Review of the 2021 PwC Report about Conti cyber-attack on the HSE using NIST CSF 2.0

Scope

This review provides an analysis of the 2021 PwC report detailing the Conti ransomware attack on the Irish Health Service Executive (HSE). It identifies one significant weakness or risk for each of the six functions of the NIST Cybersecurity Framework (CSF) 2.0 - Identify, Protect, Detect, Respond, Recover and Govern.

For each identified weakness, appropriate security and privacy controls were mapped using NIST SP 800-53 and measurable metrics were proposed to assess the effectiveness of each control over time.

1. Identification of a significant weakness or risk found for each of the six functions of the National Institute of Standards and Technology (NIST) CSF 2.0.

Govern (GV)

The 2021 PricewaterhouseCoopers (PwC) review, commissioned by the Health Service Executive (HSE), highlighted a significant lack of leadership roles in cybersecurity with well-defined accountability. Specifically, the absence of a Chief Information Security Officer (CISO) role resulted in a lack of strategic oversight, contributing to weak cybersecurity governance and failure to implement an internal cybersecurity framework. This gap had a cascade effect creating vulnerabilities across other areas of the cybersecurity programme.
The weakness falls under the category **"Roles, Responsibilities, and Authorities"** and subcategory **GV.RR-02**, which emphasizes the importance of establishing leadership roles within the cybersecurity department.

Identify (ID)

After the incident, the response team struggled to prioritize their response and recovery efforts due to the lack of an asset register outlining critical clinical systems and applications (PwC, 2021, p.4 and p.37). Without a comprehensive asset register, the HSE could not quickly assess the recovery priority of the compromised critical systems, leading to delays in response and recovery (PwC, 2021, p.125).
The weakness falls under the **"Asset Management"** category , specifically the subcategory **ID.AM-01** that covers the maintenance of hardware inventories.

Protect (PR)

The attack originated from a workstation that was reliant only on a single antivirus with signatures not updated for over a year, leaving it vulnerable to malware. Unsurprisingly the review found an inefficient patching and updating strategy across the HSE and the interconnected National Health Network NHN (PwC, 2021, p.7).
The weakness falls under the **"Platform Security"** category and subcategory **PR.PS-02**, that deals with software maintenance, replacement, and removal.

Detect (DE)

According to the PricewaterhouseCoopers report, "the IT environment did not have many of the cybersecurity controls that are most effective at detecting and preventing human-operated ransomware attacks" (PwC, p.7). For instance, the HSE did not utilize a Security Incident and Event Management (SIEM) tool for centralised monitoring and review log events, limiting their ability to detect attacks early(PwC, p.64). This shortcoming allowed the attack to spread unchecked, further increasing the recovery time and damage.
The weakness falls under the category **"Adverse Event Analysis"** and specifically in subcategory **DE.AE-02** that covers the analysis of adverse events using a SIEM or other tools.

Response (RS)

HSE lacked an effective response policy, plan, or runbook to handle to cybersecurity incidents. A response plan and related procedures could have helped the National Crisis Management Team (NCMT) to better understand the Conti attack impact and outcomes (PwC, 2021, p.85). The weakness falls under the category "**Incident Management"** and subcategory **RS.MA-01** that covers incident containment strategies.

Recover (RC)

HSE did not have a formal crisis communication plan (PwC, 2021, p.119) to manage a ransomware scenario. During the incident, servers were shut down to contain the incident leaving both email and network phone systems non-operational. With no alternative communications available, HSE granted a formal derogation to the cybersecurity team to use personal emails and personal devices to communicate during the recovery stage (PwC, 2021, p.140).
The weakness falls under the category **"Incident Recovery Communication"** and subcategory **RC.CO-03** that covers communications of recovery activities and progress to internal and external stakeholders.

2 – Identification of Controls as per NST SP.800-53

This section will focus on identifying suitable controls, using the NIST SP-800-53 Security & Privacy Control document (NIST, 2020), to address each of the weaknesses reviewed in the previous section. Table 1 outlines the six selected controls for each function, including the related Control Family, Control Number, and Control Name.

The appointment of a Chief Information Security Officer is covered under the control family **"PM Program Management"**, control number **PM-2**, and control name **"Information Security Program Leadership Role"**, that specifically addresses the need for leadership and accountability withing an organization.

The creation and maintenance of an Asset register are addressed by the control family **"CM Configuration Management"**, number **CM-8** and control name **"System Component Inventory"**.

The absence of a coherent and uniform antivirus signature update strategy across HSE falls as

control under the Family **"SI System and Information Integrity"**, number **SI-3** and name **"Malicious code protection".**

Continuous monitoring using a Security Incident and Event Manager (SIEM) is included under control family **"SI System and Information Integrity"**, number **SI-4 (3)** and control name **System Monitoring**.

A proper response plan, including related procedures, is covered by the control family **"IR Incident Response",** number **IR-8** and control name **"Incident Response Plan".** This control includes the development of the response plan, its distribution to incident response staff, and its updates following organizational and system changes.

The need for a robust Crisis Communication Plan during the recovery and related procedures falls under the control family **"CP Contingency planning"**, number **CP-4**, and control name **"Contingency Plan Testing"**. HSE should periodically assess its communication strategy plan as, especially during ransomware attacks, a ready alternative communication strategy must be available for the recovery team and senior leadership (PwC, 2021, p.74).

A reasonable expectation is that all these controls should have been implemented before the time of the incident, as they were already considered best practices in cybersecurity.

These six controls were included in the NIS Compliance Guidelines for Operators of Essential Services (National Cyber Security Centre, 2019, appendix B), where the NIST framework and SP 800.53 Rev. 4 controls were recommended by the National Cyber Security Centre. Notably, that HSE had not filed the Operator of Essential Services (OES) return required for compliance with the Network and Information System Directive (NISD) since 2019 (PwC, 2021, p.97).

The use of a SIEM to monitor and early detect potential threats was identified as "state of the art" in the Irish transposition of the NIS European Directive, the Statutory Instrument No. 360/2018, which applies to providers of essential services like the HSE. It states: "The measures to be taken by an operator of essential services pursuant to paragraph (1) shall ensure, having regard to the state of the art, a level of security of network and information systems appropriate to the risks posed" (European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018).

While the explicit requirement for a CISO was not outlined by frameworks, standards, or regulations like NIST, ISO 27001, and NIS in 2021, they strongly recommend clear cybersecurity leadership roles. For example, the ISO standard 27001:2013 states: "Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated" (ISO, p.8), emphasizing the need for clear assignment of information security responsibility. Given the size and criticality of a national health service, appointing a CISO is of paramount importance in assessing risk, communicating HSE's cybersecurity gaps to the executive board and driving cultural transformation.

In the context of the missing asset register, the same ISO 27001 Annex A. 8 standard specifically included controls for asset management (IT Governance Ltd, 2015, p.4).

As previously mentioned, the absence of a uniform antivirus signatures update strategy, the lack of incident response plan and contingency plan testing were all addressed by controls outlined in the NIS Compliance Guidelines for Operators of Essential Services (National Cyber Security Centre, 2019, appendix B).

3 - Identification of Risk Metrics

In this section, a suitable metric based on up to three measures will be proposed for each function, in order to monitor, avoid or at least mitigate the risks associated with the six identified major weaknesses.

If a CISO was appointed by HSE before the incident, the effectiveness metric of the CISO role was the most critical metric, as the PwC report highlights the lack of leadership within the HSE cybersecurity department as a primary issue. While the other issues, controls and metrics are essential, protecting a large and critical organization is unrealistic without skilled leadership guiding it with a structured framework like the NIST CSF. A proper cybersecurity risk framework implementation can only be achieved if a cybersecurity risk culture permeates all levels of an organization structure, from the executive board level to the last employee.

A SIEM Detection Score could help to understand better the nature of the attack at its onset. However, for a proper analysis of SIEM alarms, the HSE should have had a Security Operations Center (SOC), which absence (PwC, 2021, p.94) is again a sign of poor focus on cybersecurity.

From my experience in engineering and customer support process improvement roles, I have observed that continuous improvement efforts are effective only when staff recognize a company quality culture and there is a sufficient budget support. In the same way, cybersecurity, metrics and controls should not be just buzzwords or a low-priority checklist filling activity; instead, they should be a critical "mission" accepted and owned by any employee.

Govern (GV)

Measures A, B and C parameters are chosen to build a metric the Governance Effectiveness of a Chief Information Security Officer. These measures provide a quantitative view of the CISO's effectiveness by assessing both their participation and their influence on implementing actionable cybersecurity recommendations

A = Percentage of Attendance of governance meetings
B = Percentage of recommendations implemented
C = Percentage of planned reviews conducted on time

As metric we consider the average percentage of the 3 measures CISO Governance Effectiveness = Average (A, B, C)

Identify (ID)

A = Percentage of asset register **internal audits conducted on planned time**.

B = Percentage of **asset register consistency rate** found during an asset register audit (with the hypothesis that asset register should be immediately updated if assets are added or removed).

$$B = \frac{\#items\ in\ asset\ reg - (\#unexpected\ items + \#missing\ items)}{\#items\ in\ asset\ reg} * 100$$

C = Percentage of assets in the asset register assigned to the correct owner or department.

As metric the average percentage of the three measures is used:
Asset Register Management Effectiveness = Average (A, B, C)

Protect (PR)

A = Percentage of Systems fully patched (that could give an indication of number of legacy systems without patches (NIST, 2008, p.A-23).
B = Percentage of systems where the time between patch application and patch release exceeded the assigned target time for that specific vulnerability CVSS score.
C = Percentage of attacks caused by an unpatched vulnerability

As metric we consider the average percentage of A, B and C.
Patching Effectiveness = Average (A, B, C)

Detect (DE)

A = Detection time rate, calculated as following between the Average Detection time and the Maximum Acceptable Time.

$$1 - \frac{Average\ Detection\ Time}{Maximum\ Acceptable\ Time}$$

B = Detection Accuracy rate, is the ratio of the accuracy of the SIEM. A high accuracy rate means the SIEM has a correct tuning to properly to highlight only real threats, with few false positive events.

$$B = \frac{\#alerts - \#false\ positive\ alerts}{\#alerts}$$

C = Detection Coverage: metric that helps to understand which ratio of the network is monitored by the SIEM (with range between 0 and 1).

As metric the SIEM Detection Score is used (where a minimum cap of zero is considered for the detection time rate to avoid negative values when the average detection time is bigger than the maximum acceptable time).

$$SIEM\ Detection\ score\ = C + B + \max(0, (1 - A))$$

Response (RS)

A: Response Team Questionnaire Score (a score between 0 and 1 based on surveys about the effectiveness of the response plan and procedures)
B: Tabletop exercise score (a measure from 0 to 1 of the success of the exercises without blockers)
C: Ratio of number of incidents resolved inside the maximum target time (target that could differ depending on the criticality of system affected)

Metric: Incident Response Plan Effectiveness = Average (A, B, C)

Recover (RC)

A: Rate of contingency plan testing performed as planned (0 to 1)
B: Recovery Team Questionnaire Score (a score between 0 and 1 based on surveys about the communications effectiveness of the recovery contingency plan)
C: Errors ratio in the recovery procedure (symptoms of defective communications recovery procedures) during contingency testing

Metric: Incident Recovery Plan testing = Average (A, B, C)

Reference List

European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 , S.I. No. 360/2018, Dublin: Stationery Office, available: https://www.irishstatutebook.ie/eli/2018/si/360/made/en/pdf [Accessed 22 October 2024].

International Organization for Standardization (ISO), 2013. *Information technology — Security techniques — Information security management systems — Requirements. ISO 27001:2013* Second Edition. Available at: https://cdn.standards.iteh.ai/samples/54534/3f6832e38d66411b9650e53999f99c63/ISO-IEC-27001-2013.pdf [Accessed 23 October 2024].

ItGovernance Ltd, 2015. *ISO/IEC 27001:2013 Technical guidance for transitioning from ISO/IEC 27001:2005.* Available at: https://www.itgovernance.co.uk/download/27001-2013-technical-guidance.pdf [Accessed 23 October 2024].

National Cyber Security Centre, 2019. Draft of NIS compliance guidelines for operators of essential services (OES). Available at: https://www.gov.ie/en/consultation/88b3fc-nis-compliance-guidelines-for-operators-of-essential-services/ [Accessed 22 October 2024].

National Institute of Standards and Technology (NIST), 2008. *Performance measurement guide for information security. NIST Special Publication 800-55 Revision 1*. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf [Accessed 22 October 2024].

National Institute of Standards and Technology (NIST), 2020. *Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Revision 5*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [Accessed 22 October 2024].

PricewaterhouseCoopers (PwC) (2021). *Conti cyber attack on the HSE: Independent post-incident review*. Dublin: Health Service Executive. Available at: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf [Accessed 23 October 2024].

NIST CSF 2.0 Functions	Major weakness/risk	Category	Subcategory	SP 800-53 Rev 5.1.1 Controls			Selected measures	Control efficiency metric
				Control family	Control number and enhancement	Control name		
GOVERN	Lack of high-level cybersecurity leadership roles like the **CISO**, causing a negative cascade effect on HSE culture and approach to cybersecurity, at all levels.	**Roles, Responsibilities, and Authorities (GV.RR)**	**GV.RR-02**	**PM Program Management**	**PM-2**	**Information Security Program Leadership Role**	A = % Attendance of governance meetings B = % recommendations implemented C = % planned reviews conducted on time	CISO Governance Effectiveness = Average (A, B, C)
IDENTIFY	No centralised list of contact details for all HSE staff or **asset register**"	**Asset Management (ID.AM)**	**ID.AM-01**	**CM Configuration Management**	**CM-8**	**System Component Inventory**	A = % asset reg audits conducted in time B = % asset reg consistency rate C = % planned asset register assigned to correct owner	Asset Register Management Effectiveness = Average (A, B, C)
PROTECT	There was a lack of effective **patching** and updates strategy,	**Platform Security (PR.PS)**	**PR.PS-02**	**SI System and Information Integrity**	**SI-3**	**Malicious code protection**	A = % systems fully patched B = % systems with delay in patching weighted with CVSS score. C = % unpatched vulnerability attacks	Patching Effectiveness = Average (A, B ,C)
DETECT	Absence of a Security Incident and Event Manager **SIEM** tool.	**Adverse Event Analysis (DE.AE)**	**DE.AE-02**	**SI System and Information Integrity**	**SI-4 (2)**	**System Monitoring -** Employ automated tools and mechanisms to support near real-time analysis of events.	A = Detection Time rate B = Detection Accuracy rate C = Detection Coverage rate	SIEM Detection Score B+ C + max(0, A)
RESPOND	No suitable **response policy, plan or run books**	**Incident Management (RS.MA)**	**RS.MA-01**	**IR Incident Response**	**IR-8**	**Incident Response Plan**	A: Response Team Questionnaire Score B: Tabletop exercise score C: Ratio of number of incidents resolved inside the maximum target time	Metric: Average (A.B.C)
RECOVERY	Absence of an incident communications plan	**Incident Recovery Communication (RC.CO)**	**RC.CO-03**	**CP Contingency plan**	**CP-4**	**Contingency Plan Testing**	A: Rate of contingency plan testing performed as planned B: Recovery Team Questionnaire Score C: Errors ratio in the contingency testing	Metric: Incident Recovery Plan Testing Average (A, B, C)

Table 1