Post PSN Compliance for Local government?

Mark Brett

Programme Director NLAWARP / C-TAG

NLAWARP

Issue

The PSN Code of Connection Compliance regime has become a proxy for Assurance. The Code of Connection was never meant to be an Assurance regime.

HMG Departments are now assessed against a Cabinet Office compliance Framework.

The NHS and Policing have their own national support teams, Local government does not.

To prevent a roll back to beyond 10 years ago, how can we agree an approach that HMG Depts, Police and NHS will accept from Local government to permit the sharing of their data?

NOT a Solution, an approach for discussion

We have developed a strawman approach, which hopefully reflects the learning across this space over the last ten years and many conversations had at this gathering over the years.

The Key questions;

- 1) Does it cover the bases?
- 2) Is there anything missing?
- 3) What are the key blockers to adopting a single approach?
- 4) Who should lead on this work?

Post PSN Assurance Process (P2AP) Approach **Part 1 Scope**

1) IASME Cyber Essentials Plus as a minimum covering.

1.1 The Corporate ICT Core Network

1.2 The Social Care systems

1.3 The Corporate CRM System

1.4 The Corporate websites

1.5 Corporate email

1.6 remote network access services (VPN)

1.7 Wireless network access

1.8 BYOD

1.9 Remote working

Post PSN Assurance Process (P2AP) Approach **Part 2 Technical Requirements**

2.1) Adherence to and reporting on the Minimum Cyber Security Standard [8]

2.2) Adherence to and reporting on NCSC legacy guidelines: https://www.gov.uk/guidance/managing-legacy-technology

2.3) Monthly internal vulnerability scans of the core network and servers.

2.6) Monthly scanning and reporting of all digital certificates in use.

2.7) Monthly scanning and health checking DNS Records.

Post PSN Assurance Process (P2AP) Approach **Part 3 Technical Requirements**

3.1) Have suitable Information Governance, training and awareness regime in place.

3.2) SIRO / IAOs DPO appointed, Corporate IG Board in Place,

3.3) Adherence to Local Public Services Data Handling Guidelines. (V6)

Post PSN Assurance Process (P2AP) Approach **Part 4 Holistic requirements**

- 3) Deployment, reporting and active use of NCSC Active Cyber Defence 3.1Webcheck
- 3.2Mailcheck
- 3.3 PDNS (or acceptable alternative if not technically possible).
- 3.4 NEWS Network Early Warning Service
- 3.5 Logging Made Easy (or Acceptable alternative)
- 3.6 Have an NCSC point of contact (POC) email box in place.
- 3.7 Have an active NCSC CISP account.
- 3.8 Member of Regional WARP

Post PSN Assurance Process (P2AP) Approach **Part 4 Resilience Requirements**

4.1) Have carried out a Cyber Incident exercise within the last twelve months.

4.5) Documented Cyber Incident Response process and plan in place. 4.6) Key data backup / isolation processes in place.

Discussion

Mark Brett

Programme Director NLAWARP / C-TAG

mark.brett@nlawarp.net

NLAWARP