Príomhoifigeach Faisnéise

rShláinte agus Teicneolaíocht
BhunathraitheachFSS, Ospidéal Dr Steevens, Baile Átha Cliath 8, D08

Chief Information Officer

eHealth and Disruptive Technologies, HSE, Dr. Steevens' Hospital, Dublin 8, D08 W2A8

www.hse.ie
ehealthireland.ie
@hselive
t 01 635 2732

26th May 2023

Deputy Robert Troy
Dáil Eireann
Leinster House
Dublin 2

Re: PQ ref 2329/23

"To ask the Minister for Health the progress being made on implementing the recommendations of a report (details supplied).

(PWC report on the cyber-attack on the HSE)"

Dear Deputy Troy,

Thank you for your above correspondence which has been referred to me for response.

Following receipt of the final Report of the Cyber Post Incident Review [PIR] in November 2021, an implementation programme was established to give effect to the Report's recommendations.

The 4 programmes sitting under the overall implementation programme are the:

- Cyber and ICT Transformation Programme
- Legal and Data Programme
- Operational Resilience Transformation Programme
- Portfolio Management Office

The individual Programmes report to the EMT Oversight Group, chaired by the CEO, which meets twice monthly. In June 2022 an Interim Chief Technology and Transformation Officer [CTTO] and Chief Information Security Officer [CISO] were appointed to lead the ICT/ Cyber Transformation Programme, in advance of the filling of these roles on a permanent basis. The interim CTTO reports to the CEO and is a member of the HSE's Executive Management Team [EMT].

The PIR document [PWC Report] contained a detailed review of the Conti Ransomware attack and published the original 245 strategic & tactical recommendations to uplift the HSE's ICT & Cyber capability. This document and recommendations were signed off by the HSE for implementation.

- PIR published 245 recommendations across 3 workstreams ICT & Cyber, OCR & Programme

- From the original 245 recommendations, 51 were assigned against the ICT & Cyber workstream
- The 51 recommendations were then grouped based on similarity into a logical grouping of 27 recommendations that are outlined in the investment case for 2023
- The ICT & Cyber programme element outlined an investment of €656M million over a period of 7 years.

A Cyber transformation programme was established, and a seven-year investment case was submitted to the Department of Health and shared with the Department of Public Expenditure and Reform. In response to this, in 2023 Department of Health provided €40m of additional Cyber funding to existing cyber funding provided in 2021 and 2022 to support the programme implementation.

The programme assigned the 27 recommendations into seven groupings and prioritised these groupings based on criticality to the HSE. The priorities defined can be described as follows:

- Foundational Technology: It is critical to invest in modernisation of the technology estate. The technology stack in the HSE has critical end of life and end of vendor support technologies which creates significant risk of failure and cyber-attack (out of life software is not security patched or maintained by vendors)
- Compliance: The HSE are subject to a compliance order by the National Cyber Security Centre under the NISD directive. It is critical that the HSE continues to engage in complying as an operator of essential service (OES) under NISD
- Threat & Vulnerability Management: Focus on proactive measures to ensure the environment is consistently managed from a threat and vulnerability management.
- IT Service Management: Rolling out the asset register, and configuration management database (CMDB) and ensuring currency of same.
- SOC: The HSE is continuing to progress interim arrangements with 24x7 enhanced cyber security operations monitoring with specialist external partners whilst working on strategic procurements to maintain and enhance the HSE's security posture

The ICT & Cyber programme continues to deliver on the recommendations through:

- Establishment of the Office of the CTTO
- Establishment of the Office of CISO and supporting security organisation
- Continued investment in key security technologies
- Focus on modernisation of core technology foundation infrastructure, and
- Increasing Cyber Security Awareness at all levels within the organisation
- Develop and enhance in-house Cyber resilience and response capabilities.

The HSE continues to deliver on the PIR recommendations through the evolution of the security organisation under management of the Office of the Chief Information Security Officer.

If you feel that the question has not been fully answered or require any further clarity, please contact me by email at fran.thompson@hse.ie or by phone on +353 86 2546036

Yours sincerely,

Fran Thompson,
Chief Information Officer, eHealth, HSE.