STRATEGY – understanding the issues and why digital and cyber resilience is central to operational effectiveness and efficiency

DESIGN PRINCIPLES

- Develop a strategic overview why digital and cyber resilience matters
- Understanding the local dimension and need for organisation wide awareness
- Know the key security measures and skills required
- Prioritise partnership and collaboration

STRATEGY		
DOCUMENTATION		
Name	Link	Description
Understanding Local Cyber Resilience	Here	This paper, commissioned by the Department for Communities and Local Government and prepared in collaboration with the Cabinet Office, outlines the key cyber resilience threat to Local Government. This is a persistent threat that, if left unchecked, could disrupt the day- to -day operations of councils, the delivery of local public services and ultimately has the potential to compromise national security.
The National Security Strategy	Here	The National Security Strategy and Strategic Defence and Security Review 2015 sets out the government's approach to national security.
The UK Cyber Security Strategy	Here	The Cyber Security section of Gov.UK sets out how the UK will support economic prosperity, protect national security and safeguard the public's way of life by building a more trusted and resilient digital environment.
Cyber Incident Response (CIR) service	Here	When an organisation has been attacked its most immediate concerns are likely to be: What action needs to be taken? Who has the proven knowledge and experience required to contain and eradicate the incident? Drawing on the experiences of a CESG/CPNI drawing on the experiences of a CESG/CPNI pilot, there is a twin track approach for the provision of certified Cyber Incident Response services

CESG Advice and Guidance at a Glance	**Here**	**Background briefing collections from CESG covering Cyber Security, and related good practice.**
INFORMATION SECURITY BREACHES SURVEY 2015 | technical report	**Here**	**This is the latest of the series of Information Security Breaches Surveys, carried out since the early 1990s. PwC carried out the survey, analysed the results and produced the report; Info Security Europe assisted with marketing the survey.**
Cyber primer	**Here**	**Introduction to the subject of Cyber primer is divided into 2 parts. Part 1 explores the boundaries of cyber and cyberspace and introduces the terms and definitions that are used. Part 2 references several examples from media reports of alleged use by individuals and extremist groups to foreign military allegedly using cyber to their advantage.**
Cyber security: advice for small businesses	**Here**	**This guidance explains the threat from cyber-attack and shows how you can protect your business. It includes advice on: using strong passwords ; updating software ; providing simple staff awareness and training ; managing risk ; using the Cyber Essentials scheme to protect against common online threats. The advice will help you to protect your: ; business information ; cash flow ; customers ; reputation**
Good practice and technical guidance catalogue	**Here**	**This is a catalogue of cyber and cyber related guidance that has been produced by CPNI. The guidance is sorted alphabetically with all guidance older than 2010 filed under the archive tab at the bottom**