SECURITY – highlighting the key steps and controls to ensure that public bodies are cyber resilient

DESIGN PRINCIPLES

- Adopt the key security steps, controls and processes
- Understand how to reduce the impact of attacks
- Establish strong incident reporting and response processes
- Access and use security policy frameworks and standards

Think Cyber Think Resilience

SECURITY		
DOCUMENTATION		
Name	Link	Description
Cyber Security	Here	Gov.uk main post
10 Steps to Cyber Security: Advice Sheets	Here	The actions and measures detailed in each of these advice sheets collectively represents a good foundation for effective information risk management. The degree of implementation of each step will vary between organisations depending upon the risks to their individual business. However, GCHQ's recommendation is that Boards should require their CIO and CISO to be able to articulate why a particular measure is not applicable. This document is part of the 10 steps to cyber security document set.
CESG Advice and Guidance at a Glance	Here	Background briefing collections from CESG covering Cyber Security, and related good practice.
CESG Security Operations & Management	Here	Exploring what security operations and management is, and how it can help organisations.
Critical Security Controls guidance	Here	The Critical Security Controls for cyber defence are a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence. CPNI is participating in an international government-industry effort to promote the Critical Security Controls for computer and network security.
CPNI – Passport to Good Security	Here	CPNI has produced the Passport to Good Security for Senior Executives. It sets out strategic headlines for best practice and provides relevant prompts for the actions you need to take as part of your strategy. It will help you to identify, assess and mitigate the threats to your organisation.

Cyber Street Wise	**Here**	**Be Cyber Streetwise is a cross-government campaign, funded by the National Cyber Security Programme, and delivered in partnership with the private and voluntary sectors. The campaign is led by the Home Office, working closely with the Department for Business, Innovation and Skills and the Cabinet Office. We aim to measurably and significantly improve the online safety behaviour and confidence of consumers and small businesses (SMEs).**
Cyber-security Information Sharing Partnership (CiSP)	**Here**	**A joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.**
Common Cyber Attacks: Reducing The Impact	**Here**	**Common Cyber Attacks: Reducing The Impact has been produced by CESG (the Information Security Arm of GCHQ) with CERT-UK,and is aimed at all organisations who are vulnerable to attack from the Internet. The paper helps CEOs, boards, business owners and managers to understand what a common cyber attack looks like.**
Security policy framework	**Here**	**The security policy framework describes the standards, best-practice guidelines and approaches that are required to protect UK government assets (people, information and infrastructure). It focuses on the outcomes that are required to achieve a proportionate and risk-managed approach to security that enables government business to function effectively, safely and securely.**
Cyber security guidance for business	**Here**	**Advice from security and intelligence experts across government about how to prevent the majority of cyber (information technology) attacks, and how to manage common cyber risk. This guidance has been updated to include the document 'Common Cyber Attacks' which sets out what a common cyber attack looks like and how attackers typically execute them.**
Security for Industrial Control Systems	**Here**	**This good practice guide is primarily intended for those who are directly responsible for securing ICS, whether they are looking to establish a new programme or complement one that already exists. It will assist ICS professionals in improving their knowledge of security as well providing IT professionals with insight into the ICS environment. Senior leaders in an organisation will be informed about the rationale for establishing an ICS security capability and the potential activities involved in securing assets.**
BCS: Security Top Tips	**Here**	**Basic security guidance from the British Computer Society**

Cyber security and fraud: The impact on small businesses	**Here**	**The FSB is pleased to partner with BIS and the Home Office to bring you this report looking at the issues of fraud and online crime based on research and evidence from our 6,500 strong survey panel, including ways of tackling the problem. The risk of fraud and online crime, both real and perceived, and the serious costs that can be involved are a clear barrier to growth for small businesses, costing each business up to £4,000 per year 1. The recently published BIS guidance 'Small businesses: what you need to know about cyber security' sits alongside our simple Top 10 Tips to cyber security giving accessible and straightforward advice to small businesses, without the jargon**
UK cyber security standards research	**Here**	**The standards landscape for cyber security is highly complex with various government and industry-led standards and schemes in existence, developing domestically and internationally. This report provides a clearer understanding of this landscape, and the current and potential uptake of standards. This information will assist government with identifying and developing evidence-based policies to close the gaps in the landscape. It will also support industry uptake of good standards for cyber security products and services.**
Action Fraud	**Here**	**We provide a central point of contact for information about fraud and financially motivated internet crime.**
The Information Security Breaches Survey 2015	**Here**	**The average cost of the most severe online security breaches for big business now starts at £1.46 million – up from £600,000 in 2014, according to government research published today (2 June 2015) to raise awareness of the growing cyber threat.**