Príomhoifigeach Faisnéise

Teicneolaíocht agus Claochlú
FSS, Ospidéal Dr Steevens,
Baile Átha Cliath 8, D08 W2A8

Chief Information Officer

Technology and Transformation,
HSE, Dr. Steevens' Hospital, Dublin
8, D08 W2A8

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

18th June 2025

Mr Malcolm Byrne TD
Dáil Eireann
Leinster House
Dublin 2

Re: PQ ref 34051/25

"To ask the Minister for Health the financial cost to date of the May 2021 cyberattack on the HSE; the measures now in place to address the exposed vulnerabilities; and if she will make a statement on the matter."

Dear Deputy Byrne,

Following the 2021 Conti ransomware attack, the Health Service Executive (HSE) in Ireland has taken several measures to bolster its cybersecurity defences. €102,099,792 has been invested in cybersecurity related initiatives since May 2021, in response to the attack. The costs of the cyber attack are not expected to change pending legal case outcomes. The HSE has in recent months hired a permanent CISO, growing the CISO Office from 5 FTE's to just over 50 FTEs, while increasing the budget in a similar ratio.

The HSE has a broad range of cyber initiatives, the following are some of the key initiatives:

1. **National Cybersecurity Plan:** A three-year plan has now been signed off and is being implemented. This will deliver upon three core objectives:
    1. Closing findings from previous audits, reports, and assessments
    2. Improving our NIST CSF Maturity, NIS2 compliance and our overall cyber resilience readiness
    3. Deliver on several technology capability focused detection, defensive and corrective solutions

2. **Cyber Security Statement of Strategic Intent (2024-2027)**: This document outlines a unified approach to embedding security into digital health services and continuously adapting defences

3. **Defence in Depth:** Cybersecurity strategy, using multiple layers of defence to protect our systems and data

4. **Post Incident Review (PIR)**: A comprehensive review was conducted to identify vulnerabilities and recommend improvements

5. **Regular Risk Assessments**: Continuous assessments to identify and mitigate potential vulnerabilities

6. **Incident Response Plan**: Development of robust plans to respond effectively to any future cyber incidents

We work very closely with National Cyber Security Centre to ensure that we manage our cyber profile, in addition we work with a range of external service providers, who augment our internal team.

If you feel that the question has not been fully answered or you require any further clarity, please contact me.

Yours sincerely,

_____

Fran Thompson,
Chief Information Officer, Technology and Transformation, HSE.