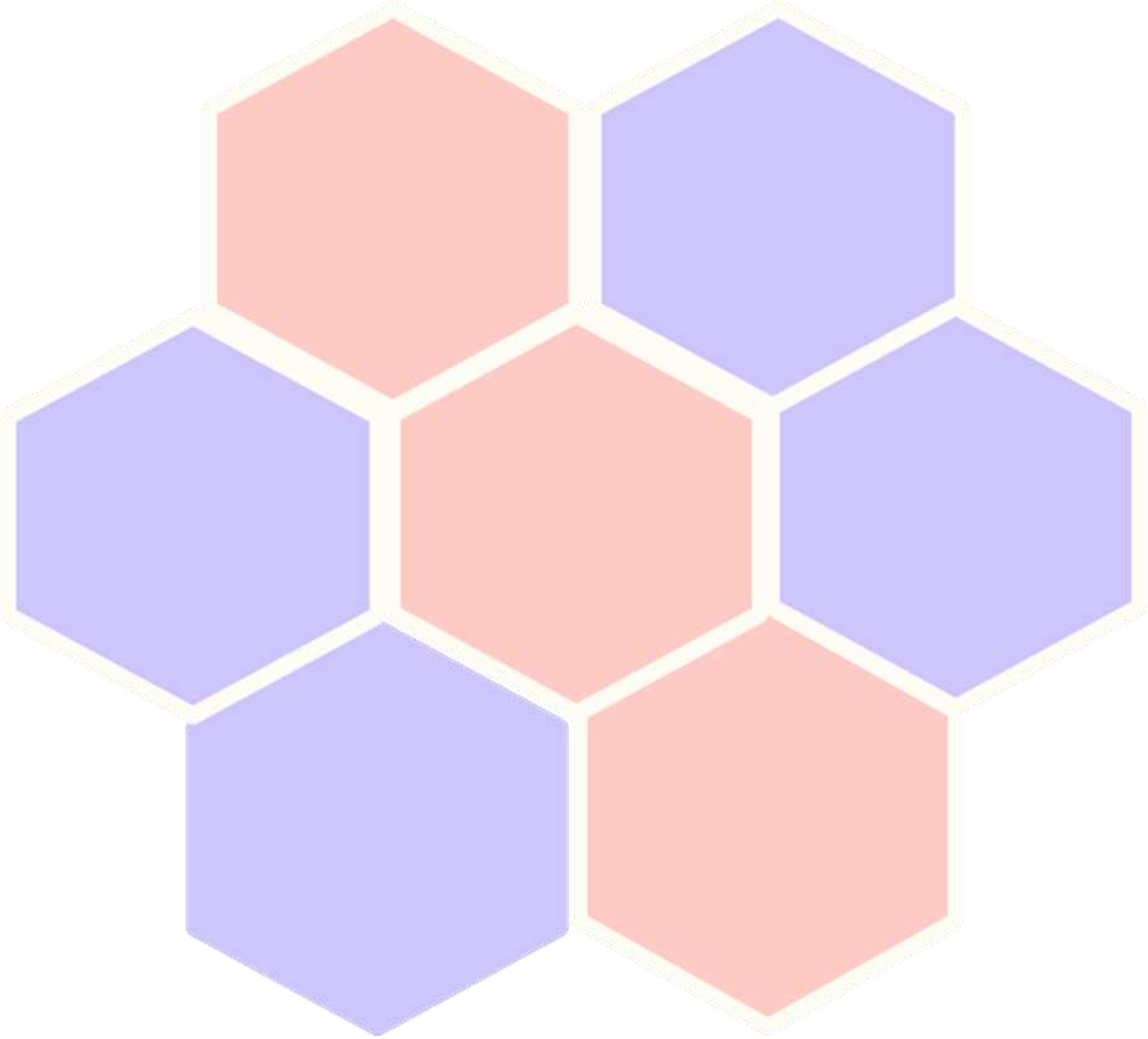
Think Cyber
Think Resilience

Building Resilience Together :
Briefing Paper

Cyber Emergence Response: Understanding the role of a Computer Security Incident Response Team (CSIRT)



CYBER UK STRATEGY

Think Cyber Think Resilience

iStandUK BRIDGING THE INFORMATION GAP

ST GEORGE'S HOUSE

Cyber Emergence Response: Understanding the role of a Computer Security Incident Response Team (CSIRT)

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.

The need for local leaders, policy makers and practitioners to have a better understanding of cyber emergency response capabilities has been a recurring theme amongst roundtable participants and how these can help inform closer working across agencies, Local Resilience Forums (LRFs) and Warning and Advice Reporting Points WARPs).

This booklet outlines the basic cyber emergency response capabilities that are contained in the internationally recognised Carnegie Mellon's Software Engineering Institute Computer Security Incident Response Team (CSIRT) model [1] which the Think Cyber Think Resilience roundtable delegates have identified as helpful reference framework for building up organisational cyber security and resilience across localities.

[1] Computer Security Incident Response Team (CSIRT) service framework see Carnegie Mellon's Software Engineering Institute model

The role of a Computer Security Incident Response Team (CSIRT)

A Computer Security Incident Response Team (CSIRT) is a service organisation that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client.

A CSIRT can be a formalized team or an ad-hoc team. A formalised team performs incident response work as its major job function. An ad-hoc team is called together during an ongoing computer security incident or to respond to an incident when the need arises. Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. When computer security incidents occur, it will be critical for an organization to have an effective way to respond.

The speed with which an organization can recognise, analyse, and respond to an incident will limit the damage and lower the cost of recovery. A CSIRT can be on site and able to conduct a rapid response to contain a computer security incident and recover from it. CSIRTs may also have familiarity with the compromised systems and therefore be more readily able to coordinate the recovery and propose mitigation and response strategies.

Their relationships with other CSIRTs and security organizations can facilitate the sharing of response strategies and early alerts to potential problems. Proactively, CSIRTs can work with other areas of the organization to ensure new systems are developed and deployed with "security in mind" and in conformance with any site security policies. They can help identify vulnerable areas of the organization and in some cases perform vulnerability assessments and incident detection.

They can focus attention on security and provide awareness training to the constituency. CSIRTs can also provide expertise to do preventive and predictive analysis to help mitigate future threats.

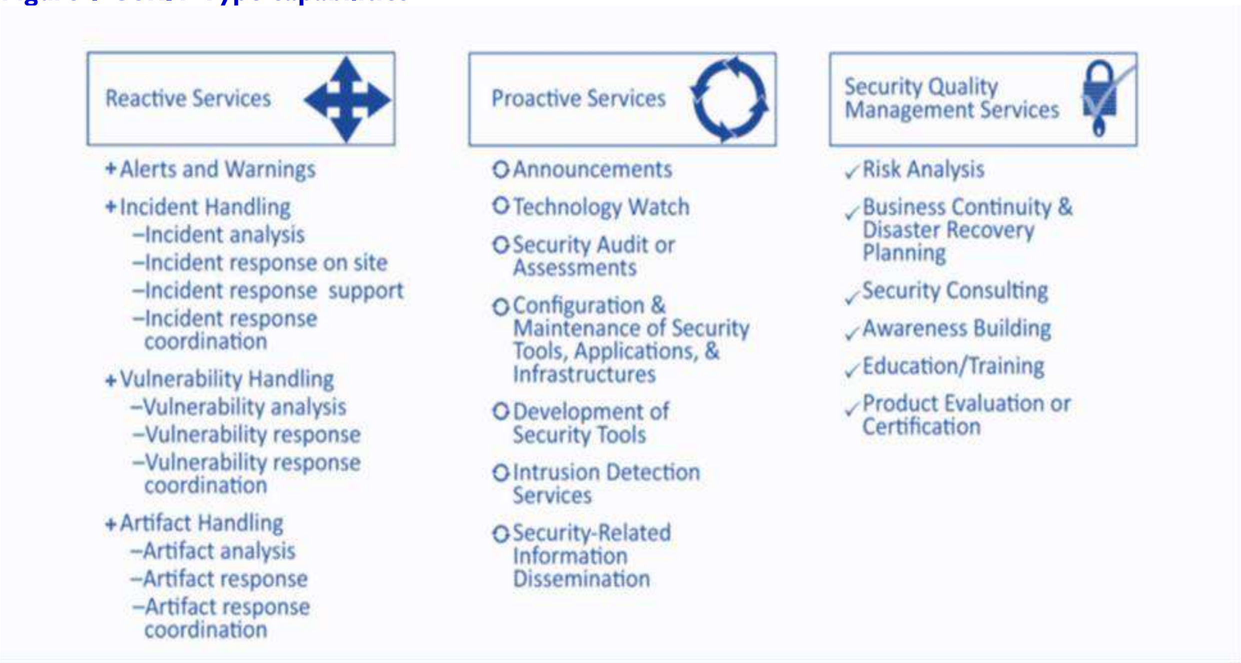
The specific services provided vary from one CSIRT to another. A computer security incident can involve a real or suspected breach or the act of wilfully causing a vulnerability or breach. Typical incidents include the introduction of viruses or worms into a network, DoS (denial of service) attacks, unauthorized alteration of software or hardware, and identity theft of individuals or institutions. Hacking in general can be considered a security incident unless the perpetrators have been deliberately hired for the specific purpose of testing a computer or network for vulnerabilities. (In that case, the hackers can form part of the CSIRT, in a preventive role.) CSIRTs may provide proactive services, such as end-user security training, besides responding to incidents.

Response time constitutes a critical consideration in assembling, maintaining and deploying an effective CSIRT. A rapid, accurately targeted, and effective response can minimize the overall damage to finances, hardware, and software caused by a specific incident. Another important consideration involves the ability of the CSIRT to track down the perpetrators of an incident so that the guilty parties can be shut down and effectively prosecuted. A third consideration involves "hardening" of the software and infrastructure to minimise the number of incidents that take place over time.

There are then many services, which a CSIRT can choose to offer. Each CSIRT is different and provides services based on the mission, purpose, and constituency of the team. Under the Carnegie Mellon's Software Engineering Institute model [2] services can be grouped into three categories:

- **Reactive services**. These services are triggered by an event or request, such as a report of a compromised host, widespread malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work.
- **Proactive services.** These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.
- **Security quality management services**. These services augment existing and well-established services that are independent of incident handling and are traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

Figure 1 CSRIT Type capabilities


Reactive Services
+Alerts and Warnings
+Incident Handling
–Incident analysis
–Incident response on site
–Incident response support
–Incident response coordination
+Vulnerability Handling
–Vulnerability analysis
–Vulnerability response
–Vulnerability response coordination
+Artifact Handling
–Artifact analysis
–Artifact response
–Artifact response coordination
Proactive Services
O Announcements
O Technology Watch
O Security Audit or Assessments
O Configuration & Maintenance of Security Tools, Applications, & Infrastructures
O Development of Security Tools
O Intrusion Detection Services
O Security-Related Information Dissemination
Security Quality Management Services
✓Risk Analysis
✓Business Continuity & Disaster Recovery Planning
✓Security Consulting
✓Awareness Building
✓Education/Training
✓Product Evaluation or Certification

[2] Computer Security Incident Response Team (CSIRT) service framework see Carnegie Mellon's Software Engineering Institute model Also see international examples: -

- US Department of Homeland Security: https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams
- New Zealand Government: https://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf
- Organisation of American States (study sponsored by Canadian Government): https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf
- ENISA's CSIRT-related capacity building activities: https://www.enisa.europa.eu/publications/leading-the-way-enisa-s-impact-in-operational-security
- Janet Network CSIRT https://www.jisc.ac.uk/csirt
- University of Cambridge Computer Emergency Response Team (CamCERT):https://help.uis.cam.ac.uk/user-accounts-security/security/camcert

Reactive Services

Reactive services are designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems.

- **Alerts and Warnings:** this service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected.

- **Incident Handling:** this involves receiving, triaging, and responding to requests and reports, and analyzing incidents and events.

- **Vulnerability Handling:** this involves receiving information and reports about hardware and software vulnerabilities; analyzing the nature, mechanics, and effects of the vulnerabilities; and developing response strategies for detecting and repairing the vulnerabilities.

- **Artifact Handling:** this involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorized or disruptive activities. Once received, the artifact is reviewed. This includes analyzing the nature, mechanics, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts.

Proactive Services

Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

- **Announcements:** Announcements include, but are not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

- **Technology Watch:** The CSIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies.

- **Security Audits or Assessments:** This service provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards that apply. It can also involve a review of organizational security practices.
- **Configuration and Maintenance of Security Tools, Applications, Infrastructures, and Services:** This identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CSIRT constituency or the CSIRT itself.

- **Development of Security Tools:** This service includes the development of any new, constituent-specific tools that are required or desired by the constituency or by the CSIRT itself. This can include, for example, developing security patches for customized software, and developing tools or scripts that extend the functionality of existing security tools, such as a new plug-in for a vulnerability or network scanner, scripts that facilitate the use of encryption technology, or automated patch distribution mechanisms.

- **Intrusion Detection Services:** CSIRTs can perform this service view reviewing existing IDS logs, analyze and initiate a response for any events that meet their defined threshold, or forward any alerts according to a pre-defined service level agreement or escalation strategy.

- **Security-Related Information Dissemination:** This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security.

Security quality management services.

These services augment existing and well-established services that are independent of incident handling and are traditionally performed by other areas of an organization such as the IT, auditing, or training departments.

- **Risk Analysis:** CSIRTs may be able to add value to risk analysis and assessments. This can improve the organization's ability to assess real threats, to provide realistic qualitative and quantitative assessments of the risks to information assets, and to evaluate protection and response strategies.

- **Business Continuity and Disaster Recovery Planning:** Based on past occurrences and future predictions of emerging incident or security trends, more and more incidents have the potential to result in serious degradation of business operations.

- **Security Consulting;** CSIRTs can be used to provide advice and guidance on the best security practices to implement for constituents' business operations. This service includes providing guidance and assistance in developing organizational or constituency security policies. It can also involve providing testimony or advice to legislative or other government bodies.
- **Awareness Building:** CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies.

- **Education/Training:** This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials.

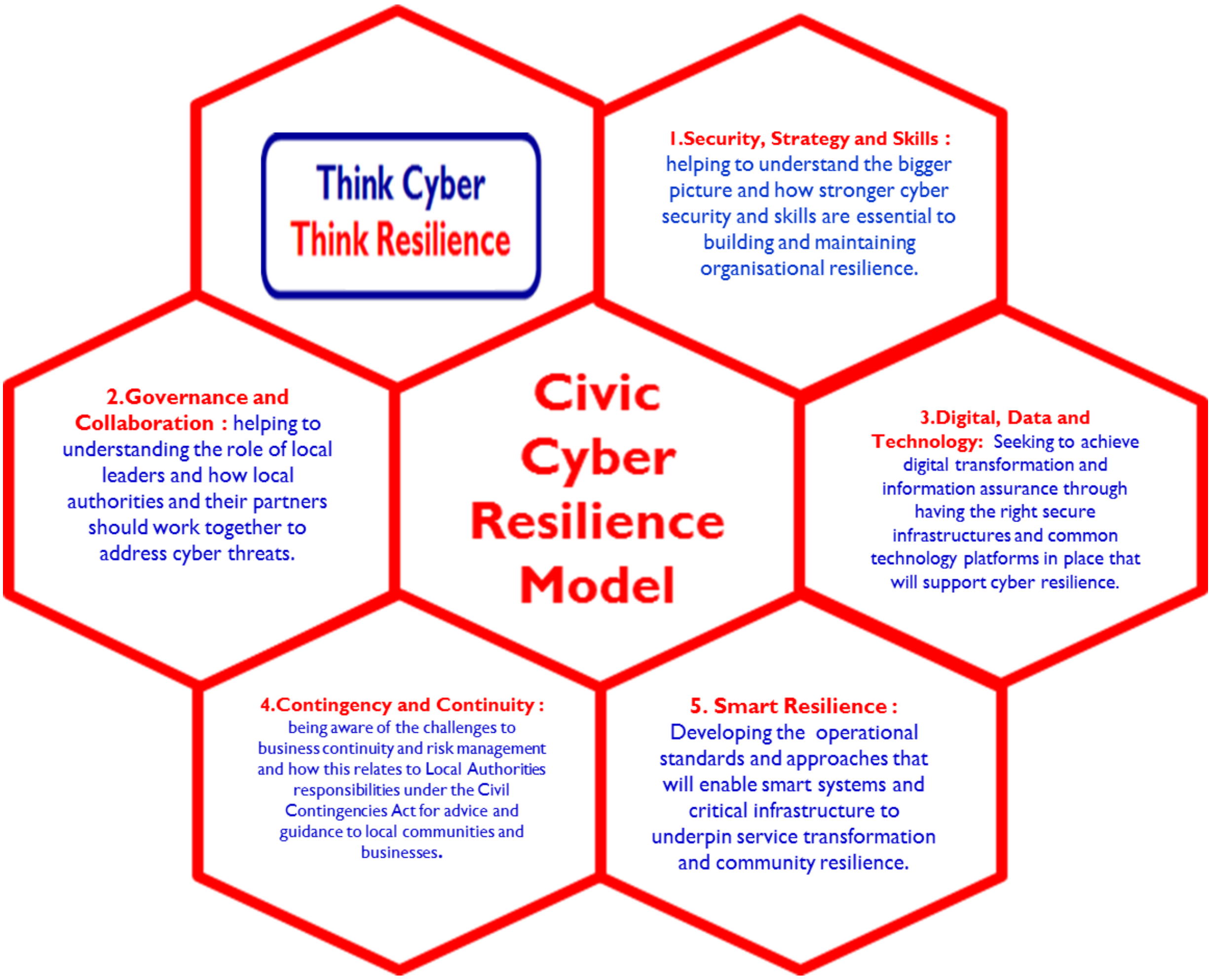
- **Product Evaluation or Certification:** For this service, the CSIRT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable CSIRT or organizational security practices.

"Extract from the Carnegie Mellon's Software Engineering Institute model for CSIRT services"
September 2017 (updated July 2019)

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)

❑ **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: 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.

To find out more visit: www.stgeorgeshouse.org

iNetwork: 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.

To find out more visit: www.i-network.org.uk

Society of IT Managers: 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.

To find out more visit: www.socitm.net

Society of Local Authority Chief Executives: 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 most 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.

To find out more visit: www.solace.org.uk

National Local Authority WARP and CyberShare: The National Local Authority WARP (NLAWARP) is a not for profit programme which was created in 2009 at the end of a government funded programme of work to establish the regional local government Warning and Advice Reporting Points (WARP). NLAWARP is self-sustaining and works to facilitate regional WARP coordination and provides support services to several of the WARPs.

CyberShare is not for profit initiative to support of improving cyber emergency response capabilities and awareness across the WARP community which is being piloted (2019/20) with NCSP support across a test group of local authorities. The intention being that the initiative will going forward, look to provide incident response training, exercising and provide cyber threat intelligence to assist local government through a central fusion cell and several distributed regional nodes.

To find out more visit: www.nlawarp.net and www.cybershare.net

Research Institute in Science of Cyber Security: RISCS takes an evidence-based and interdisciplinary approach to addressing cyber security challenges. By providing a platform for the exchange of ideas, problems and research solutions between academia, industry, and both the UK and international policy communities, RISCS promotes and supports the development of scientific approaches to cyber security. Central to the RISCS agenda is the application of bodies of knowledge to stimulate a transition from 'common practice' to 'evidence-based best practice' in cyber security. Recognising that cyber security is a contested concept, RISCS operates within a national and international cyber security framework to establish a coherent set of research principles. These principles focus on the deployment of scientific methods and the gathering of evidence to produce sound interventions and responses to cyber security challenges.

We actively seek to maximise collaboration amongst our diverse community through a culture of open publication, sharing and expanding our network. Through this collaboration, RISCS develops techniques that enable communities to anticipate emergent cyber security issues from public policy, social practice and technological perspectives. Our end goal is to deliver a world-class portfolio of activity and research findings that maximises the value of social, political and economic research into cyber security and which results in a set of scientifically based options that individuals, institutions and nation states can use to respond to imminent and long-term cyber security challenges. RISCS is managed by a team based in University College London's Department of Science, Technology, Engineering and Public Policy (UCL STEaPP).

To find out more visit: www.riscs.org.uk

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

T