Observatory of Public Sector Innovation

OECD BETTER POLICIES FOR BETTER LIVES

Horizon 2020 European Union Funding for Research & Innovation

"Think Cyber – Think Resilience" Local Leadership in Cyber Society Initiative

Published On: 03 April 2017

Organisation: Department for Communities and Local Government

Country: United Kingdom

Level of government: Central government

Sector: Defence, General public services

Type: Communication, Digital, Methods, Partnerships, Public Service

Launched in: 2015

Overall development time: 1 year(s)

Link to the innovation's website

Description

The Think Cyber – Think Resilience” Local Leadership in Cyber Society Initiative is a unique collaboration involving central government, local authorities, academia and specialist bodies focusing on raising awareness about cyber resilience and related issues with the intention of building strong local leadership
culture and common understanding of civic cyber resilience.

Why the innovation was developed

- Recognition of growing threat to individuals, local communities, businesses and public service providers requires a new approach to local civic cyber resilience based on collaborative horizon scanning of both existing resources and gap analysis (ensuring that individual localities are not forced to reinvent the wheel by duplicating or re-purposing current solutions)

Objectives

Develop staff capacity, Enhance public trust, Improve efficiency, Improve service quality

Main beneficiaries

Civil Society, General population, Government bodies, Government staff, Students

Results

Efficiency

- The programme outputs rationalised an array of official briefing and guidance material to provide a single-point of access on civic cyber resilience for policy makers and practitioners across local public sector bodies.

Effectiveness

- The programme provided immersion training and resources for over 700 key local leaders so that they could embed leading edge best practice on cyber security and resilience across their localities.

Service quality

Responsiveness:

- The programme championed the closer networking of local cyber resilience teams with peers and the HMG sponsored Cyber Information Sharing Partnership.
- A key case study (Lincolnshire County Council) was the way in which this collaboration help developed a model approach to ransom ware incidents based on the sharing of a real time local case study.

Other improvements

- As a result of the programme Local Government is now establishing a new local public sector collaborative bodies (e.g. cyber stakeholder and technical security sounding boards) to engage with central government, academia, or other interested bodies and act as leaders for local digital transformation and civic cyber resilience

Development

Design

Developed by Department for Communities and Local Government and INetwork (via IStandUK the Local eGovernment Standards Body) as part of the UK Government National Cyber Security Programme. The design process encompassed a detailed Horizon Scan of risks/issues, guidance and stakeholders DCLG working in partnership with the local government bodies (LGA/SOLACE/SOCITM), to commission crosssector horizon scanning activities and host consultation events to help the National Cyber Security Programme to develop of products, services and solutions aimed at helping local government.Design time: 3 month(s)

Testing

- Capacity consultation workshops with national LG bodies and local resilience forums in conjunction with Cabinet Office (and the Oxford University Martin School (Global Cyber Security Capacity Centre) to establish base line on local sector capabilities.
- Drafting and Testing Local Cyber Storyboard and “Think Cyber ThinkResilience” model and testing it as part of Cyber briefing seminars 700 senior regional leaders and practitioners.
- Senior Leaders Open Policy Consultation on the development of a Civic Cyber Resilience model and help inform the LG with the National Cyber Security Strategy.

Testing time: 3 month(s)

Implementation

Tools used:

- Via 6 regional briefing seminars for local authority executives/managers and resilience leaders – delivering immersion briefings for up to 700 local leaders between October 15 and March 16.
- Publishing the Civic Resilience model and profiling it as part of the CyberUK16 UK Government Cyber Security and Policy Showcase May 2016 .

Resources used:

- Joint resource team from DCLG/INetworkwith budget of £575,000 GBP

Implementation time: 6 month(s)

Challenges and solutions

- The biggest challenge was the cultural differences between the key stakeholder groups – central government bodies, local governance, and academic bodies.
- DCLG programme played the role of ‘honest broker’ bringing all the parties to the table and helping each of them to understand each other’s viewpoint. As each group of stakeholders became more engaged and more aware of the concern of others, so they became more willing to take part – leading to breakthrough proposal to engage locally with the target audience
- Users were asked to review the ideas and thoughts of the project team. Wider consultation and testing took place on early drafts of the model.
- On the road show events, a wide range of communication activity took place – including using social media which continued throughout the regional events and afterwards.

Partnerships

Various partners
Academics and Research Bodies, Civil Society

INetwork (via IStandUK the Local eGovernment Standards Body) Cabinet Office Office of Cyber Security and Information Assurance CERTUK – the UK National Computer Emergency Response Team
and coordinators of Cyber Security Information Sharing Partnership GDS – Public Services Network (PSN) National Archives
LGA/SOLACE/SOCITM and NLAWARP Corporation of the City of London, City of London Police and Gloucestershire Constabulary Regional Cyber Crime Units (RCCU) Oxford University Martin School (Global Cyber Security Capacity Centre)

Civil Society, Academic & Research Bodies, Public Sector – partners helped in the initial design of the civic cyber model ensuring existing material was taken into account, new research or latest developments were fully understood and all parts of the model were relevant (or adapted to be more relevant). Their continued support helped to test the model and with the involvement of local government sector bodies begin the process of two-way

engagement.
Critical to the success of the programme were the series of regional events and the attendance of partners to engage directly with local leaders. The whole process was constantly iterative – learning together, refining the model, delivering at events, and adapting material as events progressed and new learning emerged – for nearly all of the partners, the presentations changed as a result of the iterative process.

Lessons Learned

Lessons Learned

- There are real cultural differences between different sectors these impact on expectations, timings and processes so be patient
- Be consistent about what you want to achieve but flexible about how to achieve objectives and (where possible) on timescales

Conditions for success

- Early engagement of key stakeholders is critical but be prepared to work with the willing while informing or educating the less engaged stakeholders
- Be open about objectives and what can or cannot be achieved within existing timescales and budgets – make sure everyone agrees priorities • Never assume you have all the answers nor that testing has identified all the issues – be prepared to reiterate and learn as you develop

Other information

Given the political context, understand the scope of the project and set boundaries to avoid scope creep (e.g. for this project health services were excluded as they were covered by a separate project but a key issue from the local perspective is the interrelationship between health and social care).

We live in an increasingly interconnected world and cyber threats know no boundaries but all too often cyber resilience is left national governments' or big business. The innovative approach taken by the Local Leadership in Cyber Society programme is the creation of a common "Think Cyber – Think Resilience" model that can be adapted and used for engaging with the wider public sector (and beyond) within regions (or smaller localities) to help increase awareness of the issues and develop local resilience.