• Role of the “Architectural Team”
• The Foundations
• Building Blocks & Design Principles
• Linking-up with Civic Cyber Resilience Knowledge Bank
“Architectural Team” – Chief Executives

- 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
“Architectural Team” – Enabling function executives (e.g. Finance, HR, etc)

- 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
The foundations to successful local cyber resilience

1: Embed a People Centred culture

2: Be aware of the threats & opportunities

3: Decide what matters

4: Monitor and manage

Transforming Local Cyber Resilience
1: Embed a People Centred culture

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
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
Transforming Local Cyber Resilience

3: Decide what matters

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

- Decide which information assets are businesses critical
- Decide on the level of risk that is acceptable – the risk appetite
- Agree and plan a proportionate response
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
The following building blocks and design principle are intended to 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.

- Strategy
- Skills
- Security
- Leadership
- Partnership
- Information
- Infrastructure
- Business Continuity
- Civil Contingencies
- Risk Management
- Transformation
- Community Resilience
STRATEGY – understanding the issues and why digital and cyber resilience is central to operational effectiveness and efficiency

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

- Access and use the Cyber Essentials and skills guides
- Use CESG approved training
- Support SIRO and Information Assurance Guidance training
- Provide access to Massive Open Online Courses and other online resources
LEADERSHIP – understanding what leaders need to know and how they need to place cyber awareness at the heart of organisational resilience

- Place the issue at the heart of corporate business – not just an IT issue
- Understand the key role of SIRO and wider Governance implications
- Ensure Board level leadership accesses the right help and advice
- Know and use the key questions Leaders need to ask
PARTNERSHIP – recognising that cyber resilience is about building strong partnerships both within and across organisational boundaries

- Join the Cyber Security Information Sharing Partnership
- Work with WARPS and Local Resilience Forums
- Adopt boundary spanning approaches and learning across other sectors
- Develop and share “what works” Case Studies
INFORMATION – ensuring that cyber resilience is underpinned by strong and effective information assurance and information governance

• Have a robust Information Assurance policy
• Ensure you have effective training for both leaders and staff
• Regularly access and use published Data Handling guidance
• Develop a culture of trust, both within and beyond your organisation
INFRASTRUCTURE – ensuring the management and operational systems are focussed on the maintenance of cyber resilient infrastructure

- Adopt secure networks and robust connectivity
- Work towards adopting common platforms and standards
- Use assured products and technologies
- Support resilient infrastructure for communities and businesses
BUSINESS CONTINUITY – ensuring that internal Business Continuity Arrangements are focussed on identifying and combatting cyber vulnerabilities and challenges

• Use the Business Continuity Management Toolkit
• Understand the Local perspective
• Undertake regular Cyber Security Planning
• Maintain Incident Response and supervisory control systems through out your organisation
CIVIL CONTINGENCIES – understanding Local Authorities role under the Civil Contingencies Act to provide advice and guidance to local businesses and communities around cyber resilience

- Monitor Civil Contingencies Act compliance
- Work with the wider Civil Contingencies community both central and local
- Partner with Local Resilience Forums and use Resilience Direct
- Focus on supporting Communities and Business that may be impacted by cyber attacks

Transforming Local Cyber Resilience
RISK MANAGEMENT – understanding the organisational risk appetite so as to help manage the risks and consequences of a cyber-attack and understand how organisations need to plan as to how to recover from an major incident

- Understand how risk assessment processes can help
- Learn how to define your organisation's risk appetite
- Identify the Cyber risk management issues for your locality
- Understand how to tackle Cyber Risks and reduce their impact
TRANSFORMATION – understanding how effective cyber security and resilience is essential to underpin service transformation and digital delivery

- Keep in touch with the wider Public Service Transformation agenda
- Understand the changing role of data sharing and strong analytics
- Adopt common design standards based on User Centric Focused Delivery
- Understand how digital platforms and approaches can support wider change
COMMUNITY RESILIENCE – recognising that good cyber resilience an essential precondition for resilient communities and cities

- Champion whole place approaches to building resilient communities and businesses
- Actively contribute to the creation of resilient Infrastructure and Communication systems
- Understand how focussed leadership and innovation can help to create resilient communities
- Foster collaborative working and networked learning
Civic Cyber Resilience Knowledge Bank hosted on Resilience Direct

**Civic Cyber Resilience Building Blocks**

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

**Transforming Local Cyber 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**

**Knowledge Bank**

**Key Reads**

Transforming Local Cyber Resilience
Resilience Direct and Civic Cyber Resilience Working Group

Resilience Direct

- Information sharing
- Civic Cyber Resilience Knowledge Bank
- Think Cyber Think Resilience Events outputs

Transforming Local Cyber Resilience
Building a Civic Cyber Resilient Organisation

WORK IN PROGRESS

Transforming Local Cyber Resilience