Think Cyber
Think Resilience
Building Resilience Together

ST GEORGE'S HOUSE

St George's House Consultation

Local Leadership in a Cyber Society 3: Building Resilience Together – Lessons for the Future

Monday, 10th (0900) – Tuesday, 11th (1500) June 2019

In partnership with the National Cyber Security Programme-Local and the following sponsors: -

Think Cyber
Think Resilience
Building Resilience Together

iNetwork
involve influence inspire

RISCS
Research Institute in Science of Cyber Security

Foreword

It is my pleasure, as Programme Director, to introduce this latest report on the theme of Local Leadership in a Cyber Society which summarises the detailed discussions that took place here in Windsor in early June 2019 and I hope it will act as a stimulus, not just for those of you who were with us for those discussions but also to interested parties elsewhere who might benefit from the findings contained in these pages.

St George's House, situated in the grounds of Windsor Castle, provides a safe physical and intellectual space where people of influence from all parts of society and, indeed, from across the globe, can gather to grapple with topics of national and international importance. The approach taken by the National Cyber Security Programme and its Think Cyber Think Resilience Initiative is very much in keeping with our ethos.

Founded in 1966 by HRH The Duke of Edinburgh and the then Dean of Windsor, Robin Woods, the House endeavours to nurture wisdom through dialogue. We offer a safe haven, as it were, away from the world of soundbites and headlines.

So much of what passes for debate these days happens in the media, social and otherwise. This of course has its place but there appears to be less and less opportunity for considered debate and discussion. St George's House attempts to fill this gap by creating time and space for a more reflective approach to topics that matter to society. Through open, frank and confidential discussions we hope our guests will reach a fuller understanding of the issues pertinent to the topic at hand, together with a richer appreciation of the diversity of opinion around that topic.

Participants at a St George's House consultation usually spend twenty-four hours with us. There is of course a formal programme of work, carefully calibrated to make full and fertile use of our time together but a great deal gets done too in the margins. People break bread together, attend Evensong, if they wish, in the iconic St George's Chapel and, spend informal time probing and developing the conversations begun in the fifteenth century Vicars' Hall. Ideally, they will leave St George's House, better informed, better acquainted and intellectually enriched.

Barely a week goes past without the word cyber hitting the headlines and impacting on people's lives and local communities. Over the last 3 years St George's House has partnered the Think Cyber Think Resilience initiative in bringing local leaders, policymakers and practitioners together with government, industry and academia to look at the "wicked issues" arising from providing local leadership in a Cyber Society. Over that time the cyber agenda has extended and grown and thrown

up new challenges from WannaCry to hostile actors targeting political institutions, businesses, media and sport.

Taking time to listen and learn from the direct experience of others on how these issues impact on local people and their communities is at the heart of Think Cyber Think Resilience approach and has seen the initiative develop the internationally recognised tools, techniques and training approaches to support both leaders and front-line staff across local government and the local resilience community.

This latest paper developed in partnership with the Research Institute in Science of Cyber Security (RISCS) sets out the importance of learning such lessons for the future and offers signposts to how these can help turn cyber security and resilience policy into practice across local communities.

I hope it will help stimulate wider debate and thinking on the next steps of this key aspect of the cyber agenda.

Gary McKeone, Programme Director
St George's House

Background Note to the Consultation[1]

"Our vision for 2021 is that the UK is secure and resilient to cyber threats, prosperous and confident in the digital world."

National Cyber Security Strategy 2016-21

"Our leaders, service managers, board members and politicians will …. champion the continuous improvement of cyber security practice to support the security, resilience and integrity of their digital services and systems…."

Local Digital Declaration – Cyber Commitment 2018

The rapid pace of technical change is creating new opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store or transfer data such as mobile devices and cloud services. The seriousness of this challenge has been brought home recently by the UK and its allies exposing a campaign by the GRU, the Russian military intelligence service, of indiscriminate and reckless cyber-attacks targeting political institutions, businesses, media and sport.

The scale of the targeting, coupled with the difficulty of monitoring all possible attack methods, means some attacks will get through but our collective responsibility is to both reduce the likelihood and the impact of such a threat succeeding. Foreign states, criminals, hacktivists, insiders and terrorists all pose different kinds of threat. They may try to compromise public sector networks to meet various objectives that include:

- Stealing sensitive information to gain an economic, diplomatic or military advantage over the UK
- Financial gain
- Attracting publicity for a political cause
- Embarrassing central and local government
- Controlling computer infrastructure to support other nefarious activity
- Disrupting or destroying computer infrastructure

Whilst the level of threat will vary across local organisations, they all possess information or infrastructure of interest to malicious cyber-attackers. Across the country local civic and public service organisations are working hard to reduce these threats every day and the active support and

[1] The following broad definitions informed discussions

- **Cyberspace** is the complex environment that results from the interaction of people, software and services on the internet by means of the technological devices and networks connected to it. This environment does not exist in any physical form.
- **Cyber resilience** is all about being confident in your own knowledge and how to keep your information and that of others safe. It is the actions or steps taken to mitigate and respond to threats from cyberspace (sometimes referred to as "cybercrime" or "cyber-attacks"). It means being able to prepare for, adapt to, withstand and rapidly recover and learn from disruptions caused by cybercrime.
- **Cyber security** is the protection of systems, networks, infrastructure and data in cyberspace.

For a supporting Glossary See https://www.ncsc.gov.uk/information/ncsc-glossary

engagement of their senior leaders with the technical and structural issues thrown-up by the cyber agenda is vital to ensuring the continued focus and profile of this work.

In the face of these challenges, it has never been more important, to look at the role of local leadership in a cyber-society. Critical to this is the development of common understandings of the technical issues and capabilities that will be needed going forward to underpin cyber resilience in localities. Our consultation proposes to look in depth at the emerging research and cyber exercising techniques, examine the impact of cyber-attacks on local communities and hear from senior leaders, policy makers and practitioners on how they are using the lessons to be learnt to build local cyber resilience for the future.

Building on the successful format used in the initial Local Leadership in Cyber Society Consultation. This new consultation in particular will look at the emerging lessons from local case studies (Wiltshire and Copeland) , the Think Cyber Think Resilience - NCSP Cyber Pathfinder[2] programme and the Evaluating Cyber Security Evidence for Policy Advice (ECSEPA) project[3] and how they can inform the ongoing Local Leadership in a Cyber Society activities and how localities can be supported to work in step with the wider aspirations of the National Cyber Security Strategy[4] and Local Digital Declaration[5] Cyber Commitment.

The intention being as we explore the following underpinning questions and refine existing ideas or identify new avenues of inquiry it will help to generate new insight for leaders, policy makers and practitioners in addressing their own roles and their wider roles in a cyber society:

What are the consequences for local services of a cyber-attack?

- Using case studies to establish a common picture of cyber risks, threats and what are our technical interdependencies and the consequences of an attack?

[2] Think Cyber Think Resilience - NCSP Cyber Pathfinders: Is commissioned by Ministry of Housing, Communities and Local Government and funded by the National Cyber Security Programme. The Pathfinder exercises and seminars are designed to help participants think about the impact of cyber incidents on their organisational plans for multi-agency working under the Civil Contingencies Act.

[3] Evaluating Cyber Security Evidence for Policy Advice (ECSEPA) project is funded by EPSRC and supported by the Sociotechnical Security Group at the National Cyber Security Centre (NCSC). It is intended to learn more about how the UK Government cybersecurity advisory and policy-making community evaluate evidence in their roles.

[4] National Cyber Security Strategy sets out the Government's 2021 Vision that the UK is secure and resilient to cyber threats; prosperous and confident in the digital world (see additional notes below).

[5] Local Digital Declaration is a joint endeavour initiated by the Ministry for Housing, Communities and Local Government (MHCLG), the Government Digital Service (GDS), and a collection of local authorities and sector bodies from across the UK. The declaration sets out a collective ambition for local public services in the internet age, and shared commitments to realising it. It commits partners working on a new scale to:

- design services that best meet the needs of citizens
- challenge the technology market to offer the flexible tools and services we need
- protect citizens' privacy and security
- deliver better value for money

and includes a dedicated commitment on cyber security and resilience for partners to proactively … ***"Champion the continuous improvement of cyber security practice to support the security, resilience and integrity of our digital services and systems"***

How do we build a multi-agency response?

- What is the core technical capabilities local organisations and their leaders need to have in place to mitigate cyber incidents and how can exercising together help?

What is the leader's perspective?

- How do we successfully combine learning and leading roles in the cyber environment?

What is the practitioner's perspective?

- How do we combine learning with implementing organisational and technology change in the cyber environment?

How can Policy makers help?

- What do we see as the learning challenges for policy-makers and how can they make a positive contribution to imbedding cyber-resilience across organisations?

The intention is that as the Consultation refines existing ideas or identify new avenues of inquiry it will help to generate new insight for leaders, policy makers and practitioners in addressing their own and their wider roles in a cyber society.

1. Introduction

This, the third, Consultation on Local Leadership in a Cyber Society, focussed on distilling lessons on leadership and organisational collaboration from real experiences. The purpose was to use the collective wisdom of a group of experienced practitioners and policy-makers to help set the direction for further work.

Previous Consultations in the series have involved the Think Cyber Think Resilience Initiative and participants considering how best to raise awareness of the government's Cyber Security strategy, policies and solutions. A key part of these discussions focussing on the need to effectively map those policies and their potential impacts on local public services and the local resilience community. As a direct result of using the St George's House process to bring senior leaders and stakeholder together to focus on these issues the initiative has: -

- Developed the Civic Cyber Resilience Model and its supporting Online Knowledge Bank
- Launched Building Resilience Together Through Leadership executive briefing papers, blogs, and seminars for over 2000 participants
- Established a National Civic Cyber Pathfinder Training Curriculum encompassing a range of Multi-Agency exercises and over 3000 seminar day places covering the interaction between cyber security and community resilience.
- Developed and rolled-out a Cyber Hub containing operational guidance and advice, on the ResilienceDirect platform for over 50,000 members of the wider local resilience community.
- Supported the creation of a National Resilience standard for Cyber Incident Handling and the Local Digital Declaration Cyber commitment.
- Creation of the MHCLG Resilience and Emergencies Directorate (RED) Cyber Resilience Programme and team to actively engage with the Local Resilience Forum community to improve their Cyber preparedness
- Secured £5m in Local Growth Fund match-fund support for the creation of the Greater Manchester Cyber Hub and GM-Foundry to promote cyber skills and innovation across the public, private and academic sectors.
- Supported the establishment of the LGA Local Government Cyber Security Stakeholder Group and Local Government Technical Advisory Group to support central-local dialogue on the policy, strategy and technical solutions.
- Exploring opportunities for local public service leaders, policy makers and practitioners to benefit from the emerging lessons coming from the work of the Research Institute in Science of Cyber Security (RISCS) and GM-Foundry.

The output of this Consultation was lessons to be learned from actual events, new and significant insights on the nature of current problems, suggestions for senior local leaders on learning from the experiences of real events, and suggestions for government ministers on what they need to consider doing to help local leaders, policymakers and practitioners learn together from incidents, exercising and research.

The Consultation concluded with take-away Asks and Offers from the participants, leading to recommendations on next steps to improve the handling of cyber risk and resilience at local level.

The inputs included presentations from two local areas that had been subject to serious cyber-attacks. One suffered a direct attack on its IT systems, resulting in a sustained and complete shutdown that seriously disrupted its operations, staff and the public for a long time. The other experienced attacks on various local public bodies following a major non-cyber incident, that necessitated shutting down key communications channels, hindering the co-ordination of the response to the major incident.

The Consultation also received updates from local government practitioners and support bodies on their progress and experiences. Representatives of a large metropolitan Combined Authority described its approach to engaging the many digital and cyber actors and issues in its area. Findings from a large-scale simulation exercise, of a local incident requiring a multi-agency response, were also presented. Research conclusions from a study of the cyber policy and practitioner support landscapes, and insights from education programmes focussing on the personal characteristics of leaders, completed the inputs.

Underpinning the discussion in the Consultation was the concept of resilience: "the ability to anticipate, prepare, respond and adapt to changing circumstances". In the case of cyber, this means continually adapting to a changing set of threats. It implies that security, response and recovery need to be considered. It embraces policies, leadership, technology, processes and human aspects. It challenges an organisation to achieve it to a necessary and sufficient level in its particular circumstances, begging the question of what that level is and how progress towards it is measured. The development of national standards and guidance is intended to help, but a change in the organisational wide mind-set is required. Leaders, policy-makers, practitioners (including frontline staff) need to accept cyber-resilience is now part of their job role – cyber-security needs to be business as usual.

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

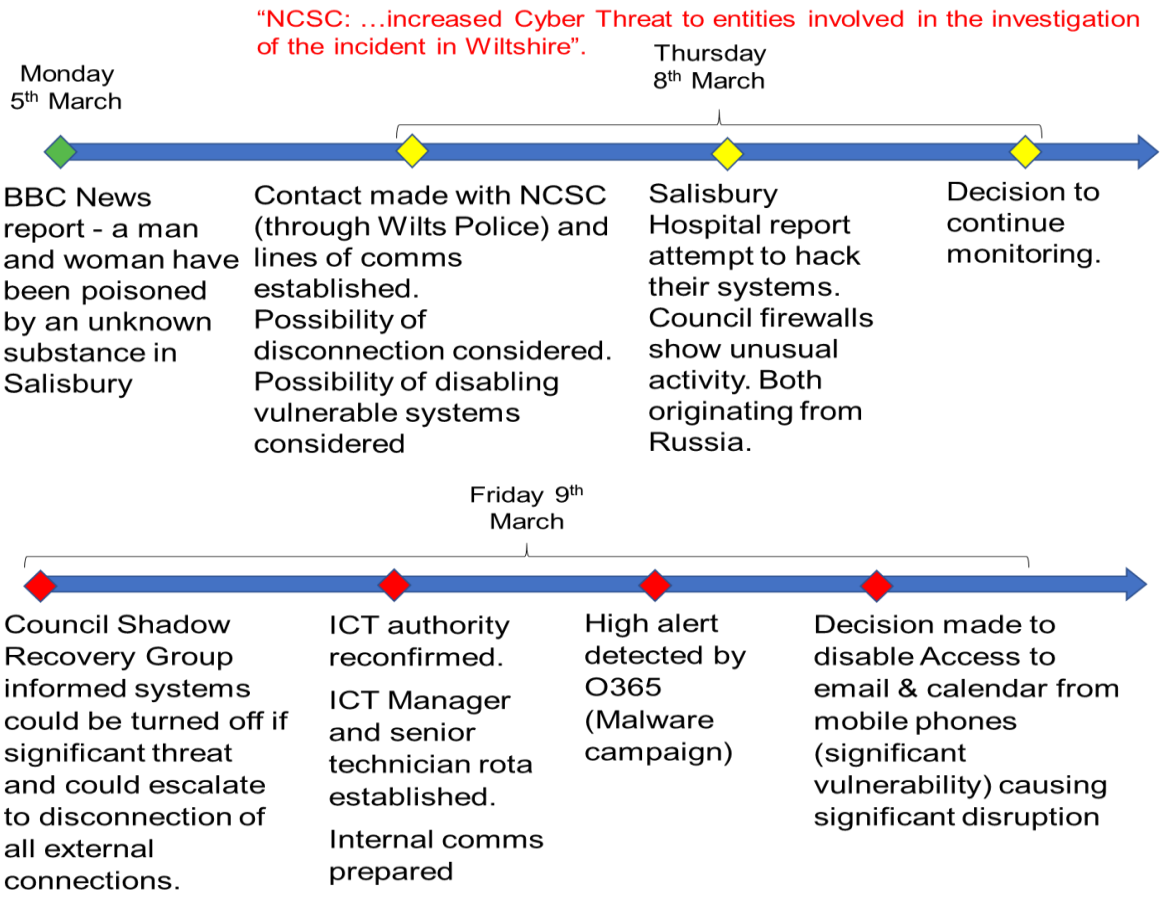
2. Experiences and lessons presented to the Consultation

The case of cyber-attacks following a major incident

Steve Vercella, Head of ICT Wiltshire Council and Wiltshire Police

The Novichok poisoning incident in March 2018 in Salisbury, Wiltshire was unexpectedly followed up by numerous cyber-attacks (see Figure 2.1). Dealing with the incident itself involved multiple public agencies including security and military units. The public was significantly affected and put at risk, and there was extensive international media coverage. Following the incident, numerous penetration attacks and malware campaigns were made against the computer systems of the local public sector bodies including a hospital and the local authority (which had systems shared with the police). The attacks were successfully defended. However, this took significant effort and the side-effects hampered the recovery from the initial incident. The incident has continuing effects as there is an increase in cyber-attacks whenever the incident or the location are mentioned in the media, and for example, on the anniversary of the initial non-cyber incident.

Figure 2.1: Salisbury Incident Initial "Cyber" Timeline



Key to the successful defence was the prior establishment of agreements on roles and authorities for decisions, for example on if and when to disconnect systems and carry out the prepared disconnection procedures (something that is often not thought through). An IT Health Check had identified particular areas of weakness and risk that would become the urgent areas of attention in the event of an attack. Exercises had been carried out with partners to rehearse these and other actions.

However, the IT department in the local authority was overstretched already, with limited capacity available and few established links with sources of help. The relationship with the police, and its links to national bodies, proved helpful. Office 365 was used by the local authority but not the police, and high volumes of attempts to access the email system appeared, resulting in many accounts being locked out. The subsequent password reset calls swamped the IT Helpdesk. As there was a known vulnerability in mobile devices, access to email and calendars on smartphones was stopped. These factors reduced both the capability of field workers and managers responding to the major incident, and the capacity of the IT team to respond to the attacks on the systems.

The incident drew attention to the risk of system maintenance and patching falling behind, and also of not taking advantage of all security and monitoring tools available such as those in Office 365. These preventative measures are now recognised as essential and continuing actions.

The key lessons arising from this experience are as follows.

- The occurrence of any event in the locality that becomes widely known may prompt a cyber-attack.
- Agreed decision models and authority structures need to be in place covering who decides what in case of an attack.
- Exercising is crucial.
- A disconnection policy and disconnection procedures need to be in place.
- Business continuity and communication plans need to be in place that cover the loss of systems, including staff relocation.
- Staff and management rotas need to be ready to ensure 24/7 coverage.
- IT health checks should be used to check for vulnerabilities not "prove" security.
- Decisions must be documented, for subsequent analysis and in case of legal proceedings.
- Sources of help and advice should be identified before any event, and any security or authentication protocols understood.

See case study presentation at Annex 1

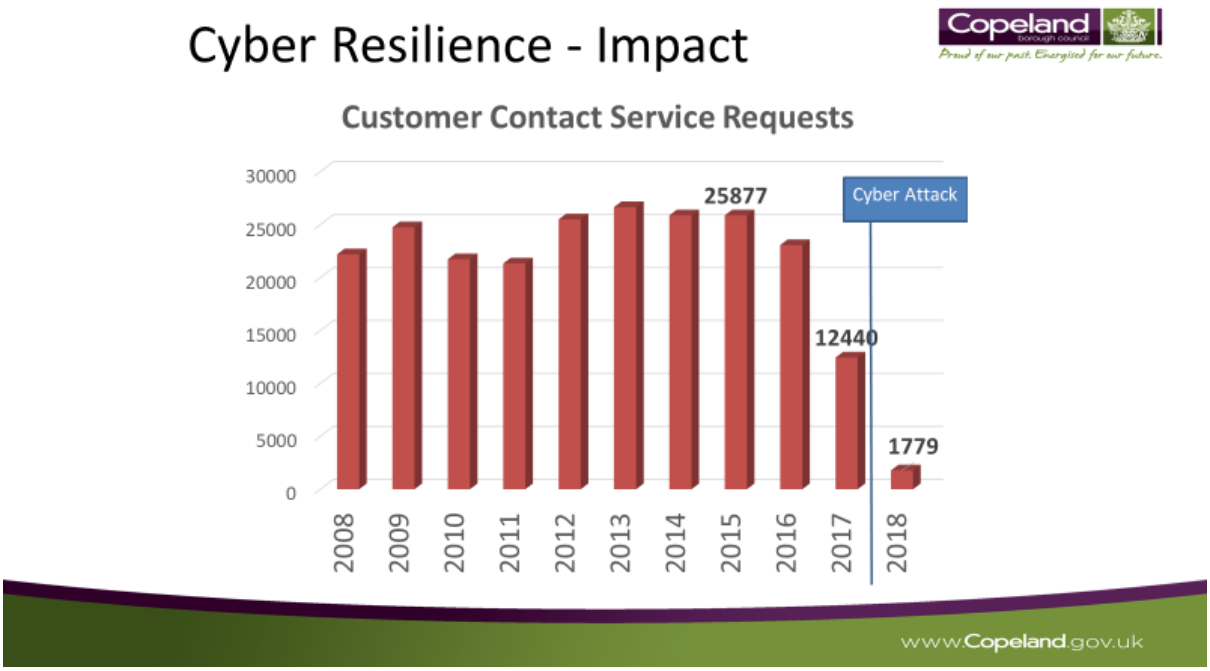
The case of a targeted attack on a local authority

David Cowan ICT Manager Copeland Borough Council

Copeland Borough Council, a small local authority in Cumbia and home to the Sellafield nuclear plant and the Nuclear Decommissioning Agency, suffered a direct attack on its IT systems over the 2017 August Bank Holiday weekend, continuing through the return to work of staff on the next working day. It was not immediately obvious what was happening, and before preventative measures could be taken, most of the IT systems and IP phones had been lost. Cloud-based systems were also hit; only separately-hosted applications survived. The attack was attributed to the exploitation of a "zero day" virus (malware that is undetected by antivirus software as it has not yet been updated to recognise it).

The small IT team was naturally overwhelmed and had few pre-set arrangements for calling in help. Communications links were largely absent. The entire operations of the local authority were disrupted: where business continuity plans were not in place, it ceased to function. The processing of online customer contact service requests ceased see Figure 2.2). Staff had to be relocated, and processes forced to fall back on pen and paper. Salaries and bills could not be paid due to the loss of financial systems. Among other disruptions, for some months, people in the area could not move house due to the loss of the property search system.

Figure 2.2: Impact on Copeland Customer Service Requests



It turned out that backups were also compromised. The result was that all IT systems had to be rebuilt from scratch. The hypothesis is that the systems had been penetrated some time before,

without detection, possibly in an attempt to obtain sensitive information on the nuclear reprocessing plants in the locality. However, the attack itself, and some of the rebuilding work, destroyed forensic evidence that may have helped to reach a definite conclusion.

Approaching two years after the event, Copeland was still in recovery mode... During that time, the stress on all the local authority staff having to try to work from distributed locations resulted in many leaving the Council.

The key lessons arising from this experience are as follows.

- The presence of any critical industry, institution or infrastructure "of interest" in the locality may give rise to an attack to obtain sensitive information or links to persons associated with them.
- An attack is an operational business issue, not just an IT one, and active senior level engagement in prevention and response is essential.
- The general public is significantly affected: management of communications and the effective participation of politicians is necessary.
- Regardless of size and limited resources that make it challenging, every local authority needs sound IT governance, management and especially maintenance.
- Full advantage should be taken of free security tools and local and national support networks.
- Cloud-based systems are potentially less secure than in-house ones (for example, through vulnerability to administrator login attacks)[6].
- Links to partners and service providers must be understood and disconnection protocols put in place.
- Clear ownership of data and line-of-business systems is essential, as is the establishment of responsibility and authority over them.
- Business continuity plans are crucial and must be tested through exercise to ensure that they are realistic – it is likely that few business continuity plans assume IT outages will not be quickly restored.
- Any potential sources of forensic evidence must be protected.

See case study presentation at Annex I

[6] see https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

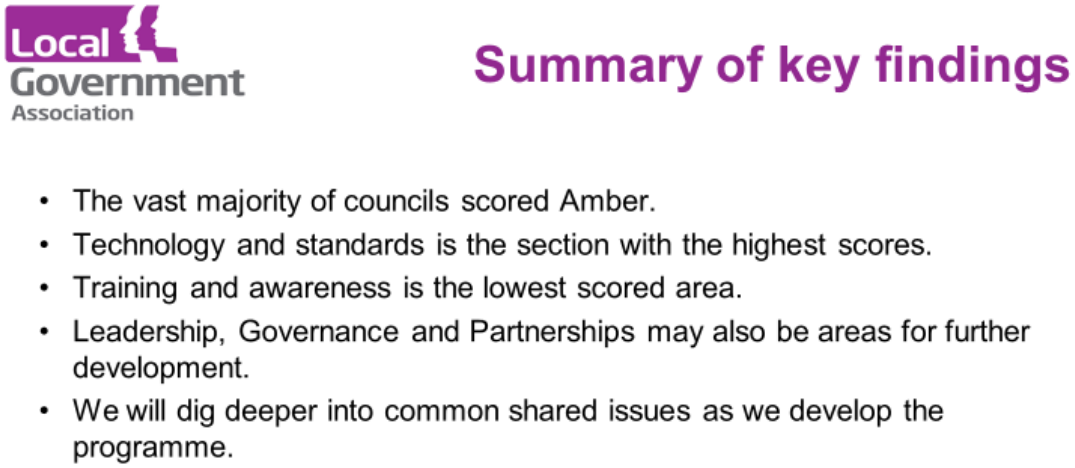
3. Reports to the Consultation

Siobhan Coughlan, Local Government Association

The Local Government Association (LGA) as part of their NCSP funded programme, conducted a cyber security Stocktake exercise with all 353 councils in England during the summer of 2018. This consisted of an online questionnaire to assesses each councils' current arrangements for cyber security including the arrangements in place for Leadership, Governance, Awareness raising and Training, IT, and their engagement with other agencies.

Each individual council's response was assessed, and RAG rated. Each council only saw their own rating no ranking was published. Those councils rated as Red or Amber Red were targeted with support to help them address the issues identified. These councils were also given private feedback at a chief executive / Leader level as well, to help get senior support to address the identified issues. A funding programme was put in place for councils to bid for funds and a this prioritised the Red and Amber Red councils.

Figure 3.1 Summary of key findings from LGA Cyber Stocktake 2018



Helen Braithwaite and Phil James, Think Cyber Think Resilience - MHCLG Cyber Pathfinders Team[7]

Exercise FinAck was a multi-agency training exercise developed as part of the wider Cyber Pathfinders Training Scheme [see Fig 3.2] to take representatives from the local public sector through a journey of discovery of the people, planning and process issues associated with being ready to deal with a major cyber-attack or incident. The purpose was to emphasise the need to be prepared, by understanding the consequences and impact of an event, which are widely underestimated.

[7] See details on Think Cyber Think Resilience - NCSP Cyber Pathfinders Curriculum and Exercises at Annex 2

It addressed the common lack of awareness of the need for non-technical training and exercising, the need for strategic leadership and engagement, the importance of a multi-agency response, the need to recognise responding to this incident within already well embedded local and national response arrangements is critical and encouraged the utilisation of the available advice and guidance.

Nearly 500 people took part in Exercise FINACK. It was delivered in 8 locations across England. Feedback confirmed the majority felt they would act differently as a result. The National Resilience Standard on cyber incident preparedness was widely welcomed. Delegates did however comment on the volume of material and resources available which made it was hard to navigate and understand what was important. Many felt this could be simplified. All the material developed to support and deliver Exercise FINACK is now available on the ResilienceDirect Cyber hub for local stakeholders and practitioners to use.

Figure 3.2 Cyber Pathfinders Training Schemer 2018-2020

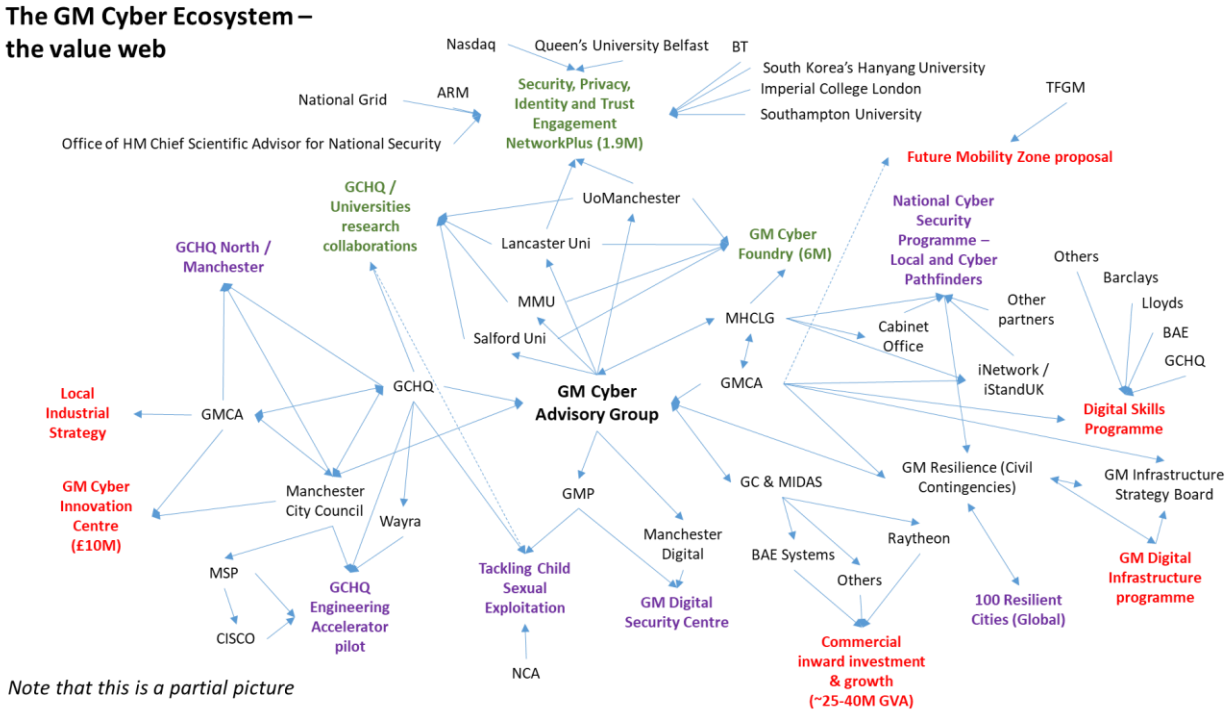
Phil Swan, CIO GMCA/GM Cyber, and Dr Daniel Dresner, Manchester University/ Cyber Foundry

GM-Cyber

The Greater Manchester Combined Authority and Greater Manchester Cyber Innovation Centre (GM-Cyber[8]) has mapped [see Figure 3.3] the actors and initiatives having an impact in its area, relating to digital technology, cyber security and relevant infrastructure, across all sectors. The map describes a large and complex network, that the authority actively curates by means of continually getting people together and encouraging them to make links and collaborate. The key challenge is how to continually encourage and facilitate that collaboration.

The purpose and motivation for driving this collaboration was set in terms of economic development, i.e. in support of making the region a thriving hub of digital research and industry. This resulted from and enabled high-level political and official engagement. The aim was not about creating new things but making the most of existing efforts by joining them up, especially the many funding streams that feed into the ecosystem.

Fig 3.3 GM Cyber Eco-system (partial map)



GM-Cyber Foundry

[8] The Greater Manchester Cyber Innovation Centre (GM-Cyber) is a match funded initiative which has received £5m in pump-primed funding as part of a wider Local Growth Fund agreement between GMCA and MHCLG. GM-Cyber now serves as a focal point (hub) for the cyber security sector in GM, enabling collaboration and joint development of related capabilities and supporting the wider national cyber security agenda and providing direct support to the Pathfinder scheme through its partner organisations INetwork and IStandUK in partnership with the MHCLG led NCSP Building Resilience Together workstream.

Within the city region, extensive collaboration has been achieved between four universities to create the Cyber Foundry (see Figure 3.4). This is a unique initiative to apply cyber security expertise from the universities as a tool to enable business development and growth for local SMEs – especially those where cyber may not yet underpin the core business of where cyber could remove the constraints of traditional business practices.

The Cyber Foundry is also proving a focal point for activity with the expected spaces of cyber law enforcement. Greater Manchester Police are partnering with the Foundry's four universities to have students give their time to SMEs to strengthen security postures with practical measures like the Cyber Essentials. These industry-academe links bring immediate impact on reducing the vulnerability of local businesses to cyber-attack and developing the skills of the students who we hope will settle locally and increase the cyber security posture of the city region as a whole.

Figure 3.4 on GM-Cyber Foundry

4. Reports to the Consultation on relevant research

Professor Madeline Carr and Dr Alex Chung, Research Institute in Science of Cyber Security (RISCS) University College London

As part of the NCSC sponsored Research Institute in Science of Cyber Security (RISCS)[9] programme of research looking at the human and organisational aspects of cybersecurity and associated policy, University College London had conducted a study into how leaders, policy-makers and practitioners deal with the deluge of information that they receive from many diverse sources. The researchers had also mapped out all the UK policy statements, information channels, policy clusters and initiatives relating to cyber security. The map had 2,500 data points. When printed, it was longer than the height of the researcher who prepared it, substantiating the intuitive sense of those working in this space of it being a confusing and complex ecosystem and that cyber security is a "wicked" policy problem that a tick-box approach cannot resolve [See Figure 4.1].

Figure 4.1 'wicked' policy problems

The study of how people engage with information overload was carried out through a combination of face to face interviews and an online survey that captured the feedback of 84 policy specialists and practitioners within and outside central government. Between them they used a wide variety of mechanisms for coping with voluminous information, with the most popular approaches being selection by "source trust and reputation", "prioritisation", and "relevance".

When faced with conflicting information, respondents sought resolution through (most often) "source trust and reputation", "second opinion", and "corroborate/independent research". When

[9] See Annex 2 for background details on RISCS

asked from whom someone sought a second opinion, the replies strongly indicated a reliance on personal relationships that had led to trust in an individual.

Trusted networks and relationships dominated the apparent behaviour. However in many aspects, the responses of policy makers and practitioners differed. Policy officials were more likely to go to primary institutions, whereas practitioners relied on personal networks of peers.

Open questions on what might be useful to respondents elicited many thoughts, such as having a central support body, a common lexicon, peer reviews, and a collaboration space. Noting that many of the things suggested already existed, the interpretation was that these were instinctive "cries for help", [see Figure 4.2] and indicators of a deeper systemic problem.

Figure 4.2 ECSEPA "cries for help" findings

Dr Edward Brooks, Executive Director of the Oxford Character Project

Insights from the Oxford Character Centre's education programme focussing on the personal characteristics of leaders proved relevant to the discussion of leadership in the digital society, the qualities of character, both virtues and vices, are shaped by the institution within which people grow — the culture. It may be cultural to pretend to know more than you do, in order to progress, or attribute blame when things go wrong, as examples of negative characteristics that hinder cyber security. Other common characteristics are optimism bias and over-compensation, leading to a false belief in safety.

It is the role of leaders to steer the culture in a positive direction. Characteristics for leaders to exhibit and encourage that help deal with the cyber challenge would include humility (acceptance of fallibility), resilience (adaptability as circumstances change), and honesty (to admit when something goes wrong). In short, the human and cultural dimension is hugely significant in an organisation's ability to deal with a cyber threat.

5. Risk and Resilience: understanding cyber as political risk and forming suitable policy advice on mitigations

In support of the wider consideration of the issues, delegates were asked to look at developing policy advice on cyber risk mitigation looking at the at the understand-analyse-mitigate-respond approach to "political" risk handling (see Figure 5.1), the NCSC Cyber Security Toolkit and the Civic Cyber Resilience Model.

Figure 5.1 Guiding questions for effective risk management[10]

UNDERSTAND	ANALYSE	MITIGATE	RESPOND
1. What is my organisation's cyber risk appetite?	1. How can we get good information about the cyber risk we face?	1. How can we reduce exposure to cyber risks we have identified?	1. Are we capitalising on near misses?
2. Is there a shared understanding of our risk appetite? If not, how can we foster one?	2. How can we ensure rigorous analysis?	2. Do we have a good system in place for timely warning and action?	2. Are we reacting effectively to crises?
3. How can we reduce blind spots?	3. How can we integrate cyber risk analysis into business decisions?	3. How can we limit the damage when something bad happens?	3. Are we developing mechanisms for continuous learning?

Delegates took part in a two-stage simplified policy crisis game format that looked at the understanding cyber as political risk and forming suitable policy advice on mitigations as follows:

Risk and Resilience Breakout One: prepare advice for senior officials

Three breakout groups were set the challenge of devising an "official level" briefing session for senior local and central government officers on how to help leaders, policymakers and practitioners learn together in the face of the lessons from Wiltshire, Copeland and FinAck.

The following pieces of advice were generated by the groups and in the discussion that followed.

- Ensure there is a clear political and official lead and accountability in place (as there is with local authority finance or data protection), to oversee a holistic approach to cyber resilience, and raise the risk to the top political level.
- Create a network of capability and trust in preparation for any event, such as a regional support network.
- Test and exercise regularly; test the assumptions, doctrines and networks, and check that decision and action logs are maintained in all agencies.
- Utilise the free tools available, standards, and existing accreditations such as for the Public sector Network (PSN).
- Train and resource senior responsible officials.

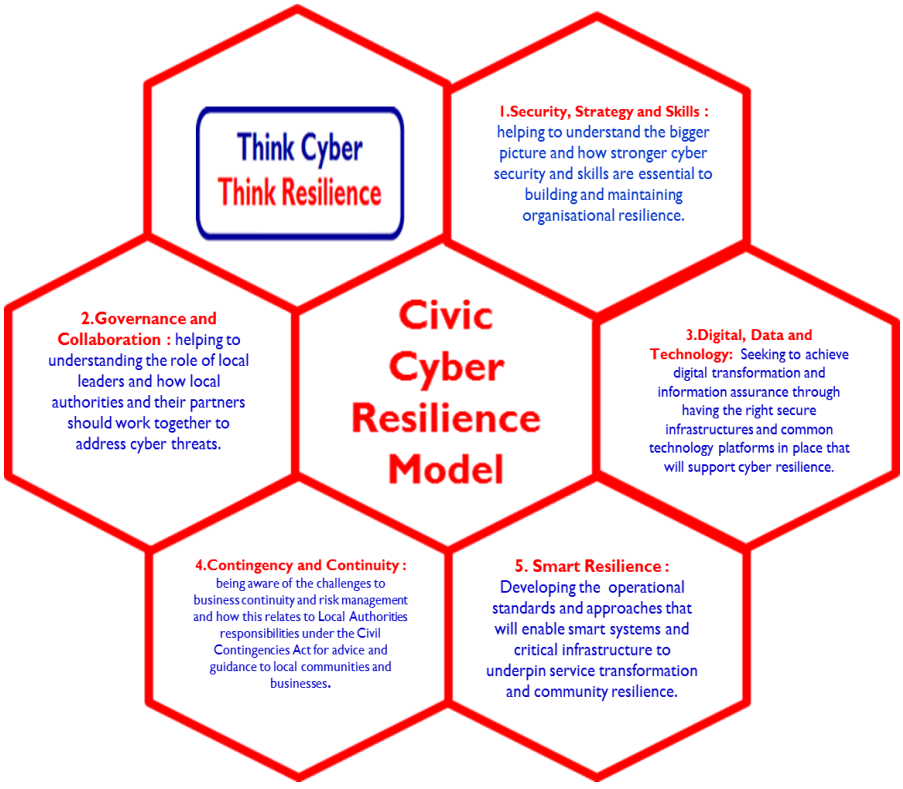
[10] Adapted from Political Risk – How organisations can anticipate global insecurity (Amy Zegart and Condoleezza Rice - Twelve 2018) see https://hbr.org/2018/05/managing-21st-century-political-risk

- Regard cyber security as business as usual, not emergency planning.
- Ensure a clearer definition of roles and ownership through light-touch regulation, assurance processes, and/or audit.
- Conduct a culture health check, supported by training, covering openness, honesty, rewards for identifying risks, and encouragement of adult-to-adult conversations.
- Put in place funded peer support, peer review, and mutual aid mechanisms.
- Develop guidance on a standard approach to detecting "trigger points", i.e. the time at which a problem is identified that triggers action and when/where to escalate.
- Produce dynamic playbooks based on addressing harms rather than static plans, because attacks are happening all the time and increasing in sophistication.
- Ensure continual monitoring of threats.
- Ensure cross-organisational collaboration e.g. between IT, HR, emergency planning, business continuity planning, data protection (noting that a cyber event is also a data protection event with statutory procedures and penalties).
- Need to identify and reach out to Senior Responsible Officers for each Local Authority.

Risk and Resilience Breakout Two: prepare advice for government ministers

The three breakout groups were challenged to work-up a briefing presentation to a Government Minister on what Government needs to consider doing to help local leaders, policymakers and practitioners learn together from incidents, exercising and research. They were also invited to suggest updates to the following core themes highlighted in the wider Civil Cyber Resilience Model [see Figure 5.2].

Figure 5.2 Civil Cyber Resilience Model



Each of the breakout groups focussed on a single aspect of the Model. The following pieces of advice were generated by the groups and in the discussion that followed.

Leadership, Governance and Collaboration

- Strengthen the roles in local government at councillor and official level — they are often held too low in the organisation. Consider a statutory approach.
- Establish a place-shaping and civic responsibility role for local government, i.e. a wider place-based approach, with strategic leadership roles worked out. This does not exist at present, but maybe build it around Local Resilience Forums (LRFs).
- Simplify communications and messages to reinforce that cyber is everyone's business; make use of visual aids and videos.

Digital, Data and Technology

- Agree a formal central-local government concordat to address the issue of the varying compliance regimes used by authorities and government departments that have data exchange connections.
- Consider setting up a central team to provide a single point of contact and support.
- Consider a "kite mark" scheme to demonstrate compliance with law and national standards.
- Ensure any funding programmes drive collaboration and sharing, not competition.
- Clarify where localism is appropriate and where national cyber-resilience requirements should take priority.

Contingency, Continuity and Risk

- Ensure local government planning reflects a whole-of-business continuity approach, based around services and impact not just IT.
- Ensure that the plan is active, dynamic and continually reviewed, through a regime for checking, and emphasise that not having such a plan is a major risk.
- Put in place a programme for continually developing cyber-security professionals.

More widely the current Civic Cyber Resilience Model [see Figure 5.2 above] was viewed as helpful and containing many important elements, the participants made the following comments on how it needs to be developed: -

- It is too "tick-box", i.e. "do this", with the need for a stronger emphasis on leadership capabilities.
- It should be presented in a simpler format: include pictures (maybe Venn diagrams), with clearer, less abstract wording.
- Support the Model with guidance on what constitutes a clear resilience plan, providing templates for practical approaches, based on case study material.
- It is currently focussed on response; it needs to address business continuity, and mind set and culture.
- The silos in the model are too narrow and need to convey the message that it is a cross-organisational, place-based, and dynamic issue.

- Recent cyber capacity modelling and mapping, together with the findings of the LGA Stocktake and Cyber Emergency Response functions should to be considered. [11]
- The next iteration of the model needs to support the development of policy, tools and techniques that will strengthen the focus across localities around inter-relations between IT security, organisational business continuity and community resilience.

The discussions concluded that there is an outstanding requirement for those involved in Cyber Security in Whitehall to create a 'virtuous circle' of well signposted online policy documents. Each of the principle organisations concerned with Cyber Security on the Local Government (Cabinet Office, DCMS, MHCLG, NCSC, LGA) should each have a single landing page that comes up when people search for "cyber security/resilience" and "local government/councils". Each of the landing pages would be written with their audience in mind and direct the reader not only to key policy documents and products from their own website but to the splash pages of others.

[11] See Developing Cybersecurity Capacity - A proof-of-concept implementation guide Rand Europe, Evaluating Cyber Security Evidence for Policy Advice (ECSEPA) project and http://ecsepa.coventry.ac.uk/strategic-coordination-summit-cyber-emergency-response/ studies around response frameworks see http://www.cert.org/incident-management/services.cfm?%20-%20alerts.

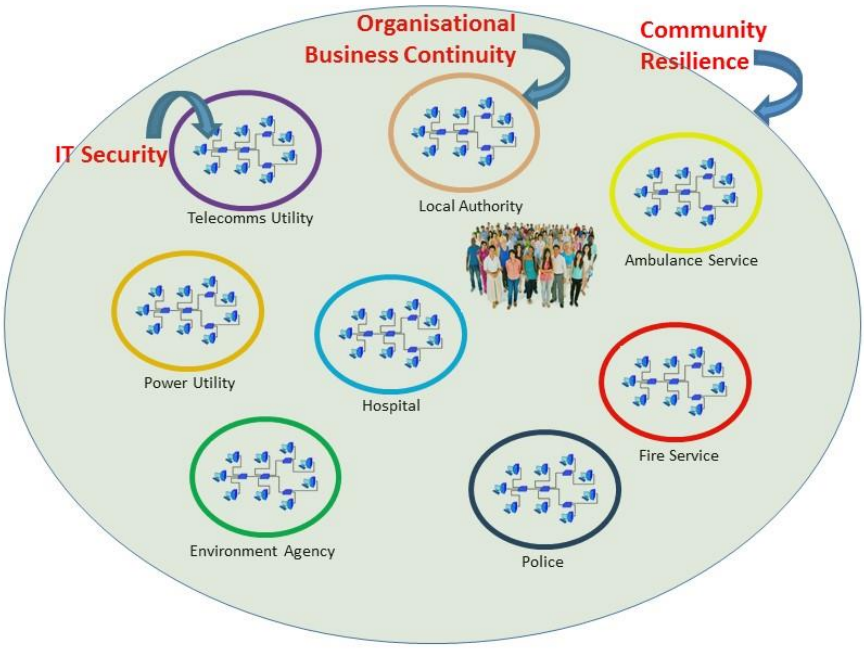
6. Redefining the policy into practice challenge of Building Resilience Together

The consultation then looked at the need to define and sharpen our understanding of the policy challenges facing all tiers of government and local multi-agency working. A key challenge is how best to focus policy and practical effort on three distinct, but inter-related capabilities:

- IT Security – highlighting the key steps and controls to ensure that local public bodies are protected.
- Organisational Business Continuity – ensuring that internal Business Continuity arrangements cater for damage to or loss of IT systems, communications, or data.
- Community Resilience – recognising that strong inter-agency collaboration is an essential precondition for cyber resilient communities and partnerships.

Across all organisations, leaders, policy makers and practitioners were having to develop a repertoire of tactical approaches around not just their own operational requirements, but also for building collective resilience across agencies by recognising these inter-related capabilities. Figure 6.1 illustrates how these capabilities are in effect "nested".

Figure 6.1: The "Nested" Capabilities Challenge

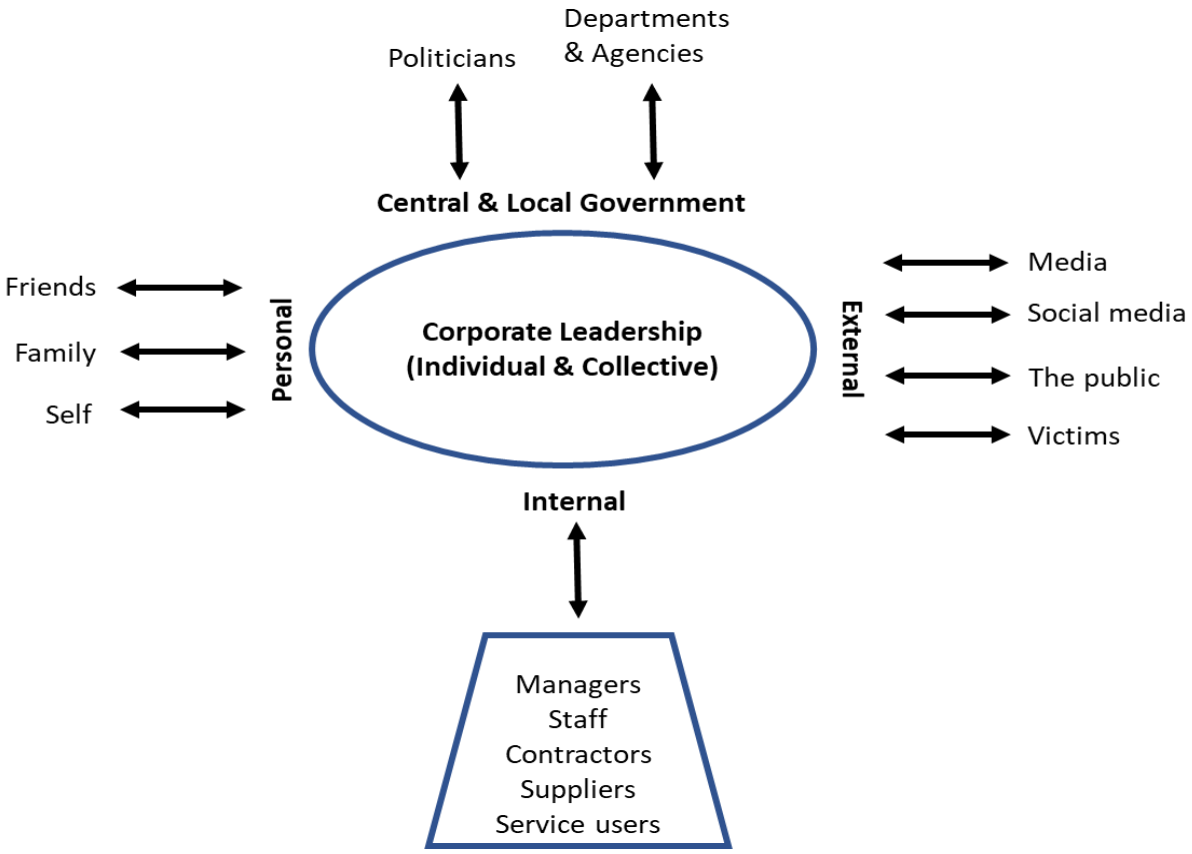


The "nested" dilemma is that a failure of IT security in one agency has a direct impact on its organisational business continuity. If operational continuity partially or completely fails as a result, that can impact other agencies and the public. If the collective community resilience measures are inadequate to deal with this, then serious consequences are likely. Therefore responsibility and accountability for planning, response and recovery lie not just at technical level but also at the senior

management and political levels in each organisation, and collectively among agencies at community level.

As a practical step, participants supported the idea of digging deeper into the Wiltshire and Copeland case studies as a way of understanding the human and leadership issues that are at play [see Figure 6.2] in such circumstances and help identify what real-life lessons emerge that could help sharpen policy thinking, inform operational guidance and the development of practical support across the local sector.

Figure 6.2: Human and Leadership issue mapping

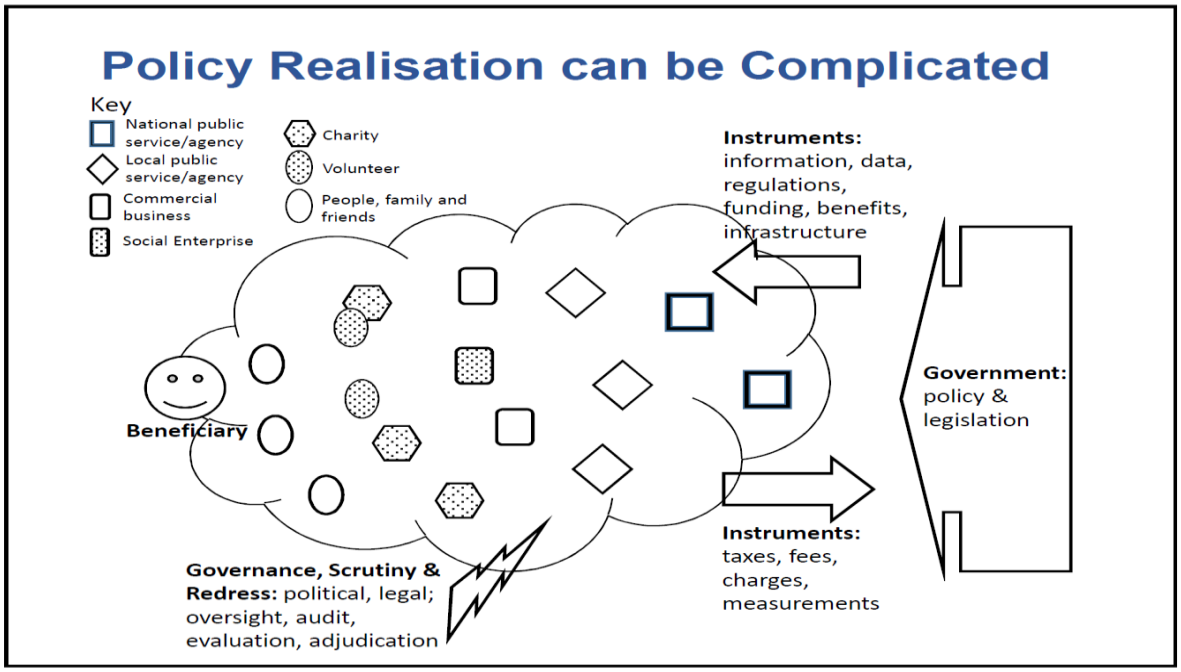


The participants observed that given the institutional environment within which local officials work they also are often required to mitigate political and policy risks (as highlighted in the "Risk and Resilience" sessions). The underlying challenge of emerging complexity from so many policy initiatives (highlighted by ECSEPA research) and operational structures (see GM-Cyber Eco-System at Fig 3.3) makes navigating this policy and political mix very difficult.

Consequently, it becomes necessary to cope with complexity through reliance on a few known operational models and trusted sources. This does mean, as previously highlighted, that there is a need to simplify and streamline official guidance to make it effective.

The session moved on to consider the work the Cabinet Office Policy Lab and MHCLG's "Grey Cells" project[12] in looking at differing forms of government intervention and policy instruments[13] that have been used to address a range of similar "wicked issue" complexity [see Figure 6.3. below]

Figure 6.3: "Wicked issue" of complex policy realisation



Source: Waller, P. (2017). Co-Production and Co-Creation in Public Services – resolving confusion and contradictions. International Journal of Electronic Government Research, 13(2), 1–17.

In response participants emphasised the need for redefining, simplifying and clarifying policy expectations and providing "one-stop" access to supporting implementation tools and techniques. This theme was consistently highlighted in the concluding "post it" note session where a "back to basics" approach was advocated that would help determine the current situation, identify desirable policy objectives, and design feasible policy instruments (considering information collection and provision, regulatory action, funding, new organisational roles, and physical assets) and associated action/implementation plans.

[12] See https://openpolicy.blog.gov.uk/2014/06/03/joining-up-the-grey-cells/
[13] Policy instruments are the tools that governments choose from to intervene in the economy, society and environment to make change, such as regulations, permits, information provision and campaigns, grants or subsidies, taxes, measurement, and more tangible things like support organisations and infrastructure.

7. Key messages from discussions during the Consultation

The discussions during the Consultation were very wide ranging and a number of important observations stood out in relation to cyber security and resilience.

Complacency, myths and flawed assumptions create problems, e.g. the reality is that security is never certain, cloud solutions are not more secure, people would bother to attack you, it is not just an IT issue, human beings don't always remember what they are supposed to do. Assumptions must be identified, understood, changed if necessary and kept under review.
The language used can add to the confusion — not just the use of jargon, but much of the published material inadvertently reinforces a presumption that the problem is solely about IT security within a single organisation, whereas the Consultation has revealed that it is much wider than that.

There is an interplay between cyber security and data protection. Most cyber events will put data at risk, and therefore will be reportable under GDPR. There is more to be done to define the relationship between organisation's roles in cyber security and its statutory obligations for data protection — as well as with business continuity planning. In similar vein, IT teams are often not formally included in business continuity, community resilience planning, or emergency planning, and need to be. These issues were also seen as being highlighted in experiences arising from the recent spate of civic sector cyber incidents in the USA such as Atlanta, Cleveland and Baltimore.

In contracting with suppliers, detailed and in-depth investigation of their security arrangements must be carried out. In the local government market, many systems are old and have weak security — the market is not lucrative enough to sustain the necessary continuing investment. It was felt that there should be more use of smarter/collaborative procurement across local public sector and that the localism agenda should not be barrier to enable local organisations to procure in a more joined-up way than a present and thereby maximise the opportunity for collective efficiencies and savings. In particular the Crown Commercial Service should be encouraged to provide a third-party supplier framework that includes standards and certifications.

Risk is not precisely definable with defined responses. Consequently, standard risk registers, while important, are not enough in themselves. More focus and understanding are needed on the impacts of the risk on services, localities, and service users. Similarly, a tick-box approach to compliance is dangerous in a complex situation where threats and risks change constantly. Insurance is also not necessarily an answer. Companies set the compliance bar very high and, nothing can be certain — this will be reflected in premiums.

Organisational culture is important: staff need to be encouraged to be open and honest if something goes wrong, and not be in fear of punishment. Technical staff need verified competency — standards and certifications are emerging.

Cyber security and resilience is a team sport. Making good inter-agency and inter-personal relationships ahead of any incident makes response and recovery substantially quicker and easier. A little black book of phone numbers should be in everyone's pocket.

8. Conclusions

The most striking conclusion from the Consultation was that there is still little awareness across the public sector that cyber-attacks may cause real and significant harm to the general public. That realisation raises questions over the responsibility and roles of public bodies and their leaders, and the adequacy of national policy.

The discussions revealed that a key challenge is how best to focus policy and practical effort on any or all of three distinct, but inter-related capabilities:

- **IT Security** – highlighting the key steps and controls to ensure that local public bodies are protected.
- **Organisational Business Continuity** – ensuring that internal Business Continuity arrangements cater for damage to or loss of IT systems, communications, or data.
- **Community Resilience** – recognising that strong inter-agency collaboration is an essential precondition for cyber resilient communities and partnerships.

Critical to addressing these issues was the development of policy, tools and techniques that will strengthen the focus across localities around inter-relations between these three capabilities in relation to cyber threats and attacks. It was also noted that greater clarity is needed on which of these capabilities is being considered at any time.

It was clear that there was still much to be done to engage senior leaders, political and official, in the challenges posed by this "nested" phenomenon. It was also necessary to clearly identify (at all levels – policy-making, leadership, practitioner and multi-agency response) points of responsibility and processes of accountability.

Within each of these three capabilities, there was a need for greater clarity on what constituted a desirable outcome for public sector leaders to work towards. Practitioners also need greater clarity, to determine whether the outcome had been achieved especially in a dynamic and evolving set of conditions. Guidance for senior leaders tailored to the achievement of the clarified outcomes would be most helpful, as would a simplification of the support structures and guidance available to practitioners.

It was not yet clear what would be the most effective and desirable policy interventions to support or ensure the achievement of the defined outcomes. The discussion considered the merits and challenges of a range of possible policy instruments including the provision of information and advice, legislation, funding, measurement, organisational support, or shared infrastructure and tools.

The discussion noted the plethora of policy initiatives and related guidance, which is often complex, confusing or contradictory from the perspective of local leaders and practitioners. Policy makers could help local public sector leaders and practitioners by providing clearer, simplified guidance on a set of cross-sector priority objectives, that have been developed and agreed with government and in partnership with wider stakeholders.

The evidence of the consequences from the risk of harm to the general public may suggest that it is reasonable to consider the creation of statutory obligations on public bodies for protection, response

and/or recovery. However, before that it would be sensible to explore whether there is a non-regulatory means to demonstrate that bodies were taking all reasonable measures (such as self-regulation or a code of conduct; the LGA cyber-readiness stocktake is a light-touch instrument in this regard). In the event of any statutory obligations being created, the issue of the cost of compliance must be addressed — where it falls and by whom it is borne — particularly in light of the financial pressures on local authorities.

Overall, the Consultation concluded that the scope and scale of the problem was greater than commonly appreciated in the public sector, and much work needed to be done to achieve greater clarity and understanding, put in place sufficient leadership structures, and then to establish the measures to be taken to achieve the necessary level of security and resilience across a number of dimensions.

9. Recommendations

The tone and content of the discussions throughout the Consultation, and in particular the "Asks and Offers" contributions at the end of the event, imply that the following warrant attention by the appropriate authorities.

- The development of policy, tools and techniques that will strengthen the focus across localities around inter-relations between IT security, organisational business continuity and community resilience in the face of cyber threats and attacks.
- Simplification and reform of national policy, with consideration of strengthening requirements, monitoring, planning and testing.
- Stronger messaging to move perceptions of the issue being about IT security to being about place-based resilience involving cross-organisational collaboration with active, dynamic leadership and planning.
- Wider and clearer communication on leadership roles, responsibilities, accountabilities and proactive collaboration.
- Production of advice on how to deal with a constantly adapting ecosystem with multiple actors, influences and threats.
- Reforming funding mechanisms to remove constraints on relevant funding streams and to make the level of funding appropriate to the risks faced.
- Clarification and simplification of national and local support organisations roles and responsibilities.
- Rationalisation of communication channels and advice sources.
- Development of methods for the assurance of veracity of materials and communication links.
- Wider promulgation of the lessons learned from case studies, exercises and wider NCSP/NCSC sponsored research initiatives.
- Champion the extension of the Local Digital Declaration community to encompass the Government's cyber research partners to support wider collaborative working.
- Collaborate in consolidating the wider lessons coming from the Local Leadership in a Cyber Society initiative in association with St George's House, RISCS and wider stakeholders to help inform policy and strategy development.

10. Next Steps

Think Cyber Think Resilience: Next Steps

As a follow-up to this consultation the Think Cyber Think Resilience initiative and the Research Institute in Science of Cyber Security (RISCS) look to work in partnership with the 90 plus participants of the related local leadership sessions that have been run in conjunction with St George's House since 2016 to: -

- **Define:** a series of steps to develop and implement clearer policy in relation to the three capabilities of local IT security, organisational business continuity and community resilience in the face of cyber threats ~~and~~ or attacks.

- **Determine**: the current situation, identify desirable policy objectives, and design feasible policy instruments (considering information collection and provision, regulatory action, funding, new organisational roles, and physical assets) and associated implementation plans.

- **Champion:** the continuing development of high-quality standards, guidance, communications and tools that will strengthen the focus across localities around inter-relations between IT security, organisational business continuity and community resilience.

- **Collaborate:** with wider stakeholders on ~~the~~ identifying the lessons coming from the St George's House Local Leadership in a Cyber Society discussions than can help inform the longer-term development of National Cyber Security Strategy and the Local Digital agenda.

In support of this, Think Cyber Think Resilience initiative will use the findings and recommendations from this consultation to help inform the development of Phase 2 of the Cyber Pathfinder training schemes [September 2019 to March 2020] covering: -

- **Pathfinder 4: Resilience Preparedness, Planning and Embedding Awareness:** To assist participants to integrate existing resilience arrangements with cyber resilience issues and to raise cyber resilience awareness within their organisations.

- **Pathfinder 5: Incident Management, Crisis Management and Communications:** To enable participants to understand the requirement for an effective incident management capability and crisis management requirements during a cyber incident.

- **Pathfinder 6: Business Continuity and Recovery from Cyber Incidents:** To enable participants to appreciate how business continuity complements cyber resilience and understands the requirement for effective recovery planning.

- The curation and development of the Pathfinder Academy Cyber Hub (built around Pathfinder outputs) on the Resilience Direct portal providing secure networking and a "one stop shop" for support and guidance to over 50,000 frontline users.

- Scope with local sector stakeholders and RISCS a high-level map signposting key policy and guidance to support cyber resilient strategy and standards for publication on Resilience Direct Cyber Hub and IStandUK

- Develop with the RED Cyber Team an update model for table top/live exercises to provide Warning and Advice Reporting Points (WARPs) and LRFs the opportunity to develop, test, exercise and review their Cyber Response Plans including their Cyber Technical Advice Cell (C-TAC) approaches[14]. This would test multi-agency response approaches and linkages to NCSC / National Cyber Incident Response arrangements.

- Work with the MHCLG Local Digital Collaboration Unit (LDCU) to help the Local Digital programme gain a deeper insight into the cyber risks in local sector and look at the scope to prototype additional support offerings to ensure that cyber skills and awareness are embedded across localities beyond the current National Cyber Security Programme.

The Research Institute in Science of Cyber Security (RISCS): Next Steps

RISCS supports the active continuation of the Local Leadership in Cyber Society dialogue and its participants aspirations to promote civic cyber resilience by building upon the collaborative work and networking of its diverse community.

Some forms of support that can be offered by RISCS and examples of collaboration to date include:

- Conducting collaborative research exploring the challenges and possible benefits of establishing a local sector Cyber Emergency Response capability (CERT-type) in the UK and its potential for building capabilities and capacity in handling cyber incidents and managing risks at the local level;

- Bridging the RISCS community's research insights and emerging lessons with usable policy implications so that local leaders, policy makers and practitioners can better contextualise the challenges they face with the state of play in cyber security and resilience research;

- Partnering in the development of future investigative and deliberative spaces for participants of the NCSP sponsored Think Cyber Think Resilience events, Cyber Pathfinder Training Scheme and St George's House consultations with the intention on establishing a capability building community of cyber security and resilience practice across the civic sector and its partners;

- Exploring the potential for developing bespoke, sector-specific maps of the policy landscape that could be aligned with the National Cyber Security Strategy objectives to help support the localised adoption implementation, delivery and impact of its policies;

- Initiating discussions with the RISCS community about how to better support local authorities and local resilience organisations in dealing with cyber security and resilience challenges.

[14] See Annex 3 Cyber-Technical Advice Cell guidance for Local Resilience Forums in England

Participants

Mr William Barker	Head of National Cyber Security Programme – Local MHCLG
Ms Helen Braithwaite	Head of Standards, Training and Exercising, NCSP-Local MHCLG
Mr Mark Brett	Cyber Security Advisor MHCLG
Dr Edward Brooks	Executive Director: The Oxford Character Project
Dr Madeline Carr	Associate Professor in International Relations and Cyber Security UCL STEaPP
Dr Alex Chung	Research Fellow University College London, Department of Science, Technology, Engineering and Public Policy (UCL STEaPP)
Ms Joanna Clift	Owner Jo Clift Consulting
Mr Geoff Connell	Head of IMT Norfolk County Council
Ms Siobhan Coughlan	Programme Manager Local Government Association
Mr David Cowan	ICT Manager Copeland Borough Council
Miss Alice Crilly	Policy Advisor Cabinet Office
Mr Jamie Cross	Advisor – Cyber Security Local Government Association
Ms Maewyn Cumming	Data Protection Officer MHCLG
Dr Daniel Dresner	Academic Lead for Cyber Security University of Manchester
Mr Andrew Everitt	Resilience Capability Lead Cabinet Office Emergency Planning College (EPC)
Mr William Harvey	Head of Government Cyber Defence Cabinet Office

Mr Michael Horrigan	Programme Delivery Lead MHCLG Digital Directorate
Mr Philip James	National Capabilities Research and Development Manager MHCLG
Mr Andrew Jones	Head of Strategy, Capability and Training Information Risk Management Ltd
Mr Bob Kamall	Programme Manager MHCLG
Dr Robert MacFarlane	Deputy Director Cabinet Office, Civil Contingencies Secretariat
Mr Paul Mitson	Chief Inspector (Hemel Hempstead Police Station) Hertfordshire Constabulary
Mr Steve O'Connor	Group Chief Technology Officer MHCLG
Mrs Helen Olsen Bedford	Publisher - UKAuthority
Mr Owen Pritchard	Cyber Security Programme Manager LGA
Mr Paul Sheehan	Non-Executive Director of Solace in Business - Society of Local Authority Chief Executives (SOLACE)
Mr Erik Silfversten	Senior Analyst RAND Europe
Mr Louis Stockwell	Local Cyber Resilience Programme Lead iNetwork (Tameside Metropolitan Borough Council)
Mr Phil Swan	Chief Information Officer and Digital Lead Greater Manchester Combined Authority
Mr Jeffrey Thomas	Chairman - Hartham Group Ltd
Mr Stephen Vercella	Head of ICT Wiltshire Council
Mr Paul Waller	Researcher - University of Bradford

Mr Nik W	Cyber Security Business Consultant National Cyber Security Centre
Mr James Young	Cyber Resilience Programme Manager MHCLG

St George's House Consultation

Local Leadership in a Cyber Society 3: Building Resilience Together – Lessons for the Future

Annexes:

1.1 **The case of cyber-attacks following a major incident**: Steve Vercelli, Head of ICT Wiltshire Council and Wiltshire Police

1.2 **The case of a targeted attack on a local authority:** David Cowan ICT Manager Copeland Borough Council

2.0 **Local Leadership in Cyber Society: Sponsoring Initiatives**

3.0 **Cyber-Technical Advice Cell guidance for Local Resilience Forums in England**

Annex 1.1 The case of cyber-attacks following a major incident: Steve Vercelli, Head of ICT Wiltshire Council and Wiltshire Police

"As the novichok poisoning incident unfolded in Salisbury in early 2018, we realised that Wiltshire had become a centre of attention worldwide. What we were slower to realise was that this interest was not restricted to the media, but also manifested itself as a **huge increase in activity to break into our systems** causing significant additional work to ensure they remained secure."

Wiltshire Council
Where everybody matters

Wiltshire Council

- A unitary authority
- The Council's ICT department provides ICT services to Wiltshire Council and Wiltshire Police on a shared ICT infrastructure
- We support approximately 4,000 Council users and 2,000 Police users
- ICT has an establishment of 118
- Support is 24x7 but minimal coverage out of office hours
- Council currently use O365, Police do not.

Wiltshire Council
Where everybody matters

2017 – Important Learning Before the Event

Cyber incident exercises with Wiltshire Police

- Where do ICT get their decision making authority?
- Use of decision models to guide and document decisions (NDM/JDM)

Poor IT Health Check

- Good understanding of vulnerabilities
- Focus on security within organisation.

Wannacry

- Development of a disconnection process.

Wiltshire Council
Where everybody matters

Initial Incident

"NCSC: …increased Cyber Threat to entities involved in the investigation of the incident in Wiltshire".

Monday 5th March		Thursday 8th March	
BBC News report - a man and woman have been poisoned by an unknown substance in Salisbury	Contact made with NCSC (thro Wilts Police) and lines of comms established. Possibility of disconnection considered. Possibility of disabling vulnerable systems considered	Salisbury Hospital report attempt to hack their systems. Council firewalls show unusual activity. Both originating from Russia.	Decision to continue monitoring.

Wiltshire Council
Where everybody matters

Initial Incident

Friday 9th March

Council Shadow Recovery Group informed systems could be turned off if significant threat and could escalate to disconnection of all external connections.

ICT authority reconfirmed.

ICT Manager and senior technician rota established.

Internal comms prepared

High alert detected by O365 (Malware campaign)

Decision made to disable Access to email & calendar from mobile phones (significant vulnerability) causing significant disruption

Wiltshire Council
Where everybody matters

Learning from initial incident - 1

Security risk is not a constant (secure or not secure), it continuously changes

- Interest in your organisation varies and spikes
- ICT systems constantly change, therefore so do their security vulnerabilities
- As a result, security risk is constantly changing

Need to react to these changes

- We shut down systems with vulnerabilities when the threat changed

Need to proactively plan for changes in risk

- When your organisation is "of interest", the threat increases

Wiltshire Council
Where everybody matters

Learning from initial incident - 2

Are processes, authorities & attitudes fit for purpose (cyber attack)?

- Is ICT authority clear? – learnt from exercise
- Can ICT disconnect at **any** time? – learnt from Wannacry
- Can you quickly put necessary out of hours cover in place (technical & management)? – learnt this in incident

Need to proactively plan for changes in risk

- When your organisation is "of interest", the threat increases

Documentation

- Use of NDM to document decisions provided valuable information after the event

Wiltshire Council
Where everybody matters

Learning from initial incident - 3

Business Continuity

- Business areas don't understand their reliance on ICT very well

Wiltshire Council
Where everybody matters

Initial incident - Question

Do you use your IT Health Checks, security audits, etc to prove you are secure or to understand your vulnerabilities?

Wiltshire Council
Where everybody matters

The Incident That Keeps on Giving

- Increased interest – Wiltshire is now known worldwide
- Led to increased attempts of unauthorised access to O365 accounts
- Led to high instances of account lockouts
- Led to ICT Service Desk being swamped with account reset requests
- Impacted the services provided by ICT

Wiltshire Council
Where everybody matters

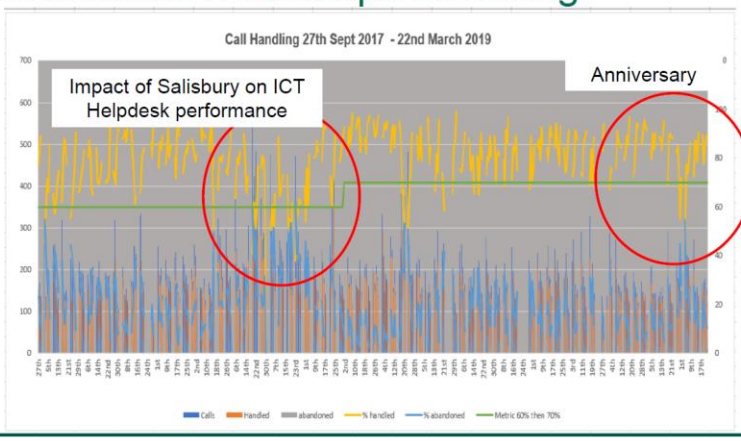
The Incident That Keeps on Giving

- Prior to event 28k authentification attempts every 3 day. During event 86k in 24 hours
- An attempt to authenticate every 1-3 seconds
- Service desk receiving 500 calls per day to unlock accounts (reminder – 4,000 users)
- 5 accounts trying to authenticate from overseas investigated

- This increase in activity happened each time incident was in the news (e.g. Amesbury)
- And when it wasn't in the news (e.g. anniversary of Salisbury)

Wiltshire Council
Where everybody matters

The Incident That Keeps on Giving



Wiltshire Council
Where everybody matters

Learning from continuation of incident (and not learnt)

- External events can impact your internal service
- Plan for them
  - We planned for physical disruption by protesters at a Council Meeting, but didn't plan for possible cyber disruption
  - But we are planning for National Armed Forces Day (being held in Salisbury
- Technical
  - Need to move to MFA or biometrics
  - Need to exploit O365 security more

Wiltshire Council
Where everybody matters

Other Stuff

- Not all external communications are helpful
- Working at different security levels is "interesting"
- Authentification with NCSC can be lengthy
- Significant ICT work to support evacuation of Salisbury offices for decontamination (and to move back in)
- Engagement with NCSC provides a level of reassurance (NCSC on site visit)
- MHCLG also provided additional support

Wiltshire Council
Where everybody matters

Summary of Impact

- Council/Police data was not compromised

BUT….

- It felt like a Denial of Service Attack
  - Service Desk stopped functioning
  - Works queues built up a backlog
  - 10%+ Council workers were locked out of their accounts on a daily basis
  - Mobile phones could not be used for email/calendar

Wiltshire Council
Where everybody matters

Annex 1.2 The case of a targeted attack on a local authority: David Cowan ICT Manager Copeland Borough Council

Background

Copeland borough council
Proud of our past. Energised for our future.

- Copeland Borough Council is a very small local authority nestled on the west coastline of Cumbria, largest town is the port of Whitehaven.
- We have an Elected Mayor, 33 elected members and 230 staff.
- Primary employer within the local authority area is the Nuclear Decommissioning Authority (NDA) at Sellafield.
- In 2017, the council suffered what is believed by many to be one of the most devastating Cyber Attacks to ever occur within UK Local Government and at the present time 2019 the Council remains in recovery mode.

www.Copeland.gov.uk

Cyber Attack 2017

Copeland borough council
Proud of our past. Energised for our future.

- Despite having fully updated and active Anti-Virus software in place, the council systems were hit by what is known as a **"zero day" virus** and therefore the active Anti-Virus software did not recognise the virus and did not prevent the attack
- The **cyber attack** was also conducted over an August **bank holiday weekend**, providing a long period of time before discovery and the start of the Council's response. This helped maximise the impact of the virus to Council IT servers.
- By the time of discovery and the commencement of containment actions, the Council was at the point of having **lost nearly all key IT systems**, **all network services** and near **100% of the end-point devices** such as desktops and laptops.
- As soon as our partners in our shared service initiatives were informed of the problem, the Council was also **immediately cut-off from all access to shared services** to all partners to prevent cross-contamination.
- The Council found itself in a position where **technology effectively no longer existed**.

www.Copeland.gov.uk

Cyber Resilience

Copeland borough council
Proud of our past. Energised for our future.

- The Council found itself in a position of **assuming** the **internal IT team would just sort** everything quickly, but this quickly became apparent that this was not a realistic expectation.
- Copeland has a very **small IT team**, the scale of total loss suffered over-whelmed what IT resources were in place and extra IT help needed to be brought in quickly to help recovery.
- The Council also discovered that existing **emergency plans** and **business continuity plans did not cater sufficiently for a scenario of 100% IT loss,** and in a scenario where you no longer have email or IT systems to communicate, the Council found itself in needing to setup a new daily physical meeting of key managers to deal with the new scenario.
- The **IT network was compromised** and it took many days just to regain control of some pockets of the network. It was at this early point in the recovery that the most significant impact of the attack was discovered, the **system backups in place were compromised**, so a straight-forward restore of the IT systems to a state prior to the Cyber attack was not an option
- The **IT infrastructure was going to need to be rebuilt from the ground up** and that meant a long period of time (months) with no IT systems at all.

www.Copeland.gov.uk

Cyber Resilience - Impacts

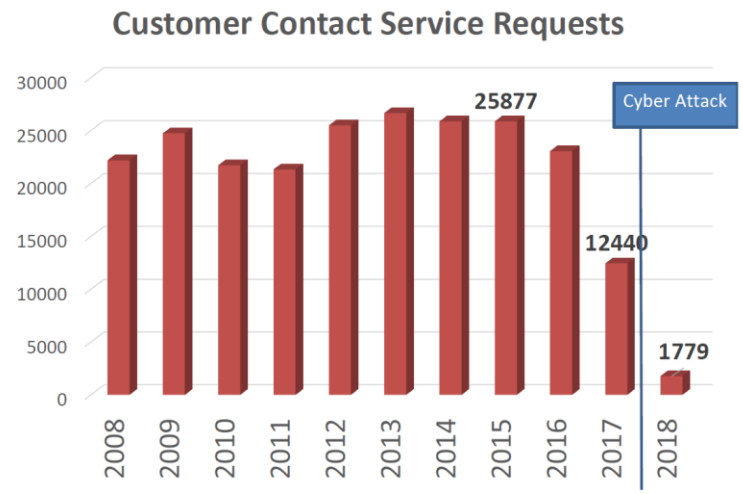
Copeland borough council
Proud of our past. Energised for our future.

- Nearly all Council activity had to **revert to pen and paper**, even the ability to pay Council staff was lost and the authority was forced to revert to organising paper cheques to pay staff wages.
- Staff where possible were dispersed to work in non-council locations and where feasible neighbouring local authorities, if that enabled them to have access to relevant IT systems external to the Council.
- Approaching 2 years after the initial event, **Copeland remains in recovery mode** with some IT systems still in the process of undergoing remediation. Some data has been subject to total loss.
- Leaving aside the costs of lost productivity and the enormous service impacts, this one Cyber attack has to date **cost a minimum of £2.5 million pounds** and the recovery costs continue. Total council budget for all services is circa £9m per annum
- Our customer service IT systems recorded an average of 25,000 processed service requests per annum prior to the Cyber Attack

www.Copeland.gov.uk

Cyber Resilience - Impact

Copeland borough council
Proud of our past. Energised for our future.



www.Copeland.gov.uk

Key Learning Points

Copeland borough council
Proud of our past. Energised for our future.

- **Chief Exec and Leadership Team Buy-in** and Active Support is Crucial
- **Be Prepared**
  - Make sure your Cyber Defence Investment is Appropriate **AND** Sufficient
  - Make sure you have plans for a total IT loss scenario
  - **Do not default to assuming IT is Safe** – Ask and Verify.
- **Data and System Security** is the **Responsibility of All Staff**
  - Everyone has a Stake in Data and Systems Being Safe and Secure
  - **Don't forget your Service Partners and Suppliers**
- As the Systems needed to be rebuilt decisions were taken to adopt a **Cloud Hosted First** approach to empower a **future Agile workforce** to avoid a repeat of this scenario.
  - Where key IT systems were completely external to the Council, such as hosted solutions, the Council was able to utilise these systems.
  - Control your deployed end-point devices – Laptops, Phones, Tablets, IoT Devices

www.Copeland.gov.uk

,

Key Advice

Copeland borough council
Proud of our past. Energised for our future.

- **Take Cyber Defences Seriously** and **Be Prepared**
- Well maintained and configured Firewalls and Supporting Network Devices
  - Ensure all points of ingress and egress are covered
- Forced **Regular vulnerability patching** across the entire estate.
  - Copeland force patch at least once per week, and will push key security vulnerability patches out the same day when required, but only after testing the patch on our lab kit.
- **Defence in Depth**
  - Make sure you are not vulnerable to a single point of failure
  - Zone and Segment the network to control the network traffic flows
- **Backup in Depth**
  - Follow an appropriate regime for the data
  - Backup at least once per day, with transaction log backups inter-day where appropriate.
  - Do not rely on single location backup
    - Copeland backup all data to 3 locations per day – 2 onsite, 1 offsite.
  - Ensure users are not saving files to any location that is not being backed up
    - Files should not be saved on local hard drives
  - Make sure Cloud and Hosted data services are being backup up properly
- **Follow Advice** From **National Cyber Security Centre Programme**

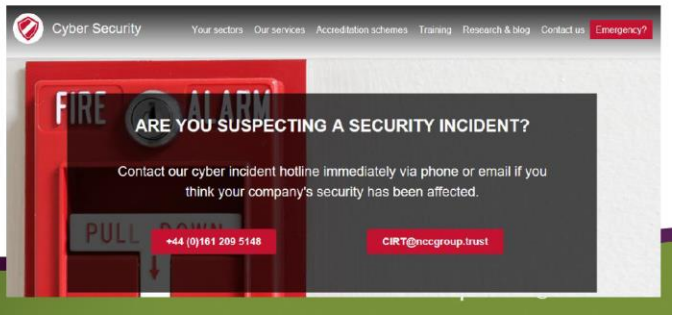
www.Copeland.gov.uk

Key Advice

Copeland borough council
Proud of our past. Energised for our future.

- **Make sure you have a "Phone a Friend"**

- Know the organisations you could reach out to for help before you need them and embed in your emergency planning in a sensible fashion.
  - Key Supplier Contacts
  - Key Partner Organisation Contacts
  - NCSC
  - Cyber Crime Units
  - Trusted Organisations who run "Cyber Incident Services"
    - NCC Group
    - Claritas
    - etc



So We Are Safer In The Cloud ?

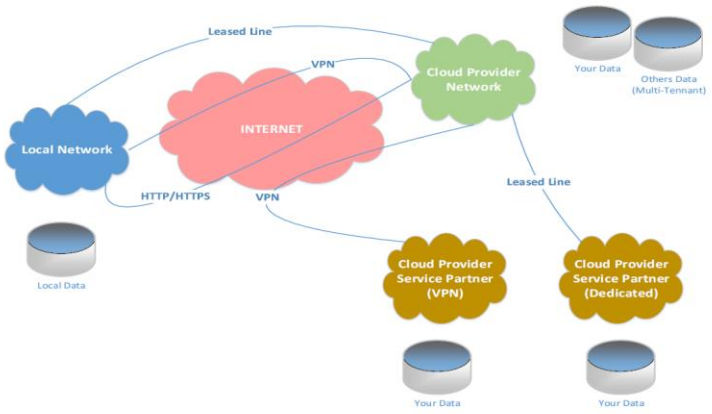
Copeland borough council
Proud of our past. Energised for our future.

- Very Misleading and Widespread misconception, it very much depends on what you have done to protect yourself in the Cloud.
- **Basic Cyber Risk Profile (Premises vs Cloud)**
  - Very hard to compare, but the risk surface area for a potential Cyber Attack before applying any measures is higher by its nature and **therefore more NOT less** needs to be done to protect Cloud systems.
  - Before any security measures are deployed, we explain it as:
    - Risk Locally **On Premises 5 out of 10**
    - Risk for **Cloud Hosted 8 out of 10 (**Recent Pen Tester suggested more like 9/10**)**
  - If you running a **Hybrid Setup** – part-on site and part in Cloud, you have increased risk not reduced risk.
    - If you are running a Key System which is not 100% Cloud, it is also not 100% Agile or Resilient, it is subject to failure both On Premises and in The Cloud

www.Copeland.gov.uk

Understand Your Risk Scope

Copeland borough council
Proud of our past. Energised for our future.



- **Supplier Information Security Assessment**
  - Conduct Full Cyber Security Risk Profile on All Suppliers AND Their Suppliers

www.Copeland.gov.uk

Supplier Information Security

Copeland borough council
Proud of our past. Energised for our future.

- Start the Cyber Security supplier risk assessment early in the procurement process and do regular reviews.

- Sample Questions To Consider Asking Your Suppliers
  - Who am I entrusting with my data – do they hold verifiable certifications?
    - Think of Yahoo, LinkedIn, Facebook, Hosted Web Sites, Forms Servers
  - Where is my data stored in terms of geography – Not just **"in the Cloud"**
  - What backup strategy is followed with my data
    - Is it Backed up and in a resilient fashion, what is recovery RTO
  - Is my data "encrypted at rest"
  - Is my data "encrypted in transit"
  - Is the Cloud Host wholly owned or sub-contracted out
    - If contracted out ask all the same questions of them as well
  - What Cyber defences does the Cloud provider follow
  - What security vetting do the providers staff have
  - How is the system monitored
  - Single versus Multi-Tennant – How does supplier assure separation
  - Who controls sign-on permissions
  - How long to Recover in Disaster Event

www.Copeland.gov.uk

Cyber Security Technology

Copeland borough council
Proud of our past. Energised for our future.

- **Firewalls**
- **Anti-Virus** – all points
  - Network Ingress, Egress, All user end-points and Servers
  - Everybody uses don't they – Do They?
- **Regular Patching** of All software
  - Allowing software to drift away from upgrades is bad news
- **Email Phishing defences** – DMARC/DKIM
  - Assuring sender is the real sender
- **Check your Logs**
  - Know what attacks/probes you are catching
  - Review daily, Take action
  - NCSC Logging Made Easy (LME)
    - https://www.**ncsc**.gov.uk/b**log**-post/**logging**-made-easy
- **Network Zoning and Segmentation**
- **Physical protection**
  - Removable media, portable disks, physical Access to Infrastructure
- **Regular IT Health Checks and Pen Testing**
  - Consider Rotating Suppliers Each Time – Once per year is insufficient
- **Cyber Training for All Staff and Members**

www.Copeland.gov.uk

Cyber Security Technology

Copeland borough council
Proud of our past. Energised for our future.

- **Information Classification**, supported by technology
- **Data Loss Prevention**
  - What ways can someone remove copies of your data
- **Cloud Access Security Broker**
  - Do you have control of who in your authority can access what?
- **White-listing** all Browser Cloud Access
  - Protective DNS service (National Cyber Security Centre provide service)
- **Advanced Log Collection**, filtering and monitoring
  - Patterns Searching
- **Intrusion Detection**
  - Has someone actually got in despite your Cyber defences
  - Remember Copeland was hit with "Zero Day"
- **Advanced Monitoring**
  - 24x7 Active Monitoring and Alerting (SOC or Managed SIEM)
- **External, independent reviews**
  - Annual PSN Re-certification and IT Health Checks
- **Regular Drills**
  - National Cyber Security Centre is running programme of events

www.Copeland.gov.uk

Annex 2: Local Leadership in Cyber Society: Sponsoring Initiatives

"Think Cyber – Think Resilience" Initiative

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 3000 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. In recognition of this work the OECD awarded MHCLG's work on leading the NCSP "Think Cyber – Think Resilience" Local Leadership in Cyber Society Initiative Public Sector Innovation Exemplar status and the project now forms part of the OECD Innovation Observatory.

Key note Think Cyber-Think Resilience deliverables in support of the NCSP presently include: -

- The establishment of a National Civic Cyber Pathfinder Training Curriculum [see table 1 below] comprising 12 specialist exercise and training modules providing over 40 hours of cyber training for use of local public sector, leaders, policymakers and practitioners. The curriculum was developed in association with the Cabinet Office Emergency Planning College, NCSC Digital Government Unit, Resilience and Emergencies Directorate, LG Cyber Stakeholder Group and inputs from the NCSC sponsored Research Institute in Science of Cyber Security (RISCS) and its Evaluating Cyber Security Evidence for Policy Advice (ECSEPA) project.

- Creation and roll-out of a Cyber Pathfinders Training Scheme offering over 3300 free Cyber training places to local government and local resilience leaders to build their understanding and preparedness. A full programme of over 50 events across 8 regions is fully prepared with content, venues and training material in place to be delivered from April 2019 to March 2020. Pathfinders has been recognised in the DCMS National Cyber Skills Strategy as a Leading the Way Public Sector cyber skills training exemplar.

- The development and roll-out of National Multi-Agency Cyber Exercise scheme comprising 8 regional eight regional cyber exercises/training events around the country (January to March 2019) to give over 500 local government colleagues the practical opportunity to test local cyber capability and awareness issues with MHCLG, Cabinet Office, Police, NHS and the NCSC.

- Funding the establishment and development of a Cyber Hub on the Resilience Direct portal providing secure networking and operational support guidance to over 50,000 frontline users. Initial content is in pilot for an online Pathfinder Academy to be launched mid-2019. This has been under pinned by the development of the National Cyber Resilience Standard, updated Continuous Improvement Civil Cyber Resilience Model and supporting Cyber Planning and Self-Assessment tools in conjunction with the LRF community and the Resilience and Emergencies Directorate.

- Launch of the Greater Manchester Cyber Innovation Centre (GM-Cyber) which has been pump-primed funded as part of a wider Local Growth Fund agreement between GMCA and MHCLG. GM-Cyber now serves as a focal point (hub) for the cyber security sector in GM, enabling collaboration and joint development of related capabilities and supporting the wider national cyber security agenda and providing direct support to the Pathfinder scheme through its partner organisations INetwork and IStandUK though the MHCLG led NCSP Building Resilience Together workstream.

- The establishment of the Resilience and Emergencies Directorate – Cyber Resilience Programme to focus on supporting improved risk assessment, planning, training and exercising across localities. The RED Cyber advisors have built strong relationships at the local level across the country bringing together technical, resilience and leadership communities and under taken the following key activities: -

    - Delivery of Roving Storm Exercise to 19 of the 38 LRFs in the first 8 months of the programme. The majority of LRFs have also sent representatives to the National Pathfinder Training and Exercising events.
    - Delivery of clear, practical templates for LRFs to pick and use at the local level. This has helped LRFs to understand the risks and what they mean at a multi-agency level and to begin producing cyber specific response plans for their LRF.
    - Development of RED specific Cyber Hub guidance for the resilience community and as a place for the local resilience community of interest to come together to share experiences, best practice and lessons.
    - Support to the wider NCSP activities to ensure that products such as the Pathfinder series and NCSC's Active Cyber Defence are taken up and embedded in the LRF community.

- Participated in the establishment of the new Local Digital Declaration and the UK Resilience Cyber Standard that outlines a coherent set of expectations and codified good practice around civic cyber resilience. The standard forms part of the wider suite of UK Resilience standards and draws upon National Cyber Security Centre (NCSC) advice and guidance and the NCSP-Local developed Civil Cyber Resilience Model.

Table 1: Cyber Pathfinder Training Scheme Curriculum

Cyber Pathfinder Training Scheme:

Cyber Pathfinders is a new National Cyber Security Programme (NCSP) sponsored scheme to help the local public service and resilience community navigate their way through the complexities of cyber security and cyber resilience. The scheme will provide a range of free of charge cyber exercises and training seminars for local public sector participants running from January 2019 until March 2020.

Building on the success of the MHCLG led 'Think Cyber Think Resilience' initiative (that inducted over 2000 senior local leaders, policy makers and practitioners in raising cyber awareness) the NCSP in partnership with MHCLG and the Cabinet Office Emergency Planning College has specifically developed the **Cyber Pathfinder** scheme to provide participants with guidance on how to build a cyber-aware culture across their organisations, partnerships and the wider civil contingencies community.

Cyber Pathfinder events will see the roll out of over 3000 free training day places across 8 regional centres with online access to the learning materials and cyber exercising formats for local public service and resilience community participants. The event programme will provide participants with a deeper understanding the cyber agenda as follows: -

PATHFINDER EXERCISE: MULTI-AGENCY CYBER EXERCISE

Aim: To build a shared understanding of the implications for local multi-agency partners in responding to a major cyber incident.

Overview: This cyber exercise will help organisations to develop a shared understanding of the implications for Local Resilience Forums of responding to a major cyber incident. It will provide the opportunity for participants to consider how their well-established multi-agency crisis management procedures support the cyber response.

The exercise has been developed in partnership with the National Cyber Security Centre and Cabinet Office Emergency Planning College. Working in teams, participants will reflect on their own organisation's cyber preparedness and the wider multi agency considerations when responding to a major cyber incident.

Objectives:

- Examine and consider the implications and impacts of a major cyber incident on multi agency partnerships (LRFs) during a major incident
- Consider multi-agency response arrangements in managing the impact of a major cyber incident and highlight areas of vulnerability
- Identify common steps for individual organisations and the wider multi-agency (LRF) community in responding to a major incident of this nature.

PATHFINDER 1: CYBER LANDSCAPE, GUIDANCE AND SUPPORT

Aim: To provide participants with an overview of a baseline common understanding of the current cyber landscape and signpost participants to authoritative sources of guidance and support

Cyber Landscape: overview of a baseline common understanding of the current cyber landscape.

- Identifying the evolving nature of the cyber landscape
- Defining commonly used cyber terminology
- Understanding the evolving cyber risk picture
- Describe how cyber resilience fits into the wider resilience capability

Guidance & Support: signpost to authoritative sources of guidance and support

- Outline the work and role of the National Cyber Security Centre
- Reviewing the key guidance documents and online sources available;
- Signposting the key support and practitioner organisations and their roles
- Identify the legal, standards and regulatory requirements that organisations need to address

PATHFINDER 2: CYBER THREATS AND CORE RESILIENCE CAPABILITY

Aim: To provide participants with an understanding of the cyber threat landscape and the core components of a cyber resilience capability

Cyber Threat: provide a detailed understanding of the cyber threat trajectory.

- Identify why your organisation may be vulnerable;
- Describe the various types of attack methodology
- Role of threat analysis and its impact on organisational decision making
- How to identify supply chain dependencies (outsourcing and managed services)

Capability: outline the core components of a cyber resilience capability

- State the core components of a cyber resilience capability;
- Review current capability.
- Overview of core roles and responsibilities
- Interaction of policy and governance functions in support of capability building

PATHFINDER 3: PEOPLE, PROCESS, TECHNOLOGY

Aim: To provide participants with the core components to develop their own cyber resilience programme build around people, processes and technology

People, Processes and Technology: outline the core components to developing a cyber resilience programme.

- How to treat cyber resilience as a people centred issues and keep people involved and informed
- Focussing on staff roles and how cyber resilience is everyone's responsibility
- Ways to champion and develop a culture of cyber awareness both within and beyond your organisation
- Know and understanding how business critical systems , assets and data need to be cyber secure
- How to look at the cyber agenda as being beyond the organisational technology brief
- Understand the role Active Cyber Defence and key cyber technology standards
- Identify the core components of cyber policy that needs to be addressed in any organisational programme
- Clarify the approaches to cyber threat analysis and how they can inform approaches to risk.

PATHFINDER 4: RESILIENCE PREPAREDNESS, PLANNING AND EMBEDDING AWARENESS

Aim: To assist participants to integrate existing resilience arrangements with cyber resilience issues and to raise cyber resilience awareness within their organisations.

Resilience, preparedness and planning: integrate existing resilience arrangements with cyber resilience issues.

- Consider how responding to a cyber incident can be made part of your business as usual routines
- Describe the additional considerations rising out of a cyber incident;
- Look at how to develop procedures and tools to manage a cyber incident based on established guidance
- Create an outline cyber exercise programme and how to capture lessons learnt.

Embedding Cyber Resilience: raise cyber resilience awareness and education within their organisations

- Introduction to a range of awareness offerings and how they can be applied across organisations
- Support awareness programmes on cyber resilience
- Identify the competencies to support a cyber resilience capability
- Recognise the need for continuing professional development in order to maintain readiness for a cyber incident

PATHFINDER 5: INCIDENT MANAGEMENT, CRISIS MANAGEMENT & COMMUNICATIONS

Aim: To enable participants to understand the requirement for an effective incident management capability and crisis management requirements during a cyber incident.

Incident Management: To develop a clear understand of the requirement for an effective incident management capability.

- Describe incident management response mechanisms;
- Differentiate between the unique considerations during a cyber incident and a typical incident;
- Understand the role of the Joint Emergency Services Interoperability Programme (JESIP) principles in incident management
- How to access Local Resilience Forum model - Incident Reporting and Cyber specific Response Templates

Crisis Management and Communications: To embed the take-up of crisis management requirements during a cyber incident

- Differentiate between incident management and crisis management requirements;
- Define the thresholds for escalation within the response;
- Recognise the requirements of effective internal and external communications
- Understanding working with the Media during an incident

PATHFINDER 6: BUSINESS CONTINUITY AND RECOVERY FROM CYBER INCIDENTS

Aim: To enable participants to appreciate how business continuity complements cyber resilience and understands the requirement for effect recovery planning.

Business Continuity: Establish an appreciation of how business continuity complements cyber resilience.

- Outlines the linkages between business continuity life cycle and cyber resilience
- Explain the relationship between service recovery time objectives and disaster recovery
- How to assess BCM recovery time objectives against a cyber incident
- Identify the need to assess critical suppliers' resilience arrangements

Recovery: Outline the requirements for effect recovery planning

- Understand the need to review recovery plans in relation to cyber incidents
- Post incident report and how to implement lessons through a change management processes
- Role of remediation planning (quick fixes for restoring to a normality);
- Need to agree recovery priorities (cyber systems and prioritised services)

Building Resilience Together – Executive Briefing Papers

Several of the participants in the Local Leadership in a Cyber Society strategic round tables and discovery days at St George's House Windsor, 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 now form a series of Building Resilience Together briefing papers (see below) which contain articles and guides on the need to take a strategic approach to leadership issues arising from the civic cyber resilience agenda.

To find out more about how Think Cyber Think Resilience though leadership activities are helping local public sector organisations see https://istanduk.org/cyber-resilience-2/ where you will also find the following Building Resilience Together Executive Briefing Papers and guides:

- Resilient by Design: Key strategic design principles for a civic cyber resilient organisation
- Resilient by Design 2: Sources of online guidance on applying the Civic Cyber Resilience Model
- Leadership in Practice: The role of strategic leadership in civic cyber resilience.
- Resilience in Practice: Practical steps that civic organisations can take to be cyber resilient.
- Partnering for Resilience: The role of inter-agency collaboration in supporting civic cyber resilience.
- Strengthening Technical Resilience: The role of technology leadership in helping to strengthen local civic cyber resilience.
- Cyber Emergency Response: Understanding the role of a Computer Security Incident Response Team (CSIRT)

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

Research Institute in Science of Cyber Security (RISCS)

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

University College London's Department of Science, Technology, Engineering and Public Policy (UCL STEaPP)

UCL STEaPP explores how scientific and engineering expertise can meaningfully engage with public decision making and policy processes to tackle pressing global issues and improve public wellbeing. UCL STEaPP is a uniquely policy-oriented department which sits across three UCL Faculties: the world class Faculty of Engineering Sciences, the Bartlett Faculty of the Built Environment and the Faculty of Mathematical and Physical Sciences.

To find out more, visit: www.ucl.ac.uk/steapp

Evaluating Cyber Security Evidence for Policy Advice (ECSEPA)

The ECSEPA project seeks to provide support for UK cyber security policymakers – particularly those civil servants who provide short and long-term policy advice, either in response to specific crisis incidents or in the context of longer-term planning for cyber resilience and capacity building. This two-year, EPSRC funded project was developed in collaboration with a range of partners including the National Cyber Security Centre (NCSC) and the Foreign and Commonwealth Office.

Policymakers, sometimes with little relevant expertise and often in time-critical scenarios, are asked to assess evidence from a mix of sources including official threat intelligence, academic sources, and industry threat reports. Such a diverse evidence base is then used to make judgments on threats, risk,

mitigation and consequences, and offer advice shaping the national regulatory landscape, foreign and domestic security policy, and a range of public and private sector initiatives.

This project seeks to understand the challenges faced by the UK's policymaking community in interpreting, evaluating and understanding evidence about cyber security by:

- Investigating how UK policymakers select evidence, why they privilege one source over another, and how adept they are at recognising possible weaknesses or flaws in evidence;

- Identifying the particular challenges of decision making in this context and evaluate how effectively policymakers make use of evidence for forming advice.

To find out more, visit: http://ecsepa.coventry.ac.uk/

ECSEPA Mapping Project

'Cyber Security Policy Making in the UK: Mapping the Landscape' is a RISCS-funded spin-out research project from the ECSEPA main project. It emerged from the realisation that there is a lack of clarity about how cyber security is organised within the UK Government – even for those who work at the heart of it. Understanding where cyber security policy is being developed and implemented, how different issue bases interact and coincide, where there is duplication and where there are gaps, is essential to understanding how a complex, rapidly developing policy landscape like this one should be organised to be most effective.

There are three parts to this project:

- A mind-map created using data captured from public domain websites and interviews with the policy community;

- Workshops and meetings held with the UK policy community to validate the map;

- Infographics and web content developed to facilitate the map's launch event at RISCS aimed at returning the map to the research and policy communities in a useful and accessible way.

The primary impact ambition of the ECSEPA team is directed to bringing benefit to the civil service and policy community. To do this most effectively, we are drawing support from the NCSC, RISCS, and the newly established Policy Impact Unit (PIU) based in UCL STEaPP. Together, we are developing a series of policy engagements that will be incorporated into the broader ECSEPA policy impact plan.

To find out more about the project, visit: http://ecsepa.coventry.ac.uk/ecsepa-mapping-exercise/ and to request access to the ECSEPA Map, visit: https://www.riscs.org.uk/ecsepa-map/

Annex 3: Cyber-Technical Advice Cell guidance for Local Resilience Forums in England

Ministry of Housing, Communities & Local Government

Cyber-Technical Advice Cell guidance for Local Resilience Forums in England

Any comments on this document should be sent to REDcyber@communities.gov.uk
July 2019

Introduction

This document provides guidance on the specific advice that may be required during a cyber incident and should not be confused with the national Scientific and Technical Advice Cell (STAC) guidance[15].

As with other emergencies, Local Resilience Forums (LRFs) should consider pre-planning for a Cyber-Technical Advice Cell (C-TAC), including collation of the contact details of potential members and undertake awareness training for possible C-TAC chairs and cell members not normally involved in a multi-agency emergency response.

As a first step to implementing this guidance, LRFs should identify which technical experts in the local area would advise and support the Strategic Co-ordination Group in the event of a Cyber incident.

1. The role and purpose of the Cyber-Technical Advice Cell (C-TAC)

1.1 The purpose of the C-TAC is to ensure timely coordinated advice, in a local area, during the response and recovery from an emergency with a cyber element.

1.2 The C-TAC brings together technical experts operating under the strategic direction of the Strategic Co-ordination Group (SCG) or Recovery Co-ordination Group (RCG) if responsibilities have transferred.

1.3 The establishment of a C-TAC has an important role in supporting the SCG/RCG. It provides an understanding of the likely impacts and consequences for the multi-agency partnership including understanding what the impact on one or more agencies systems has on the partnership's ability to effectively manage the response or recovery from another incident.

1.4 The C-TAC should bring together technical experts, law enforcement and various other individuals from those agencies affected, or from the local area to provide awareness and advice to the SCG/RCG and where appropriate, the Tactical Co-ordination Group (TCG).

1.5 The C-TAC also provides a useful mechanism to link the local level technical response to any national technical response as set out further in Section 6. It may be appropriate for the NCSC or other national organisations to be represented at the C-TAC and it provides a route for national technical advice and guidelines for a particular incident to be cascaded to local areas.

1.6 The purpose of the cell is to ensure that, as far as possible, technical, business continuity, risk assessment and cyber security related advice and guidance for the SCG/RCG (and others involved in the response and recovery) is clear and not conflicting. It will do this by co-ordinating technical discussions to ensure that advice given by the cell is the best possible based on the available information in a timely, coordinated and understandable way as per the Joint Emergency Services Interoperability Principles (JESIP) Joint Decision Model (JDM)[16] (see annex C) for more details.

1.7 The C-TAC is tasked by the SCG/RCG. Any member can request specific technical advice or further explanation following information previously received. This clarification may also be required by the TCG. Where this is the case, this request will be notified to the SCG/RCG so members are aware this further work has been tasked.

1.8 The role of the cell in response to an incident would be to:

[15] https://www.gov.uk/government/publications/provision-of-scientific-and-technical-advice-in-the-strategic-co-ordination-centre-guidance-to-local-responders
[16] https://www.jesip.org.uk/home

- provide a common source of specialist advice that is accessible to non-technical responders;
- monitor and co-ordinate the responding technical community to deliver on the SCG/RCG priorities;
- pool advice and guidance and arrive, as far as possible, at an agreed view on the technical merits of different courses of action;
- provide a common brief to the SCG/RCG on risk, how the situation might develop, what this means, and the likely effect of various mitigation strategies;
- identify other agencies / individuals with specialist advice who should be invited to join the cell in order to inform the response;
- liaise with national agencies (including the National Cyber Security Centre, law enforcement, ICO and sector specific cyber technical leads[17]); and, where warranted, the wider technical community to ensure the best possible advice is provided;
- liaise between agencies to ensure consistent technical advice is presented locally;
- ensure a collective and co-ordinated technical response, where possible, to avoid duplication and overcome any confliction issues;
- maintain a written record of decisions made and the reasons for those decisions.

1.9 The requirement, formation and constitution of the C-TAC is to be locally determined by the SCG/RCG at the time of the incident and is directly accountable to the SCG/RCG.

1.10 It should be noted that the cause of a cyber-attack or incident and whether it was due to criminal action is not for consideration of the C-TAC. This is a role for the individual organisations affected working with the police and other crime agencies. The C-TAC should however assist the appropriate agencies, providing relevant information ascertained regarding the incident.

2. Membership of the C-TAC

2.1 At the time of the incident response, the SCG/RCG members will identify the right composition of the C-TAC.

2.2 The composition and function of the C-TAC will be incident specific and tailored to local requirements.

2.3 Members should have the necessary knowledge and skills to collectively provide technical advice and are likely to include technical specialists from the constituent organisations taking part in the SCG/RCG, especially those affected by the cyber incident.

2.4 Agencies and individuals with specific capabilities and/or responsibilities should be represented dependent on the type of incident and requirement for specific technical advice, such as the National Cyber Security Centre, Warning and Reporting Point (WARP) leads, regional police Cyber Crime Units, utility providers and transport operators, academia and specialist corporate organisations (see Annex A for a description of national agency roles in an emergency).

2.5 Information should be shared with all SCG/RCG members and the wider LRF partnership, regardless of representation on the C-TAC, in order to ensure any preventative measures are applied should the cyber-attack have the ability to affect multiple agencies.

2.6 The chair of the C-TAC is likely to be a strategic senior director (or equivalent) from the main affected organisation however this will be determined at the time of event considering availability and suitability.

[17] This may include Competent Authorities under the Security of Network and Information Systems Regulations. Further information is provided at Annex B.

2.7 The chair will sit on the SCG/RCG, reporting back findings and resolutions as requested and required. The chair does not necessarily need specialist knowledge, but they do need the skills to actively question members and effectively chair what may be a complex technical multi-agency meeting and command the respect of their peers. They also need to have the ability to arrive at a consensus based on the information available, which may be limited.

2.8 The chair should be able to translate technical material into plain English for the SCG/RCG to make appropriate decisions given the information provided.

2.9 All cell members should have a basic understanding of command and control principles including the responsibilities of agencies during an emergency response (See annex C for Joint Emergency Services Interoperability Principles (JESIP) and the Joint Decision Model (JDM)[18]).

2.10 It should be noted that although some national organisations have a local presence i.e. Public Health England and Environment Agency, if the attack is widespread and affects more than one LRF area, these organisations may choose to co-ordinate their advice through national arrangements rather than attend local C-TACs.

3. Working alongside a STAC

3.1 Where a traditional STAC has been formed due to impacts on human health, the C-TAC will likely be a distinct and separate cell, unless it is determined at the time of the incident that combining both cells together would be appropriate.

4. Activation

4.1 At any time, any organisation involved in the response can request the formation of a C-TAC due to the potential impacts of an actual or evolving incident.

4.2 The formation of a C-TAC will be agreed by the SCG following discussion regarding the benefit of the multi-agency cell rather than single agency advice.

4.3 A C-TAC should be activated when there is an expectation that it can add value to the incident response. If the need is unknown at an early stage it is recommended that a cell is activated or on stand-by to avoid delays in advice when required.

4.4 It is likely that the C-TAC, once activated, will take some time to stand-up with all appropriate members. Therefore, immediately following an incident the SCG may be without a coordinated source of technical advice. In this situation, the primary source of advice will be national security agencies such as the NCSC and/or individual agency knowledge who will provide an early assessment of the actual or likely impacts the incident may have on the wider community. This immediate advice may include recommendations to the SCG/RCG on methods of communicating, accessing and sharing information during the response in a secure way to minimise further impacts.

4.5 Taking account of the nature and security requirements of the incident it may be suitable for the C-TAC to be physical instead of virtual. A decision regarding this will be for the SCG/RCG and C-TAC chair to discuss at the time of the incident following advice from the security services.

[18] https://www.jesip.org.uk/home

4.6 Should a physical in person C-TAC be required, adequate and suitable arrangements for the cell should be put in place at the Strategic Co-ordination Centre (SCC) or other suitable location depending on space available and resources.

5. Warning and Informing the public

5.1 As with any major incident, it is important that the public are accurately and regularly warned and informed through traditional methods and social media, of potential risks and actions they can take to keep themselves and any data safe.

5.2 Details of the cyber-attack relevant to the public such as data loss, will be notified by the single agency with responsibility for the loss of this information as specified by the Information Commissioner's Office (See annex A).

5.3 Any media messages regarding the response effort that is being managed by the multi-agency partnership should be dealt with in the normal manner as detailed in LRF emergency response plans. These will include pre-prepared lines in warning and informing plans.

6. Co-ordination between multiple C-TACs

6.1 There should only be one C-TAC per SCG, however each organisation may wish to have a subgroup to discuss their own internal issues, business continuity and recovery of systems.

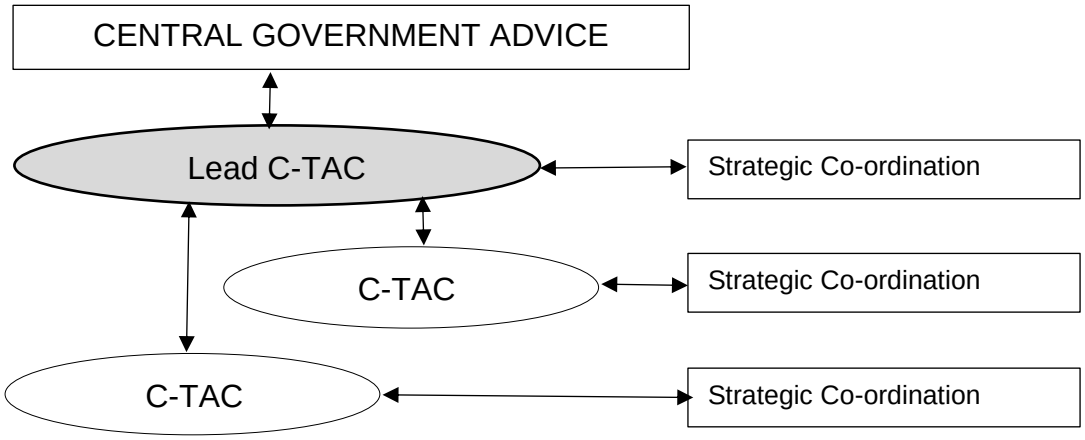
6.2 Where an incident has impacts across one or more LRF areas, including Scotland and Wales, a decision can be made by the affected areas to set up multiple C-TACs or a joint cross-border C-TAC.

6.3 In the event multiple C-TACs are in operation, C-TACs should share data, knowledge and/or advice to help minimise duplication across multiple advisory groups and reduce the potential for conflicting advice arising across multiple response areas.

6.4 C-TAC chairs should agree communication and liaison arrangements, as appropriate to the circumstances, to ensure the advice provided at all levels is coordinated, consistent and meets local needs.

6.5 Where there are multiple C-TACs activated a lead C-TAC (designated by either geographical area or advice specialism) should be identified as early as possible and be communicated to all other sitting C-TACs (see figure 1 below).

FIGURE 1 – Lead C-TAC

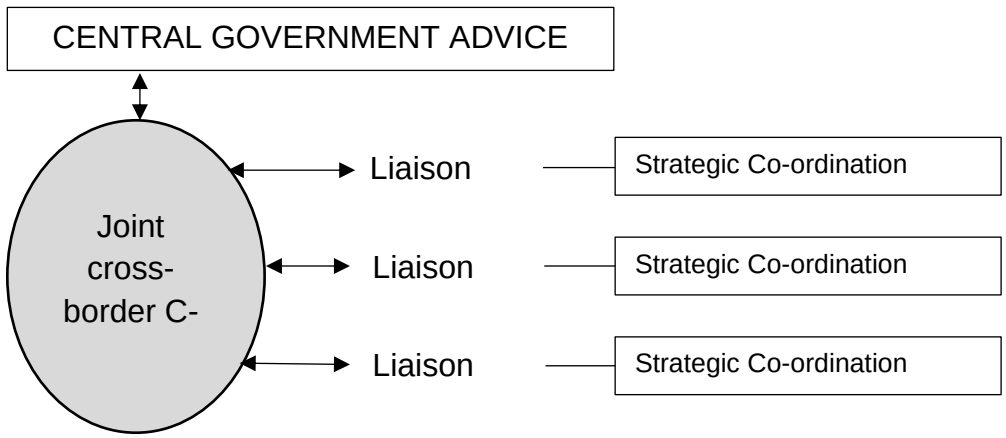


6.6 The intent for a lead C-TAC concept is to provide a mechanism to quickly cascade information from NCSC or central government and help understand wider impacts across multiple areas. It is not intended for the lead C-TAC to co-ordinate the technical response across different areas.

6.7 Where engaged, NCSC and/or law enforcement may feedback any information to the joint cross-border C-TAC or lead C-TAC, who would then be responsible for disseminating this to all parties. This may be useful were there are limited resources and/or time pressures on C-TACs.

6.8 If a decision is made to set up a joint cross-border C-TAC, the joint cross-border C-TAC concept (see figure 2 below) may be useful to help manage technical resources.

FIGURE 2 – Joint cross-border C-TAC



6.9 The chair of the cross-border joint C-TAC may be from the organisation most affected by the incident, however this will be determined at the time considering capability, resources and location.

6.10 Where a joint cross-border C-TAC is activated, each SCG responding may wish to provide a liaison officer for this cell to represent the interest of the local area and feedback to the local strategic group of findings and advice.

7. National Technical Advice through the National Cyber Security Centre

7.1 In the event of a 'significant' cyber incident, the National Cyber Security Centre (NCSC), as the National Technical Authority, is responsible for triaging cyber-incidents, notifying cross-UK incident stakeholders, and co-ordinating the cross-UK response to the cyber elements of the incident to reduce harm to victims.

7.2 This co-ordination may be through an NCSC chaired 'Strategic Leadership Group' (SLG) meeting or through COBR for the most serious national emergencies. The SLG meeting or COBR will allow central government to support the response to an incident and, if required, co-ordinate the central government response.

7.3 A 'significant' incident is one which poses a serious risk to the ongoing operation of an operation or to its customers. This could include attacks which disrupt the provision of essential services to the public, or which result in a significant loss of key data such as sensitive information or intellectual property.

7.4 The NCSC is responsible for the technical response to the incident but not for the management of consequences or impacts, especially at a local level. The management of consequences at a national level is the responsibility of the lead government department (LGD) for the affected sector. It will be the responsibility of the LGD to stand up its crisis response mechanism to manage co-ordination at the national level if this is appropriate. In the most serious cases the Cabinet Office may decide to active COBR as for other types of incident.

7.5 The C-TAC is designed to facilitate communications up to national structures, down to individual organisations and across to the multi-agency partnership.

7.6 Links to the national consequence management structures, including COBR, will be provided by MHCLG RED as for any other major emergency.

8. Deactivation

8.1 A proposed closure of the C-TAC should be recommended to the SCG/RCG when there is considered no longer issues for the cell to consider.

8.2 The decision to stand down the C-TAC will be taken by the C-TAC Chair in consultation with the SCG/RCG.

8.3 All organisations involved in the delivery of C-TAC for the incident will be invited to participate in a structured debriefing process. This will be led by the organisation providing the chairperson for the C-TAC.

8.4 A final report for C-TAC containing all of the relevant identified lessons will be produced and form part of the overall incident report to the respective LRF which will inform C-TAC planning as part of the planning cycle.

8.5 When the C-TAC is deactivated all notes and records of decisions should be kept with all other record logs relating to the incident, in line with normal emergency response procedures.

Annex A
Specialist agencies providing technical advice in an emergency with a cyber element

AGENCY	RESPONSIBILITY
The National Cyber Security Centre (NCSC)	UK's technical authority on cyber security. Its main purpose is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. It works with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management, underpinned by world class research and innovation. The NCSC identifies and responds to incidents which might impact the UK's national security or economic wellbeing, and/or which have the potential to cause major impact to the continued operation of an organisation. In the event of significant cyber security incidents, it provides direct technical support and cross government coordination of response activities. To report a cyber security incident: www.ncsc.gov.uk/report-an-incident (monitored 24hrs)
The National Cyber Crime Unit (NCCU)	The National Cyber Crime Unit (NCCU), part of the National Crime Agency, is the UK's lead for tackling the threat from serious and organised cybercrime. The NCCU leads, supports and coordinates cyber law enforcement activity across the UK, working with partners to provide specialist cyber support and expertise across law enforcement. It works closely with NCSC, Regional Cyber Crime Units, and Police Forces to build an effective cyber response across the UK. https://www.cybersecurityintelligence.com/national-cyber-crime-unit-nccu-1267.html
Action Fraud	Action Fraud is the UK's national fraud and cyber-crime reporting centre for England, Wales and Northern Ireland, providing a central point of contact for citizens and businesses. The National Fraud Intelligence Bureau (NFIB), also hosted by the City of London Police (CoLP), acts upon the information and crimes reported to Action Fraud, developing and disseminating crime packages for investigation locally, regionally and nationally, and executing a range of disruption and crime prevention techniques for victims across all sectors to target criminality and engineer out the threat from fraud and cyber-crime. https://www.actionfraud.police.uk/
Cyber Security Information Sharing Partnership (CiSP)	CiSP is a secure joint industry and Government initiative for exchanging cyber-threat information. Membership provides organisations with vital threat information and information on ongoing incidents. www.ncsc.gov.uk/cisp
Information Commissioners Office (ICO)	Legislative responsibilities in relation to the security of data held by an organisation are covered under the General Data Protection Regulation (in force from 25th May, 2018). There is no legal obligation on data controllers to report breaches of security; however the ICO encourages serious security breaches to be reported to them. Loss of personal information or sensitive data must be reported to the ICO by the organisation holding the data. The ICO operate a helpline during week day office hours on **0303-123-1113**. https://ico.org.uk/
Warning, Advice and Reporting Point (WARP)	A service where members can receive and share up-to-date advice on information security threats, incidents and solutions. WARPs have been set up generally on a regional basis, primarily but not exclusively with membership from local authorities. The nominated lead for each WARP provides security warnings and advice to the members via email, a website and/or meetings.

Annex B

Reference material

The NIS Regulations 2018

The Security of Network & Information Systems Regulations (NIS Regulations) provide legal measures aimed at boosting the overall level of security (both cyber and physical resilience) of network and information systems for the provision of essential services and digital services.
https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

Competent Authorities

The NIS Regulations establish multiple competent authorities which are responsible for the oversight and enforcement of the NIS Regulations.

What denotes a competent authority and their requirements can be found at
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701050/NIS_-_Guidance_for_Competent_Authorities.pdf

Annex C
Joint Emergency Services Interoperability Principles (JESIP) Joint Decision Model (JDM)

THE FIVE PRINCIPLES

Co-locate

Co-locate with commanders as soon as practicably possible at a single, safe and easily identified location near to the scene.

Communicate

Communicate clearly using plain English

Co-ordinate

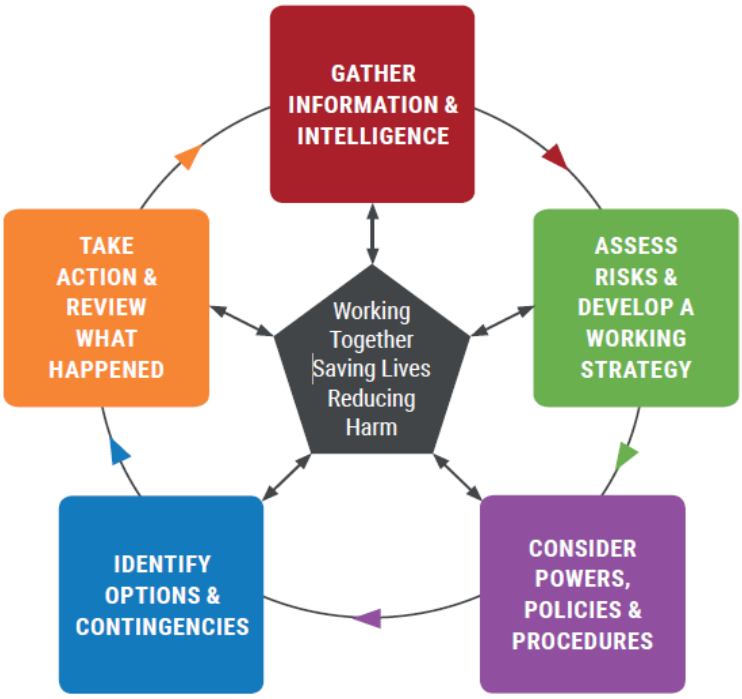
Co-ordinate by agreeing the lead service. Identify priorities, resources and capabilities for an effective response, including the timing of further meetings

Jointly understand risk

Jointly understand risk by sharing information about the likelihood and potential impact of threats and hazards to agree potential control measures

Shared Situational Awareness

Shared Situational Awareness established by using METHANE and the Joint Decision Model



ST GEORGE'S HOUSE

WINDSOR CASTLE
HONI·SOIT·QUI·MAL·Y·PENSE
COLLEGE OF ST GEORGE

For more information about
Consultations at St George's House
visit www.stgeorgeshouse.org

St George's House, Windsor Castle, Windsor SL4 1NJ

T +44 (0)1753 848848 E house@stgeorgeshouse.org F +44 (0)1753 848849