• TAKE THE LEAD
• BE A STRONG PARTNER
• BE SECURE
• BE INFORMED

• AWARENESS
• RESPONSE
• INFORMATION
• INFRASTRUCTURE
Cyber Resilience is the capacity to prevent, identify and mitigate any impact that cyber incidents have on the information your organisation requires to do business and deliver public services.

Think Cyber Think Resilience
Its the leaders job to see cyber resilience as first and foremost as a people issue and proactively create a strong cyber-aware culture so it is seen as everyone's responsibility across the organisation.

Think Cyber Think Resilience
Recognising that **100% risk mitigation is not possible** in any complex system, the overarching goal of a risk-based approach to cyber security is system resilience to survive and quickly recover from attacks and accidents.

*Partnering for Cyber Resilience*

*Then world Economic Forum*

*January 2013*
Growing Public Service Cyber Domain

Think Cyber Think Resilience
Cyber Resilience Threat Landscape

Deliberate;
- Foreign Intelligence Services
- Organised Criminals
- Investigative Journalists
- Hacktivists
- Social Media - includes social groups
- Insider threats
  - Disgruntled staff
  - Ex-Staff
  - Staff under duress

Damage to reputation /Trust

Cyber has been identified as one of the four tier one threats to UK security

Think Cyber Think Resilience
- Set overall expectations on institutional risk appetite
- Reinforce behaviour changes in senior management team (e.g. how to handle sensitive business material)
- Ensure appropriate funding.

Adapted from “Beyond Cybersecurity: Protecting Your Digital Business” Wiley
- Give input for prioritising information assets and making trade-offs between data protection and operational impact
- Incorporate cybersecurity considerations into services, customer and location decisions.
- Communicate need for behavioural change at the frontline
- Backup security team in enforcing important policies

Adapted from “Beyond Cybersecurity: Protecting Your Digital Business” Wiley
- Synchronize cybersecurity strategy with corporate policies (e.g. HR, procurement, etc.)
- Integrate cybersecurity into quality/compliance programmes.
- Incorporate cybersecurity into regulatory and public affairs agenda

Adapted from “Beyond Cybersecurity: Protecting Your Digital Business” Wiley
- Ensure enterprise risk methodology accommodates idiosyncrasies of cybersecurity risks
- Incorporate prioritised cybersecurity risks into enterprise risk report
- In some cases, provide governance and oversight for cybersecurity function.

Adapted from “Beyond Cybersecurity: Protecting Your Digital Business” Wiley
- Ensure cybersecurity programme supports institution’s risk appetite and that business strategy is in place and on plan
- Drive required changes across IT organisation
- Conduct effective dialogue with the board.

Adapted from “Beyond Cybersecurity: Protecting Your Digital Business” Wiley
Take the Lead

Guidance

Understanding local cyber resilience: a guide for local government on cyber threats

From: Department for Communities and Local Government and Cabinet Office
First published: 24 March 2015
Part of: Local council transparency and accountability and Council Tax reform
Applies to: England

A short guide for local government on cyber threats and how to mitigate them.

Document

Understanding local cyber resilience: a guide for local government on cyber threats and how to mitigate them
PDF, 511KB, 15 pages

This file may not be suitable for users of assistive technology. Request a different format.

Think Cyber Think Resilience
Be a strong partner

Cyber-security Information Sharing Partnership

Think Cyber Think Resilience
Be Secure

10 Steps To Cyber Security

Defining and communicating your Board’s Information Risk Management Regime is central to your organisation’s overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

- **Network Security**: Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

- **Malware Protection**: Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

- **Monitoring**: Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

- **Incident Management**: Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

- **Establish an effective governance structure and determine your risk appetite.**

- **Establishing the Board’s engagement with the cyber risk.**

- **Produce supporting information risk management policies.**

- **User Education and Awareness**: Produce user security policies covering acceptable and secure use of the organisation’s systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

- **Home and Mobile Working**: Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

- **Secure Configuration**: Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

- **Removable Media Controls**: Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

- **Managing User Privileges**: Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Think Cyber Think Resilience
Be informed – Think Cyber Think Resilience

**Awareness**

**CESG** - the information security arm of GCHQ and national technical authority for information assurance in the UK about the **10 Steps to Cyber Security** all organisations need to take.

**Response**

**CERT-UK** - the UK national computer emergency response team, which manages the Cyber-security Information Sharing Partnership (CiSP).

**Information**

**The National Archives** - whose role includes providing advice and guidance to public sector bodies on information management including information assurance and cyber security training.

**Infrastructure**

**Government Digital Service** - which administers the Public Services Network (PSN) and develops other elements of the Government infrastructure.

All organisations need to take steps to Cyber Security.
KEY STEPS TO SUCCESSFUL LOCAL CYBER RESILIENCE

STEP 1: Embed a People Centred culture

STEP 2: Be aware of the threats & opportunities

STEP 3: Decide what matters

STEP 4: Monitor and manage

Think Cyber Think Resilience
Cyber resilience is first and foremost a people issue and leaders need to proactively creating a strong cyber-aware culture so it is seen as everyone's responsibility across the organisation.

- Remember Cyber Resilience is a people centred issues
- Keep people involved and informed
- Provide regular training and awareness sessions
- Develop a culture of cyber awareness both within and beyond your organisation

Think Cyber Think Resilience
STEP 2: Be aware of the threats and opportunities

The players:
- Criminals
- Hackers and Hacktivists
- Spies & Espionage
- Warfare
- The innocents

The attacks:
- Phishing
- Trojan Horses
- Hacking
- Stealing
- Sabotage
- Mistakes

Think Cyber Think Resilience
STEP 3: Decide what matters

Know your key information assets
- Information
- Technology
- Processes
- People
- Infrastructure
- Reputation

- Decide which information assets are businesses critical
- Decide on a the level of risk that is acceptable – the risk appetite
- Agree and plan a proportionate response

Think Cyber Think Resilience
STEP 4: Monitor and manage

- Lead from the top
- Get the right Management Information
- Manage the risks
- Support the SIRO & Information Asset Owners
- Cyber Resilience Culture

Think Cyber Think Resilience
Civic Cyber Resilience – 5 key themes

Civic Cyber Resilience Model

Leadership & Partnership

Information & Infrastructure

Transformation & Community Resilience

Business Continuity, Civil Contingencies & Risk Management

Strategy, Security & Skills

Think Cyber Think Resilience
STRATEGY, SECURITY & SKILLS - helping to understanding the bigger picture and how stronger cyber security and skills are essential to building and maintaining organisational resilience.

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

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

**SKILLS** – gaining the essentials skills that people and organisations need to have in place to be cyber resilient

Think Cyber Think Resilience
LEADERSHIP & PARTNERSHIPS – helping to understand the role of local leaders and how local resilience forums and their partners should work together to address cyber threats.

LEADERSHIP – understanding what leaders need to know and how they need to place cyber awareness at the heart of organisational resilience

PARTNERSHIP – recognising that cyber resilience is about building strong partnerships both within and across organisational boundaries

Think Cyber Think Resilience
INFORMATION & INFRASTRUCTURE - having the right Information Assurance/Information Governance and underpinning secure Infrastructures in place to support cyber resilience.

INFORMATION – ensuring that cyber resilience is underpinned by strong and effective information assurance and information governance

INFRASTRUCTURE – ensuring the management and operational systems are focussed on the maintenance of cyber resilient infrastructure

Think Cyber Think Resilience
BUSINESS CONTINUITY, CIVIL CONTINGENCY & RISK MANAGEMENT - being aware of the challenges to business continuity and risk management and how this relates to Local Authorities responsibilities under the Civil Contingencies Act for advice and guidance to local communities and businesses.

BUSINESS CONTINUITY – ensuring that internal Business Continuity Arrangements are focussed on identifying and combatting cyber vulnerabilities and challenges

CIVIL CONTINGENCIES – understanding Local Authorities role under the Civil Contingencies Act to provide advice and guidance to local businesses and communities around cyber resilience

RISK MANAGEMENT – meeting the challenge of the consequences of a cyber-attack on organisations and understand how they would recover

Think Cyber Think Resilience
TRANSFORMATION & COMMUNITY RESILIENCE - having an appreciation of how good Cyber security can underpin Digital Transformation and supporting wider Community Resilience.

TRANSFORMATION – understanding how effective cyber security and resilience is essential to underpin service transformation and digital delivery

COMMUNITY RESILIENCE – recognising that good cyber resilience an essential precondition for resilient communities and cities

Think Cyber Think Resilience
Civic Cyber Resilience Knowledge Bank

The follow the building blocks will help you to create a **people focussed culture** that sees cyber resilience as first and foremost as a people issue and proactively creating a strong cyber-aware culture so it is seen as everyone's responsibility across the organisation.

- **Strategy**
- **Skills**
- **Security**
- **Leadership**
- **Partnership**
- **Information**
- **Infrastructure**
- **Business Continuity**
- **Civil Contingencies**
- **Risk Management**
- **Transformation**
- **Community Resilience**

Think Cyber Think Resilience
Civic Cyber Resilience Knowledge Bank

The following building blocks will help you to create a people-focused culture that sees cyber resilience as first and foremost as a people issue and proactively creating a strong cyber-aware culture so it is seen as everyone’s responsibility across the organisation.

**Civic Cyber Resilience Knowledge Bank**

- **Strategy**
- **Skills**
- **Security**
- **Leadership**
- **Partnership**
- **Information**
- **Infrastructure**
- **Business Continuity**
- **Civil Contingencies**
- **Risk Management**
- **Transformation**
- **Community Resilience**

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

- 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

**Design Principles**

**Transforming Local Cyber Resilience**

**Knowledge Bank**

**Key Reads**

Think Cyber Think Resilience
Sign-up with Resilience Direct and join the Civic Cyber Resilience Working Group

- Information sharing
- Increasing service adoption
- Mapping
- ResilienceDirect Hub
- Think Cyber Think Resilience Events outputs

www.resilience.gov.uk

Think Cyber Think Resilience
Next steps you can take in partnership with others

- Join the Cyber Security Information Sharing Platform (CiSP)
- Link-up with CiSP LG Node and help crowd source the Cyber Knowledge Base
- Sign-up with Resilience Direct and join the Civic Cyber Resilience Working Group

Think Cyber Think Resilience
Think Cyber Think Resilience