Progress of the 2016-2021 National Cyber Security Programme
National Audit Office (NAO) Progress Report – 15th March 2019

Is it time for Health and Social Care to be taking Cyber-Security more seriously?

The National Cyber Security Strategy's vision is that "the UK is secure and resilient to cyber threats, prosperous and confident in the digital world".

The recently published progress report by the NAO has profound implications, and the impact on the Health and Care sectors could be significant.

Cyber Security is a major challenge for government. The risk of cyber-attack is increasing and the UK, with one of the world's most internet-enabled economies is more vulnerable than most to the threat from hostile countries, criminal gangs and individuals. With over 4 in 10 businesses experiencing a cyber security breach or attack in the last 12 months**

In its Report, the NAO concludes that the Programme's progress has been limited and highlights the following key issues.

- The Programme was "reprofiled" to account for a lack of resources. Over 1/3rd of the programme budget was transferred to other government programmes, resulting in a shortfall in funding.
- Insufficient evidence to prioritise activities to achieve the biggest impact, identify the greatest need or provide best value.
- NAO has "low confidence" in the evidence supporting outcomes. It thinks that only 1 of the 12 objectives will be achieved.
- Programme Management weaknesses will continue.

In response to the issues identified, the NAO has made the following recommendations in the Report:

- Departments to identify areas of the Programme having greatest impact or most importance and to "focus" resources. Some areas will see a reduction in or have funding cut.
- Consultation to take place to identify cyber security priorities.
- Beyond 2021 strategy - Distinguish between centrally funded and private sector responsibilities.

Given the above, what are the implications for Health and Social Care ?

Health is rightly defined by the government as being part of the UK's Critical National Infrastructure (CNI) and its resilience to cyber-attack is subject to intense scrutiny and debate. This has been brought into sharp focus following the 2017 WannaCry cyber-attack on the NHS.

Recent legislation such as General Data Protection Regulation (GDPR) 2018 and the NIS (Security of Networks and Information Systems) Regulations 2018 add additional responsibilities to those charged with maintaining IT networks, protecting data and ensuring compliance.

Health & Social Care is not a lead department for delivery of National Cyber security Programme strategy and objectives. There is therefore a danger that in times of reducing budgets and unprecedented operational challenges, that the health and care sector's cyber security priorities may not receive the attention they deserve.

One of the key recommendations in the report is for Departments to identify which activities have the greatest impact or are most important to them. If there is insufficient focus on cyber-security by Health and Social Care, leading to a lack of understanding of impact and priorities, they may not be at the front of the queue when it comes to the allocation of the programme's resources.

This represents a significant risk in the way the sector is able to develop and maintain cyber-security, impacting on the confidentiality, integrity and availability of Health and Social Care IT systems and the data contained within them.

In order to secure the technical and monetary resources required to ensure its systems are resilient and secure from cyber-attack, Health and Social Care organisations should consider take the following action:

- Provide the risk-based evidence needed to support the prioritisation of Health and Social Care's activities above those of competing government departments.
- Ensure that evidence demonstrates which activities will provide the biggest impact for the money spent.
- Convince the Programme that Health and Social Care's priorities have greatest need and deliver the best value for money.
- In light of the issues with the national Programme, take more responsibility to secure and deliver its own cyber-security activities, using recognised, standards-based information security management principles, such as ISO27001.

The Author, Gary Peace is the CEO & Founder of ESID Consulting, specialising in Insider Threat, Cyber / Information Security and e-Discovery.

He was for 18 years a Police Officer in New Scotland Yard, Metropolitan Police, is a former Head of Digital Forensics at the Competition & Markets Authority and currently serves as a County Councillor. In addition he is Vice Chair of Governors at The Island Free School on the Isle of Wight.

Email: garypeace@esid.co.uk Tel 07973 333 106 Website www.esid.co.uk

Notes

** HMG Cyber Security Breaches Survey 2018.