Focus area 1 - key findings

Preparedness to defend against and respond to a ransomware cyber attack

There was a lack of preparedness within the HSE to defend against or respond to a ransomware cyber attack. Key findings that contributed to this position include:

1. **FA1.KF1 The HSE did not have a single responsible owner for cybersecurity, at senior executive or management level at the time of the Incident.** Limited scenario planning was performed to prepare for a ransomware incident (see focus area 2, area 12: scenario planning below for further detail). Nor were there clear articulations of the HSE's risk to a large-scale ransomware cyber attack that considered known cybersecurity weaknesses. These, alongside the lack of a detailed cybersecurity strategy, operating model or transformation plan can likely be attributed to this cybersecurity leadership absence.

2. **FA1.KF2 There was no dedicated committee that provided direction and oversight of cybersecurity and the activities required to reduce the HSE's cyber risk exposure.** A cybersecurity forum[93] had previously been established within the OoCIO but subsequently disbanded before August 2019[94] without replacement. There was a process where risks were raised to OoCIO management, but there was no centralised decision making committee to provide direction and decide on a suitable course of action to mitigate these risks, considering the cybersecurity capabilities and controls required.

3. **FA1.KF3 There were known weaknesses and gaps in key cybersecurity controls.** The Board presentation on cybersecurity[95] presented on 27 November 2020 highlighted there were many areas of known cybersecurity weaknesses, including known issues with excessive privileges on accounts.

4. **FA1.KF4 The lack of a cybersecurity forum in the HSE hindered the ability for granular cyber risks to be discussed and documented, and for mitigating controls to be identified and rapidly delivered.** When gaps or issues with cybersecurity controls and capabilities were identified, there was no cybersecurity forum for these to be raised at by OoCIO staff[96] (see FA1.KF2). As a result, once cyber risks were identified, action was not always taken with sufficient priority. One interviewee reported that petitioning for security tool or process changes was a "war of attrition".

5. **FA1.KF5 The HSE did not have a centralised cybersecurity function that managed cybersecurity risk and controls.** There was no centralised team to set the vision and tone for security and perform critical security functions, most notably security monitoring and cybersecurity control assurance activities. Further, it should be noted that at the time of the Incident the senior cybersecurity SME, the Information Security Manager, was not performing their business as usual role that included the NIST-based cybersecurity review of OES systems, but was working on evaluating the security controls for the COVID-19 vaccination system. This illustrates the lack of resources available for important cybersecurity activities.

6. **FA1.KF6 It was a known issue that the teams that included elements of cybersecurity in their remit were under-resourced.**[97] Further, within the three cybersecurity teams (which had a total FTE of 15[98]), team members predominantly had IT backgrounds, not expertise and experience in cybersecurity. These cybersecurity team sizes do not correlate with the 4,000 locations (1,200 networked), 130,000 staff,[99] over 70,000 devices and 54 hospitals[100] that make up the health service. The HSE was therefore overly reliant on its already stretched IT resources to perform cybersecurity activities in good faith, as evidenced by interview comments such as "security is not in my job description but I do it part time".

93 HSE OoCIO Security Advisory Group (SAG) Terms of Reference, February 2018
94 CLOSED - HSE Internal Audit Tracking_ICTA015OCIO0916_Internet Access Controls - Follow Up Audit, 28 August 2019
95 Cyber Security Board Awareness Draft V7.2.pdf, November 2020
96 Email with subject RE: FW: CI security solutions discussion document, UNDATED Reported as June 2020
97 Minutes of HSE Board Meeting, 27 November 2020
98 This comprises eight FTE within the Information Security Framework and Control team (two of which are students), the Security Operations team of five FTE and the Security, Standard and Policies team of two FTE. Figures are based on interviewee assertion and/(or) OoCIO Operating Model – 2020 Current State, December 2019.
99 https://www.hse.ie/eng/staff/resources/our-workforce/workforce-reporting/health-service-personnel-census-aug-2021-v2.pdf
100 Cyber Security Board Awareness Draft V7.2.pdf, November 2020

7. **FA1.KF7 The HSE's technology has grown organically and is consequently overly complex, increasing the vulnerability of the HSE to cyber attacks.** The HSE has a complex technological environment that includes a significant number of legacy systems, multiple on-premise email systems and multiple AD domains. [redacted] This included between 30,000 and 40,000 Windows 7 workstations[101] that were deemed end of life by the vendor and operating on extended support. Projects to modernise, standardise and reduce complexity of the IT estate were incomplete at the time of the Incident. This can likely be attributed to: delays reported in interviews as caused by the response to COVID-19; the under-resourcing of technology teams; the lack of a single governed programme that maintained oversight, and the complexities of the IT environment.

8. **FA1.KF8 The HSE had a large and unclear security boundary that encompassed many of the organisations connected to the NHN.** The 'flat' design of the NHN with a lack of network segmentation, paired with bi-direction trust relationships between many AD domains, resulted in many of the organisations connecting to the NHN effectively being within the HSE's security boundary. This exposed the HSE to the risk of cyber attacks from other organisations connected to the NHN, as well as these other organisations connected to the NHN to cyber attacks originating from the HSE.

9. **FA1.KF9 The HSE's effective security boundary did not align with its ability to mandate cybersecurity controls.** The HSE created a network infrastructure where they did not have the ability to mandate cyber controls to prevent and detect ransomware attacks within all organisations that fell within its security boundary (see key finding FA1.KF8).

10. **FA1.KF10 There was no effective security monitoring capability that was able to detect, investigate and respond to security alerts across the HSE's IT environment.** The HSE did not have the modern security tooling needed to detect and prevent ransomware, nor did it have trained security analysts internally or within a Security Operations Center ("SOC") that were able to monitor the available antivirus alerts to investigate, triangulate and respond to potential threats.

11. **FA1.KF11 The antivirus tool ([redacted] Endpoint Security) was over-relied upon to detect and prevent threats on endpoints.** Solely relying on antivirus is not sufficient to protect against the tools and attack techniques used by ransomware groups (and many other modern attackers). Further it should be noted that this antivirus tool:

    - was not monitored 24/7;
    - was not deployed across the full endpoint environment;
    - was evidenced as not being correctly configured on all workstations;
    - was not configured to block malicious activity within the server estate, only to monitor it.

101 Data provided from the antivirus management server (the [redacted] server) of systems that last communicated with [redacted] within the last 3 months, September 2021
National health network (NHN) describes the technology network for the delivery of Health services primarily to HSE staff and secondarily to the staff in the voluntary sector

12. **FA1.KF12 The IT environment had high-risk gaps relating to 25 out of 28 of the cybersecurity controls[102] that are most effective at detecting and preventing human-operated ransomware attacks.[103]** A high-level assessment of the HSE's cybersecurity capabilities, using PwC's proprietary ransomware readiness framework,[104] at the time of the Incident is shown in Figure 11. Further, of the cybersecurity controls implemented, limited assurance activities were performed to test their operational efficiency. This assessment has been performed to provide an illustration of the level of cybersecurity controls in place at the time of the incident specifically in relation to ransomware attacks.

    A Board presentation[105] on cybersecurity presented on 27 November 2020 highlighted how several of these controls were areas of known cybersecurity weakness, although the link to a risk of widespread impact from a ransomware attack was not made. Implementing many of these controls would have been highly likely to have prevented or detected techniques used by the Attacker and therefore significantly increased the Attacker's difficulty in compromising the HSE and achieving their objectives.

13. **FA1.KF13 The HSE did not have a documented cyber incident response plan and had not performed typical preparatory activities such as exercising the technical response.** The HSE did not have an exercised plan for managing and coordinating a cybersecurity incident that impacted the HSE as well as multiple organisations across the NHN. There were no documented cyber incident response runbooks or IT recovery plans (apart from documented AD recovery plans) for recovering from a wide-scale ransomware event.

102 Based on PwC's proprietary ransomware capability framework (see section Preparation: cybersecurity controls before the ransomware attack for further detail), HSE is scored high or very high risk against 25 of the 28 capabilities

103 Human-operated ransomware attacks are different to traditional ransomware attacks in that they are 'hands-on-keyboard' attacks. This involves human attackers using knowledge of offensive techniques and weaknesses in enterprise IT systems, to methodically compromise organisations' networks, compromise systems, overcome defence and cause maximum impact. The ransomware attack that impacted HSE is an example of a human-operated ransomware attack. For further details see: https://www.pwc.com/jg/en/publications/responding-to-growing-human-operated-ransomware-attacks-threat.pdf

104 PwC's proprietary ransomware readiness framework lists the most important cybersecurity controls we have identified to prevent, detect and respond to human-operated ransomware attacks. Focus area 1 used this framework as it allowed the review to evaluate HSE's cyber security controls at the time of the Incident against the specific threat of human-operated ransomware attacks. Focus area 3 have performed a wider review of HSE's cybersecurity preparedness and maturity levels using the NIST cybersecurity and COBIT framework

105 Cyber Security Board Awareness Draft V7.2.pdf, November 2020

Figure 11: High-level assessment of the HSE's cybersecurity capabilities against PwC's proprietary ransomware readiness framework, colour coded by their risk rating, as at the time of the Incident.

Response to the ransomware cyber attack

There were opportunities to detect malicious activity prior to the detonation phase of the ransomware. Following the execution of ransomware, the HSE mobilised a response to overcome the significant challenges posed by both the attack and its lack of preparedness.

Key findings relating to the response to Attacker activity in the days leading up to the Incident include:

1. **FA1.KF14 The cyber attack was not actively identified or contained prior to the ransomware execution, despite the Attacker performing noisy and 'unstealthy' actions.** The investigation determined that the ransomware attack originated from a malware infection on patient zero on 18 March 2021, when the user opened a malicious Microsoft Office Excel document that was attached to a phishing email. Following this, the Attacker continued to operate in the environment, including compromising and abusing a significant number of highly privileged (e.g., system administrator) accounts and moving laterally to both statutory and voluntary hospitals. Many of the tools and techniques employed by the Attacker during this time period (which included the use of basic and non-obfuscated malicious PowerShell commands), were well-known to be used by ransomware groups. As such, they would have almost certainly been identified by modern security monitoring tooling and a security monitoring capability. It should be noted that the HSE's antivirus tool ([redacted] Endpoint Security) did record detections of these tools[106] but these were not actively identified or thoroughly investigated by the HSE's teams (see next finding).

2. **FA1.KF15 The HSE's antivirus identified a tool commonly used by ransomware groups (Cobalt Strike) on six servers on 7 May 2021 (and several more servers in the following days) but these alerts were not appropriately actioned.** The HSE did not identify these alerts until after their cybersecurity solutions provider flagged them on 12 May 2021[107] and 13 May 2021.[108] At that point, the retained third party 'critical incident response service', was not invoked,[109] despite the alerts being for a tool commonly used by ransomware groups (Cobalt Strike) and being across multiple servers. The response to these detections was not sufficient as the HSE did not; invoke a cybersecurity incident; escalate the cybersecurity incident; identify the severity of the threat; or thoroughly investigate and contain the threat. This was a result of insufficient cybersecurity expertise to understand the significance of these detections and an absence of cyber response governance and processes to guide the response to cybersecurity incidents.

3. **FA1.KF16 Two voluntary hospitals identified suspicious activity prior to the execution of ransomware, but a HSE centralised response was not initiated.** On 10 May 2021, Hospital C identified activity on a domain controller ("DC") that they suspected as malicious and so sought advice from Hospital C's cybersecurity solutions provider on whether the alerts warranted concern.[110] The third-party stated that since the threat has been handled by their antivirus tool that "the risk is low here". As a result of the third party's email response, Hospital C did not initiate a cyber incident response investigation, and therefore did not identify a cybersecurity incident. On the evening of 12 May 2021, Hospital A notified the OoCIO that its network had been compromised[111] and suspected malicious activity was originating from the HSE.[112,113] The HSE performed an IT-centric investigation on 13 May 2021 that incorrectly concluded that the HSE was "under threat from Hospital A, not the other way around".[114] Following this, the HSE did not seek the help of an external cyber incident response firm nor the NCSC to investigate and provide guidance on how to respond to the detections.

106 HSE's Incident Response provider Intrusion Investigation Report, September 2021
107 Email from the HSE's cybersecurity solutions provider to the SecOps team with subject "Threat Not Handled", 12 May 2021
108 Email from the HSE's cybersecurity solutions provider to the SecOps team with subject "Threat Not Handled", 13 May 2021
109 Appendix 7: Services Contract, Health Service Executive and the HSE's cybersecurity solutions provider Information Systems Limited Agreement Relating to the Provision of Services pursuant to Request for Tenders for the Establishment of a Multi Supplier Framework for the provision of Security Software and Associated Reseller Services, 24 December 2017
110 Logging call with Hospital C's cybersecurity solutions provider on 10/05/2021 17:06, 10 May 2021
111 Email with subject: Query, 12 May 2021 23:53
112 Email with subject: FW: Recognise these addresses??, 12 May 2021 23:36
113 Email with subject: FW: Query, 12 May 2021 23:53
114 Email with subject: RE: Summary 13 May 2021 12:47

The HSE did not link these events to the antivirus tool detections that their cybersecurity solutions provider had notified.

4. **FA1.KF17 Two organisations successfully acted on detections of the Attacker preventing the deployment of ransomware within their estates.** The DoH and Hospital A successfully acted on alerts and detections of suspicious activity, and engaged third-party incident response services. The DoH quickly deployed EDR security tooling[115] that was then able to prevent the ransomware from executing on the majority of its infrastructure, including critical and data servers. Hospital A engaged the Hospital A's Incident Response provider, who worked with them to use their already deployed security tool. Had the HSE responded in a similar fashion (particularly following the escalations made by Hospital A and the HSE's cybersecurity solutions provider) then it is likely that the widespread encryption of the HSE environment would have been prevented.

Key findings relating to the response to the detonation phase of the ransomware attack include:

1. **FA1.KF18 The HSE with the help of third-parties mobilised a response to the ransomware attack and overcame many of the significant challenges the ransomware attack presented, drawing on their experience responding to crises, including COVID-19.** The HSE recognised the need for additional resources and specialist skills and engaged third parties for incident response[116,117] legal and forensics support early on. The impact of the Incident on a national scale encouraged goodwill from third party support and vendors, including the provision of pro bono work. This allowed a good cadence to be established within 24-48 hours that included multiple daily standups, Major Incident (MI) meetings and other programme governance. The HSE developed effective response structures and processes that evolved over the course of the response. The decision to set up a physical hub for operations in Citywest (on 21 May 2021[118]) was widely reported as being invaluable to working collaboratively between different response and recovery teams, whilst also boosting morale.

2. **FA1.KF19 The HSE was reliant on third-parties in the early weeks of the Incident to provide structure to the response activities.** The first physical hub for senior management was set up 15 May 2021[119] in a third party organisation, before moving to accommodation at Citywest on 21 May 2021.[120] The Defence Forces were brought in 18 May 2021 and were widely reported in interviews to have provided key response structures.

3. **FA1.KF20 Time was lost during the response due to a lack of pre-planning for high impact technology events.** The HSE was not prepared to respond to a cyber incident of this scale ("everything going offline") due to the lack of defined and exercised response processes and plans. Key examples of this include:

   - No cybersecurity response plans and playbooks;
   - No security tooling capable of investigating and remediating security alerts;
   - No centralised list of contact details for all HSE staff or asset register;
   - No offline copies of key IT and security documentation were kept, for example network diagrams;
   - No pre-established prioritised list of applications and systems for recovery, based on clinical services, that was cognisant of cross-technology dependencies;
   - No pre-agreed, setup and tested out-of-band communication system that would enable users to communicate in the event of a cybersecurity incident. Multiple collaboration and communication platforms were used after the Incident resulting in confusion and team members not being able to easily communicate; increasing the day-to-day difficulty of responders.

115 Endpoint Detection and Response (EDR)
116 HSE's Incident Response provider Intrusion Investigation Report, September 2021
117 Minutes of Cyber Attack MI Meeting 10 am - 14052021, 14 May 2021
118 Conti Cyber Response NCMT Structures Governance and Admin V1.10, 31 May 2021
119 Programme RAID Log, 2021
120 Programme RAID Log, 2021

4. **FA1.KF21 The HSE spent a significant amount of time during the response gathering information about applications, as this information was not recorded and up-to-date in a central or offline application register.** The lack of centralised information about applications caused inefficiencies in the response as the HSE did not have up-to-date information on applications. This meant that as part of their response, they had to develop a list of applications that were in use within the corporate, acute and community spaces. As well as identify and define missing details such as the application's owner, its priority for recovery, details of the systems they were hosted on and in some cases the application's purpose. For some applications, the HSE was reliant on vendors to pull this information together, and provide the information critical to the application's recovery.

5. **FA1.KF22 There was a heavy reliance on specific individuals during the response. This likely contributed to a recovery timeline that was longer than could have been achieved.** There was a heavy reliance on key members of staff in IT teams that effectively caused bottlenecks. This was due to the large scope of their BAU IT roles and responsibilities, the lack of IT resourcing and a lack of documented and standardised information and procedures. This concentration of knowledge prevented opportunities for further delegation (such as acquiring more burst capacity from third parties) and meant that the HSE had limited response resilience if these individuals had become unavailable during the critical weeks of the response.

6. **FA1.KF23 The response initially prioritised the recovery of foundational systems, and applications on the OES list[121], before advancing to an approach that focused on clinical risks and the recovery of end-to-end clinical services.** Before the incident there was not a complete and documented list that prioritised all HSE applications and systems. As a result IT teams initially focused on restoring the seven priority clinical applications that were identified in the OES list.[122] The recovery strategy advanced from the restoration of these seven applications, to be centered around recovery of end-to-end clinical service (including the dependencies of applications to restore end-to-end clinical services) following the co-location of all responders to Citywest on 21 May 2021.[123]

7. **FA1.KF24 There was a lack of clearly defined and delineated decision making authority between the HSE, hospitals and CHOs in the case of a health service-wide crisis.** After the ransomware attack was identified, the OoCIO gave a central mandate to power down systems and wait for instructions (whilst they assessed the impact and established next steps) as there was not a delineated decision making structure to allow for local nuances. At least one hospital (Hospital B) used a third party to review their environment and confirm that it was unaffected by the ransomware. Invoking local decision making during this initial interim period allowed the hospital to regain IT systems and provide critical radiotherapy services within the first week of the Incident.

8. **FA1.KF25 The OoCIO was not able to provide or source (through third party burst capacity) the scale of the IT support required by hospitals and CHOs during the extended response to restore applications, systems and services at pace.** The centralised IT team structure of the HSE meant that little IT subject matter expertise was available locally within the HSE's hospitals and CHOs. It was widely reported by hospitals and CHOs[124] that they were heavily reliant on the central OoCIO IT resources for response activities and on personal relationships with OoCIO IT teams to progress and unblock tasks. The OoCIO IT resources were however, already stretched performing national ransomware attack response activities and therefore struggled to effectively prioritise this help.

9. **FA1.KF26 The HSE had limited to no ability to investigate the attack using its own tooling.** The HSE was not centrally collecting and retaining logging from systems, network and security tooling. The central collation point for their antivirus alerts (the antivirus management server) was encrypted and deemed unrecoverable as a result of the ransomware attack. The encryption of the antivirus server meant that the HSE was unable to determine the circumstances and audit trail surrounding what detections were reported back to the central console in the lead up to the ransomware execution. Therefore, without the deployment of their Incident Response provider's

121 The Network and Information Systems Directive (NIS-D) 2016/1148 was signed into Irish law on 18 September 2018. It involves the application of security obligations on operators of essential services (OES). HSE interviewees referred to an 'OES application and system list' they compiled in line with NIS-D obligations.

122 DOE Application Catalogue and Critical Services as defined under NIS Directive Final

123 Conti Cyber Response NCMT Structures Governance and Admin V1.10, 31 May 2021

124 Observations made are based on interviews with a sample of nine hospitals (5 statutory and 4 voluntary) and 2 CHOs

endpoint agent the HSE would have had no ability to perform forensic analysis over their systems and therefore fully investigate the attack.

10. **FA1.KF27 The HSE's Incident Response provider identified evidence of how the Attacker was able to gain unauthorised access to the HSE's IT environment and the Attacker's subsequent activities.** The HSE worked closely with their Incident Response provider to ensure they had the available information required to enable an effective investigation and response. This resulted in an investigation that identified evidence of how the Attacker was able to gain unauthorised access to the HSE's IT environment and what the Attacker did once they were able to gain this access.

Key findings from the investigation[125] included that the Attacker:

- gained unauthorised access to the HSE network through a phishing email on 18 March 2021 (this activity was attributed to the Attacker the HSE's Incident Response provider refer to as UNC2633);
- used a number of tools commonly utilised by human-operated ransomware groups to perform reconnaissance and move laterally through the HSE's environment (compromising 180 systems);
- used the network connectivity provided by the NHN as well as the bidirectional trust between several AD domains to easily move laterally across to six voluntary hospitals and one statutory hospital;
- used an exploit that was widely publicised as a critical patch[126] to gain access to the networks of two hospitals;
- compromised at least [redacted] highly privileged accounts[127] across HSE, Hospital A, Hospital K, Hospital L, Hospital J and Hospital B;[128]
- browsed local or remote folders on systems across HSE and four organisations;
- opened files and attempted to view them using RDP;[129]
- made copies of files;
- created archives (.zip and .rar) of files;
- accessed the file sharing website Domain A; and,
- deployed ransomware throughout several organisations connected to the NHN.

Additionally, the [redacted] malware (which includes an Outlook module to harvest contact information and email content from infected hosts) was identified on several hosts within the HSE's environment. An output from the execution of this module was identified on one system within the HSE's [redacted] domain.

The investigation was unable to identify conclusive evidence that data exposed to the Attacker was then successfully exfiltrated by the Attacker out of the HSE's environment (for example to a file sharing website). However, it is known that the Attacker provided samples of the HSE's and Hospital D's (a Section 38 hospital and therefore independent data controller[130]) data in a chat room (accessed via a link in the ransom note) and that some data was published on the dark web.[131] It is also known that the Financial Times published redacted extracts of the published data (which was verified as originating from the attack on 14 May 2021)[132] and then worked to provide a copy of this data to the HSE's Incident Response provider on 25 May 2021.[133]

Hospital D conducted its own review of the data provided by the Financial Times and made a decision to notify identified data subjects as per Article 34 GDPR.[134] The HSE reviewed the data provided by the Financial Times and confirmed that the HSE data related to a Statutory Hospital ("Hospital M"), for which the HSE is the data controller. The HSE assessed the personal data risk to the rights and freedoms of individuals within this data set to be low[135] and therefore it was deemed not necessary to inform the relevant data subjects.

125 HSE's Incident Response provider Intrusion Investigation Report, September 2021
126 The threat actor used the [redacted] exploit to gain access to the networks of Hospital A and Hospital B. The [redacted] exploit was widely publicised and given a Common Vulnerability Scoring System (CVSS which is a framework for communicating the characteristics and severity of software vulnerabilities) score of 10/10.
127 The compromised accounts consist of two 'enterprise admins', 26 'domain admins', two 'administrator', one 'admin' and two 'service desk admin'.
128 HSE's Incident Response provider Intrusion Investigation Report, September 2021
129 Remote Desktop Protocol (RDP) provides a user a graphical interface to connect to a remote computer over a network connection.
130 Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021
131 Privileged and Confidential Terms of Reference Legal and Data Steering Group V004, June 2021
132 Privileged and Confidential Terms of Reference Legal and Data Steering Group V004, June 2021
133 Draft OoCIO Cyber Governance Report v0.2, UNDATED
134 Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021
135 Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021

The HSE retained a third party to conduct additional in-depth forensic analysis on the systems identified by their Incident Response provider (where data was exposed to the threat actor), to determine the probability of data exfiltration from these systems and to identify any other potential data exposure and exfiltration sources. The HSE has also retained two third party services to perform ongoing dark web and web monitoring activities.

At the time of this report, the work aligned to the HSE's Legal and Data workstream established on 19 May 2021[136] is ongoing. As of yet, therefore the HSE has not made any data subject notifications but continues to work closely with the DPC.

The impact of and recovery from the ransomware cyber attack

Due to the scale and impact of the ransomware, paired with the complex and legacy IT environment, the technical recovery of IT systems has been challenging. Key findings on the technical impact of the Incident include:

1. **FA1.KF28 The impact of the ransomware on the IT environment was reported by the HSE's management to lead to 80%[137] encryption.** The HSE's Incident Response provider's investigation identified encrypted files on systems within the HSE and the following voluntary and statutory hospitals: Hospital C; Hospital K; Hospital D; Hospital L; Hospital J and Hospital B.[138] The HSE was the most impacted by the ransomware attack, with all nine of its domains displaying evidence of encryption.[139] In total, the HSE's Incident Response provider identified over 2,800 servers and 3,500 workstations across 15 domains, with evidence of encryption.[140] This likely represents a lower bound on the number of systems encrypted, as some systems were restored from backups or rebuilt prior to endpoint agent deployment, reducing the HSE's Incident Response provider's ability to determine if encryption had occurred.

2. **FA1.KF29 The impact of the ransomware attack on communications was severe, as the HSE almost exclusively used on-premise email systems (Exchange and [redacted]) that were encrypted, and therefore unavailable, during the attack.** The HSE had begun to migrate users to Exchange Online [redacted] but this was limited to pilot projects at the time of the Incident and had been identified by the HSE as a complex project to deliver. Had the HSE invested in reducing email complexity and completed migrating staff to Exchange Online, the impact of the ransomware on email would have likely been minimal, reducing the impact to team collaboration. See key finding FA1.KF38 for the detail regarding email recovery.

Key findings on the recovery include:

3. **FA1.KF30 The HSE took action to contain the ransomware attack by powering down systems and disconnecting the NHN from the internet.** These containment steps restricted the ability of the Attacker to further their activities and in the face of spreading ransomware within an architecturally open environment were the most pragmatic. The HSE did not have the realistic option of carrying out a more compartmentalised approach that accounted for the impact on organisations, due to the open design of the NHN, the immaturity of cybersecurity controls and governance, and as this had not been planned for or rehearsed.

4. **FA1.KF31 It is unclear how much data would have been lost if a decryption key had not become available.** It was reported that online backups were encrypted in places and that secondary backups to tape were only made periodically. Therefore it is highly likely that segments of data would have been unrecoverable from backups, and a full recovery of data was only possible due to the provision of a decryption key by the Attacker.

5. **FA1.KF32 Without the decryption key, it is unknown how long it would have taken to recover systems from backups but it would have likely taken considerably longer.** Prior to receiving the decryption key, the HSE was recovering systems from backups. This would have required a significant amount of IT resources and equipment to be undertaken at the scale required to recover all servers and applications.

136 Privileged and Confidential Terms of Reference Legal and Data Steering Group V004, June 2021
137 Percentage confirmed in interview by the CTO within OoCIO Infrastructure and Technology
138 HSE's Incident Response provider Intrusion Investigation Report, September 2021
139 HSE's Incident Response provider Intrusion Investigation Report, September 2021
140 HSE's Incident Response provider Intrusion Investigation Report, September 2021

6. **FA1.KF33 The HSE missed opportunities for efficiencies in the recovery of systems and applications due to a lack of preparedness.** The lack of preparedness for a widespread disruptive IT event often created bottlenecks and prevented teams from being able to get to work on the highest priority tasks. In particular, the lack of a comprehensive, current asset register mapped to critical services delayed recovery efforts due to the wait between teams as this information was gathered and through unknown dependencies creating inefficiencies.

7. **FA1.KF34 The processes and response structures for recovering systems and applications were designed and developed in response to the Incident.** Many of the processes used to recover systems and applications were developed during the crisis. This resulted in a lack of immediate awareness, understanding and implementation of agreed processes from staff members potentially increasing the HSE's cyber risk at the time of the response. For example, there was at least one instance of a potentially compromised system being reconnected to the network (before it was confirmed as clean and pre-authorised by the HSE's Incident Response provider and the Tech Team[141]), inadvertently exposing the HSE to a heightened level of risk.

8. **FA1.KF35 The HSE's Incident Response provider and the HSE, developed go-to-green processes[142,143,144] to ensure the secure recovery of systems and reduce the risk of further ransomware attacks.** The HSE's Incident Response provider and the HSE developed requirements that every system within the HSE, voluntaries and CHOs must meet before being able to rejoin the network, and for organisations to be reconnected back to the NHN and the internet.

9. **FA1.KF36 The complexities of recovering applications and systems were not well understood.** Due to the unknown dependencies between systems and a lack of recovery process pre-planning, recovery efforts were complicated. For example, recovery teams reported that it was difficult to facilitate vendor support. As a result, workarounds (such as using screen shares to provide vendors with temporary access) had to be employed. These workarounds were also in some cases further complicated through the inconsistency in access to collaboration tools (see response to the detonation phase of the ransomware attack key findings FA1.KF18 - FA1. KF27).

10. **FA1.KF37 Despite the challenges presented by the ransomware attack and the lack of preparedness, the HSE was able to recover 1,075 applications and over 87,000 systems.**[145] Our review consistently noted the willingness of HSE staff members across the organisation to come together and contribute wherever needed to deliver services to patients. The HSE recovered their primary identity systems ([redacted] AD domain) within a matter of days after the ransomware attack. The HSE was able to prioritise and restore applications and systems during the response including:

    - After one month, the HSE was able to decrypt 47% of servers and fully restore 48% of Acute applications, 40% of Community Services applications and 64% of business services applications.[146]
    - After two months, the HSE was able to decrypt 94% of servers and fully restore 85% of Acute applications, 94% of Community Services applications and 79% of business services applications.[147]
    - After three months, the HSE reported that 100% of servers were decrypted and they were able to fully restore 95% of Acute applications, 98% of Community Services applications and 91% of business services applications.[148]

141 Minutes of Cyber Attack MI Meeting 11 am - 19052021, 19 May 2021
142 Voluntaries and Go-to-Green, 26 May 2021
143 CTO Document Device Go Green Draft Approach, 23 May 2021
144 CTO Document Remote Access Go Green Draft Approach, 24 May 2021
145 Weekly Brief, 21 September 2021
146 SITCEN SITUATION REPORT, 18:30 14 June 2021
147 Weekly Brief, 20 July 2021
148 Weekly Brief, 21 September 2021

11. **FA1.KF38 HSE had significant issues with restoring email back to normal operations for users, resulting in ongoing disruption to employees.** Due to the complexity of the email infrastructure, even when the service was itself restored, user level disruptions such as empty mail boxes continued to affect staff's ability to perform recovery and BAU activities. Ongoing disruption with email services impacted the staff's ability to recover applications and systems. Since the ransomware attack, there has been over 38,000 tickets raised with the national service desk relating to ongoing issues with email.[149] Over 20,000 of those tickets were raised between 20 July 2021[150] and 21 September 2021.[151]

12. **FA1.KF39 The strategy to prioritise national systems recovery over local systems meant that statutory hospitals and CHOs that were not yet using 'standard' infrastructure (some with limited local IT resources) experienced recovery delays.** Organisations not yet using 'standard' infrastructure (for example, organisations not using national applications) were effectively deprioritised by the strategy to prioritise national systems. This was then further compounded for hospitals and CHOs with little to no IT resource and who were therefore wholly reliant on the OoCIO for their recovery.

Sustainable reduction of risk since the ransomware attack

The focus of the HSE's activities since the attack has been on implementing recommendations provided by third parties and to continue to recover systems. Limited evidence has been provided to show that activity has yet to take place to ensure that the HSE's cyber risk exposure is reduced sustainably.

Key findings on the improvements made by the HSE post cyber incident, and on HSE's current approach and current ability to sustainably reduce cyber risk, include:

1. **FA1.KF40 The HSE engaged their Incident Response provider to continue providing a managed detection and response service to March 2022.** This capability is the most crucial defence the HSE has against further ransomware attacks at present, and provides a valuable 'safety net' given the inherent weaknesses in cyber security controls across the estate. The HSE has not yet identified a long-term replacement for the managed detection and response service, with the current solution ending in March 2022.[152]

2. **FA1.KF41 The HSE increased the scope of services provided by the current third parties to provide 24x7 monitoring capability of its antivirus tool[153] and cloud environment.[154]** The HSE's cybersecurity solutions provider and Third Party B provide a 24x7 security monitoring service limited to the antivirus tool ([redacted] Endpoint Security) and Microsoft Cloud platforms[155] (which includes the HSE [redacted] tenancy[156]) respectively.

3. **FA1.KF42 Improvements to the HSE's in-house Security Operations capability (for example defining processes and documenting response roles) have not yet been implemented.** These improvements along with other immediate improvements identified are critically important to ensure that alerts of malicious activity will be investigated and escalated with due care. As of yet there is little evidence to show that any 'quick fixes' to the HSE's security monitoring capability have been implemented beyond the retaining of third party monitoring services.

149 21 September 2021 Weekly Brief, 2021
150 20 July 2021 Weekly Brief, 2021
151 21 September 2021 Weekly Brief, 2021
152 https://irl.eu-supply.com/ctm/Supplier/PublicTenders/ViewNotice/248668
153 Service Contract Agreement – Addendum 1 Managed Security Monitoring & Incident Response Service 24-Hours / 365 Days, Prepared 21 June 2021 (Unsigned)
154 Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021
155 Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021
156 Confirmed by the General Manager Head of Technology, Infrastructure & Deployment within OoCIO Infrastructure and Technology by email, 8 October 2021

4. **FA1.KF43 The HSE was not empowered to mandate that voluntary hospitals continue with the improved levels of security monitoring (or other security controls); this could expose the health service to the risk of further cyber attacks.** The HSE does not have the authority to mandate voluntary hospitals continue to use the HSE's Incident Response provider's Managed Defence monitoring agent or replace this with a like-for-like replacement (which will require ongoing cybersecurity expenditure). If voluntary hospitals do not maintain the current capability or procure a similar, market leading solution, then this will expose the HSE and wider health service to risk of further cyber attacks. This illustrates how the HSE's security boundary continues to be misaligned with their ability to mandate cybersecurity controls.

5. **FA1.KF44 A finalised security improvement plan[157,158,159,160] does not exist and the draft security improvement plan and programme[161,162,163,164] is unlikely to significantly reduce the risk of future ransomware attacks.** The current draft plan and programme is a consolidation of IT projects and identified gaps. It also highlights the need to create a final security improvement plan with defined governance and accountability across the organisation. Therefore at present no improvement plan exists that is structured or architected using a cyber threat view that centres on improvements around key cybersecurity capability areas that are most effective at detecting and preventing human-operated ransomware attacks. It does identify some gaps in these capability areas as items to be addressed in long-term planning[165] but it should be noted that improvement in these gaps are crucial to reducing the risk of ransomware attacks in the short term.

6. **FA1.KF45 A holistic view of cybersecurity improvement activities does not yet exist which increases the risk that foundational improvement activities will be missed.** There is a risk that the HSE's current approach to focus action around the remediation activities outlined by their Incident Response provider, will likely lead to a piecemeal approach that does not take account of the fundamental root causes of such issues. For example, at present it is well known that there are issues with the coordination and tracking of the response to security alerts between technology teams, but the resolution of this is not yet included within any finalised plans.

7. **FA1.KF46 There is no centralised governance programme that maintains oversight of identified cybersecurity improvements, resulting in a lack of clarity about what has been delivered and what remains to be done.** Improvement actions are currently being discussed at technological operational meetings and a programme management governance structure to oversee these activities and produce centralised progress figures against agreed milestones is yet to be developed. This has resulted in a lack of clarity around what security improvements have been delivered, and what security improvements still need to be delivered in response to the Incident.

8. **FA1.KF47 A cybersecurity transformation programme, that will sustainably reduce cybersecurity risk in the long term, has not been planned, approved or resourced.** Some initial security improvement documents[166,167,168,169], as outlined in key finding FA1.KF44, exist but these do not articulate the scale of necessary change or detail the plan for such a transformation. Both a cyber transformation plan and a framework to help achieve that plan are required that will redesign how the HSE manages and maintains its cyber risk within its extensive technological estate (see medium-term recommendation FA1.KR13 for further detail).

157 HSE IT Security Planning, UNDATED Last Modification recorded 15 September 2021
158 Cyber Security Risk Management, UNDATED Last Modification recorded 15 September 2021
159 CTO Document Security Improvement Programme Draft, 31 August 2021
160 OoCIO-07 Investment Plan 2020 -Cyber Security Draft, 1 June 2019
161 HSE IT Security Planning, UNDATED Last Modification recorded 15 September 2021
162 Cyber Security Risk Management, UNDATED Last Modification recorded 15 September 2021
163 CTO Document Security Improvement Programme Draft, 31 August 2021
164 OoCIO-07 Investment Plan 2020 -Cyber Security Draft, 1 June 2019
165 CTO Document Security Monitoring V1 HSE, 04 June 2021
166 HSE IT Security Planning, UNDATED Last Modification recorded 15 September 2021
167 Cyber Security Risk Management, UNDATED Last Modification recorded 15 September 2021
168 CTO Document Security Improvement Programme Draft, 31 August 2021
169 OoCIO-07 Investment Plan 2020 -Cyber Security Draft, 1 June 2019

9. **FA1.KF48 The HSE still has a significant amount of legacy IT that needs to be modernised.** [redacted]

10. **FA1.KF49 Key artefacts created within the response are not yet being centrally and systematically collated.** The HSE was able to gather a significant amount of information in the middle of a crisis about the applications that were being used across the HSE, hospitals and CHOs. In addition, design response processes were created such as communication structures and recovery tracking dashboards (for example the decryption tracking trello board). These artefacts will be invaluable in the event of a similar attack in future. It is therefore critical that information is now collated and appropriately managed going forward.

Focus area 1 - Key recommendations

Key recommendations are outlined below. These have been split between those that are for immediate consideration and those that should follow in the medium-term (as they require further planning and preparation). The HSE should begin planning for the delivery of medium term recommendations immediately, in parallel to implementing the immediate recommendations, and start the implementation phase of these medium-term recommendations within six months:

Immediate recommendation 1

1. **FA1.KR1 Appoint an interim senior leader for cybersecurity (a CISO) who has experience rapidly reducing organisations' vulnerability to threats and designing cyber security transformation programmes *(see tactical recommendation 1.4 in Section 4.2).*** The HSE should appoint an interim senior leader for cybersecurity to be responsible for placing governance around cybersecurity improvements, identifying a sustainable medium-term managed detection and response solution (see immediate recommendation FA1.KR6), identifying future strategy for detection and response and leading the implementation of the immediate recommendations from this review. This role should also be responsible for planning and mobilising teams to deliver a cybersecurity transformation required to sustainably reduce the HSE's risk to ransomware attacks. The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. This interim senior leader should be given the ability to source the necessary expertise from the market to build a team that can give effect to the immediate recommendations listed in this section, and to begin planning for the implementation of medium-term recommendations. The prioritisation for the approval of a CISO and a cyber security team has been recorded within the Q2 Divisional Risk Register as an 'action control' to Risk ID 130 with a due date of 30 June 2022.[170]

2. **FA1.KR2 Establish an executive-level cybersecurity oversight committee, to drive continuous assessment of cybersecurity risk across the provision of health services *(see strategic recommendation 1.2 in Section 4.1)*.** A dedicated executive oversight committee is needed to provide direction and oversight to cybersecurity, both within the HSE and across other parties connected to the NHN.

3. **FA1.KR3 Create a Board committee, to oversee the transformation of IT and cybersecurity to deliver a future-fit, resilient technology base for provision of digitally-enabled health services *(see strategic recommendation 1.4 in Section 4.1)*.** The HSE should consider the inclusion of further specialist non-executive members of the committee in order to provide additional expertise and insight to the committee.

4. **FA1.KR4 Plan a multi-year cybersecurity transformation programme, and identify and mobilise the resources to deliver *(see strategic recommendation 3.2 in Section 4.1)*.** In parallel to delivering the tactical cybersecurity improvement programme, the HSE's appointed interim CISO should plan a cybersecurity transformation that will build lasting cybersecurity capabilities and sustainably reduce cyber risk exposure. This cybersecurity transformation programme should be validated at the Board level. The HSE should also identify suitable resources and expertise to plan and deliver this transformation.

170 DRR Q2 2021, 19 November 2020

5. **FA1.KR5 Appoint a programme lead and define the governance framework for the cybersecurity transformation programme *(see strategic recommendation 3.1 in Section 4.1)*.** A programme lead with experience in cybersecurity transformation should be appointed by the HSE's interim CISO to drive the execution of this transformation. It is critical that this programme lead can work hand in glove with the HSE's technologies teams, to help orchestrate secure technological transformation.

6. **FA1.KR6 Continue to use a managed detection and response service provided by a third party and identify a sustainable medium-term solution *(see tactical recommendation 2.1 in Section 4.2)*.** The current service provided by the HSE's Incident Response provider is the most crucial defence the HSE currently has against further ransomware attacks. If the HSE decides to onboard a new managed detection and response service, it should ensure there is an overlap between this and the HSE's Incident Response provider's current service, so that there are no periods when the IT environment is not monitored.

7. **FA1.KR7 Mobilise a *tactical* cybersecurity improvement programme[171] (while the cybersecurity transformation programme is being planned), with governance that feeds into the interim CISO and can provide updates on the programme's progress into the Board committee *(see tactical recommendation 1.5 in Section 4.2)*.** Dedicated cybersecurity and technology resources should be used to deliver a tactical cybersecurity improvement programme, consisting of tactical work packages that can be delivered at pace using focused governance and reporting to drive accountability. To create these work packages, the HSE should action the following activities:

- **Triage** - All third party recommendations and fixes to the security control gaps identified internally should be triaged into tactical or strategic activities. Tactical activities should be those that will rapidly reduce the risk of ransomware attacks and are achievable in 60 days or less. Note that where improvements are identified as strategic, the HSE should consider what additional tactical improvements can be implemented in the short-term to reduce risk and act as mitigating controls.
- **Test and Assess** - As well as the recommendations it has received from third parties, the HSE should also include recommendations by performing:
  - AD security assessments;
  - Vulnerability scanning of all internet-facing IP addresses;
  - Vulnerability scanning of all internal IP address ranges;
  - A comprehensive assessment of current capabilities and planned improvements against a framework that identifies key capabilities to defend against human-operated ransomware attacks (such as the proprietary ransomware readiness framework used in this report or that recently published by CISA[172]).
- **Architect** - Following the triaging activity, the HSE should use cybersecurity experts to architect and manage a series of tactical work packages to deliver the tactical improvements identified by the triage process. These should be designed to deliver directly and rapidly reduce the risk of ransomware attacks, and be achievable in 60 days or less. Examples of tactical work packages include:
  - Uplift detection and response capability;
  - Remediate priority infrastructure vulnerabilities;
  - Lock down remote access methods;
  - Protect privileged accounts;
  - Improve service account hygiene;
  - Remediate AD hygiene issues;
  - Secure local administrator accounts;
  - Enforce Multi Factor Authentication (MFA) for all remote access methods;
  - Restrict internet access to servers.

This governance should directly feed progress updates into the Board committee. These progress updates should clearly articulate:

- the HSE's vulnerability to ransomware attacks;
- the risk reduction achieved by improvement activities that have been delivered;,

171 A programme that is made up of work packages that rapidly reduce the risk of ransomware attacks and are achievable in 60 days or less

172 https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat

- the extent of the improvements required to reduce the risk of ransomware attacks to an acceptable level.

8. **FA1.KR8 Bring the governance of ongoing IT and cybersecurity improvement projects under the tactical cybersecurity improvement programme *(see tactical recommendation 1.5 in Section 4.2)*.** Governance of current on-going IT projects, that directly or indirectly result in cyber risk reduction, should be brought under the tactical cybersecurity improvement programme's governance (and therefore the CISO see key recommendation FA1.KR7), so the cyber risk reduction they deliver can be tracked, and any risk and issues can be resolved. For example, modernisation projects such as the upgrading of Windows 7 OS and platform modernisation.

9. **FA1.KR9 Use security testing 'find and fix' to identify additional security weaknesses and vulnerabilities by simulating cyber attack techniques, before identifying and triaging pragmatic fixes *(see tactical recommendation 1.5 in Section 4.2)*.** Security testing should be used to focus tactical improvement activities. By simulating the threat of human-operated ransomware attacks, improvements that make it more difficult for an Attacker to successfully compromise the organisation can be identified. The HSE should bring together red team experts[173] and cybersecurity engineers to identify pragmatic fixes to the vulnerabilities and weaknesses identified. These fixes should then be triaged with IT and Security teams to assess their feasibility and identify how best to deliver them (see key recommendation FA1.KR7 Triage). Security testing should then be used to validate improvements have been correctly implemented.

10. **FA1.KR10 Schedule a 'red team' ethical hacking exercise for early 2022 to demonstrate the effectiveness of tactical improvements made and identify areas for further improvement *(see tactical recommendation 1.5 in Section 4.2).*** The HSE's interim CISO should schedule a red team for Q1 2022 to simulate a human-operated ransomware attack from end-to-end, to identify whether improvements have been effective, and to identify additional priority and focus areas for cybersecurity improvements. This should be scheduled in addition to the recorded plans within the Q2 DRR, which recorded an 'action control' to enhance penetration testing and red team exercises with a due date of 31 December 2021.[174]

11. **FA1.KR11 Implement the following tactical recommendations identified through this review, within the mobilised tactical cybersecurity improvement programme (*see key recommendation F1.KR7) (see tactical recommendation 1.5 in Section 4.2)*:**

    a. Improve security monitoring capability

        i. Document a process for how to respond to cybersecurity alerts, that clearly outlines how alerts should be triaged, investigated, contained and responded to. This process should also include coordinating the response to security alerts and incidents raised by any organisations connected to the NHN.

        ii. Augment the Security Operations team with cybersecurity expertise.

    b. Secure privileged access

        i. Develop and implement a robust privileged access strategy that aligns with Microsoft good practice and reduces the risk of privileged accounts being compromised.

    c. Build a vulnerability management capability

        i. Stand up a vulnerability management capability that continuously scans for vulnerabilities that can be exploited by attackers.

    d. Harden the security boundary

        i. Define and communicate a 'security boundary' for the HSE to provide a clear boundary of cybersecurity responsibilities.

        ii. Perform hardening activities on the defined perimeter of the HSE.

        iii. Identify secure methods for clinical staff in voluntary hospitals to access applications hosted by the HSE.

        iv. Use security testing to validate that the HSE can not be compromised by malicious activity from outside its security boundary.

173 Red team experts are ethical hackers who perform simulated cyber attacks through the use of the same tactics, techniques and procedures (TTPs) used by attackers

174 DRR Q2 2021, 19 November 2020

e. Improve governance over the NHN

   i. Risk assess the 'flat' network design and implement segmentation controls that align to the defined level of risk appetite.

   ii. Establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, or share health data, or access shared health services.

   iii. Increase the resourcing of first and second line network teams in line with defined security responsibilities.

   iv. Define a security code of connection for connecting to the NHN.

   v. Define a minimum security standard for the networking of medical devices.

f. Improve preparedness for a ransomware attack

   i. Collect, organise and document artefacts created as part of the response and recovery to the ransomware cyber attack.

   ii. Identify documents required to respond to a ransomware attack (e.g., network diagrams, asset list) and secure these in a cloud repository. This should be aligned with work to develop an IT continuity and recoverability process which was recorded in the Q2 DRR as an 'action control' with a due date of 30 September 2021.[175]

   iii. Setup and test out-of-band communication medium that would enable IT and security teams, as well as employees, to communicate in the event of a cybersecurity incident.

   iv. Ensure that the HSE has a fit-for-purpose incident response service with complementing and embedded internal processes for its invocation.

   v. Review backups and plan for a wide-spread failure recovery mode.

   vi. Document a prioritised list of applications for recovery.

g. Accelerate foundational IT projects

   i. Accelerate the move to cloud based email [redacted] by prioritising the resources available for IT and cybersecurity improvements programmes.

   ii. Prioritise the remediation of critical legacy systems. Particular attention should be paid to the NIMIS application to understand whether the configuration changes made in one hospital (Hospital A) to enable the application to run on Windows 10 can be more widely implemented to expedite the central Windows 10 rollout plans. It should be noted that a legacy risk was recorded in the Q2 DRR, with an aligned 'action controls' to risk assess the existing estate and increase investment for replacing outdated structures both with due dates of 31 December 2021.[176]

   iii. Define a minimum standard for legacy operating systems. For systems that must run on outdated operating systems, sufficient mitigation measures must be defined.

   iv. Define minimum standard requirements for OS of medical devices.

   v. Perform asset discovery activities to continually update asset lists.

Medium-term recommendations

1. **FA1.KR12 Appoint suitable long-term senior leadership for cybersecurity (a CISO) and establish a suitably resourced and skilled central cybersecurity function *(see strategic recommendation 3.1 in Section 4.1)*.** The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. They should be empowered to execute on a defined security vision, strategy and transformation to achieve sustainable cybersecurity risk reduction across the HSE. In line with this appointment the cybersecurity governance and operating model should be defined and subsequently resourced (ideally with burst capacity resources used during any interim periods that occur while recruitment takes place). This model should align to the three line of defence model. Responsibilities,

175 DRR Q2 2021, 19 November 2020
176 DRR Q2 2021, 19 November 2020

accountabilities, reporting lines and resourcing across the extended organisation of the HSE must all be defined. This includes within the HSE's cybersecurity and IT teams and between these central teams and those within its extended organisation.

2. **FA1.KR13 Deliver a multi-year cybersecurity transformation programme to build defence in depth over time and address root-cause issues *(see strategic recommendation 3.2 in Section 4.1).*** Investment is needed in a single programme of work delivered over the next two - four years to develop core cybersecurity capabilities in a sustainable manner over the short, mid and long term. We would propose this transformation is structured according to a two-track delivery model with dedicated resources and defined target states:

    a. **Tactical track** - the HSE should bring together red team experts and cybersecurity engineers to identify pragmatic fixes to the vulnerabilities and weaknesses identified. These should then be triaged between this tactical track and the strategic track for any longer term strategic activities. Within the tactical track each activity should be defined as being achievable within either 'two-week agile sprints' or '60-days work packages', to deliver rapid risk reduction by addressing exposure to specific attack techniques. Once the cybersecurity transformation programme is operational this track should absorb the tactical cybersecurity improvement programme.

    b. **Strategic track** - To build the sustainable and enabling foundations that deliver long-term reduction and mitigation of cyber risk, the HSE should define strategic work packages for activities that will take longer than 60 days to implement. This will include the medium recommendations made in this report. For improvements that are identified to be delivered strategically, suitable mitigations should be put in place in the short-term to reduce risk.

It would be typical for tactical and strategic track work packages to be defined across topics/work streams such as those shown in Figure 12:

Figure 12: Overview of key pillars in a cybersecurity transformation. This identifies elements that should be considered when scoping a cybersecurity transformation programme

IT Foundations	Security Foundations	Access Management
Improving the hygiene of an organisation's IT estate through tactical activities like enabling security features on the Active Directory and strategic initiatives like embedding good practice data retention, backup and recovery and patch management.	**Understanding business drivers and defining the structure and blueprints for security** through tactical activities like defining the technical boundary and strategic initiatives like designing the security strategy and frameworks for risk management and architecture.	**Securing identity and access** through tactical activities like cleaning up local admin accounts and strategic initiatives like onboarding critical accounts onto a PAM solution and setting up strong authentication & SSO.
Data Security	**Network Security**	**Threat Detection & Response**
Implementing protective and detective measures to secure critical data through tactical activities like restricting file share open access and strategic initiatives like data classification and data loss prevention capabilities.	**Monitoring network activity and improving protective capabilities** through tactical activities like reviewing and hardening key firewalls and strategic initiatives like implementing network segmentation and ONS Security.	**Identifying and setting up response capabilities for key threats** through tactical activities like developing priority detection content and strategic initiatives like enhanced security monitoring, crisis readiness and IoT/OT threat management.
Attack Surface Reduction	**End User Security**	**Security Culture**
Setting up a robust vulnerability management framework and processes through tactical activities like remediating priority vulnerabilities and strategic initiatives like defining secure configuration baselines and DevSecOps processes.	**Protecting the end user compute estate with in the environment** through tactical activities like limiting the use of MS Office macros and strategic initiatives like enhancing technical endpoint protection capabilities, and improving email threat mttigation.	**Improving security awareness** through tactical activities like training high risk users and strategic initiatives like designing and delivering security awareness and phishing campaigns.

For example, within the 'IT Foundations' work stream tactical work packages might include the remediation of stale data or extending the scope of the identity directory. Strategic work packages within this work stream could include decommissioning end of life systems or implementing an operational CMDB to maintain an updated list of all systems and applications in the environment.

3. **FA1.KR14 Plan the HSE's future IT transformation that reduces cybersecurity risk *(see strategic recommendation 2.2 in Section 4.1).*** The HSE's IT transformation lead should begin documenting and planning the future IT transformation. Executing an IT transformation will allow the HSE to sustainably reduce cybersecurity risk in the long-term, as issues within the legacy IT estate can be addressed,and cybersecurity and resilience can be built into the IT architecture.

4. **FA1.KR15 Design and implement a single and centralised security monitoring capability for the defined security boundary of the HSE that reports into the CISO *(see strategic recommendation 3.2 in Section 4.1).*** This should be for all monitoring aspects including network, server and workstation environments, as well as services such as email. Any reduction in the visibility of assets for monitoring should be risk-assessed to ensure that the HSE's ability to monitor its full environment is within risk appetite. This implementation should involve establishing the following across the three fundamental pillars of people, process and technology:

- **People** - Employing security monitoring and detection SMEs (either internally or through third parties) that are trained to identify and respond to threats detected within and across the HSE security boundary.
- **Process** - Ensuring that detection and response processes are documented. This includes incident playbooks that outline the step-by-step response actions to be taken, as well as documented responsibilities and accountabilities for reporting security events between organisations (such as voluntary hospitals and reporting bodies like the NCSC).
- **Tooling** - Deployment of modern endpoint detection and response tooling/endpoint protection platform tooling across the HSE environment and security boundary. This should be in addition to the implementation of a Security Incident and Event Manager ("SIEM") and Security Operations Centre ("SOC") to centrally analyse logs from systems and security tools.

Focus area 1 conclusion

The HSE was not sufficiently prepared to defend against or respond to a ransomware cyber attack. The HSE did not have sufficient subject matter expertise, resources or appropriate security tooling to detect, prevent or respond to a cyber attack of this scale and complexity. As a result, the attacker was able to enter the HSE environment and move around with relative ease and there were several missed opportunities to detect malicious activity, prior to the detonation phase of the ransomware.

Following the execution of ransomware, the HSE mobilised a response to overcome the significant challenges posed by both the attack and its lack of preparedness. Due to the scale and impact of the ransomware, paired with the complex and legacy IT environment, the technical recovery of IT systems was challenging. The timeframe for recovery could have been significantly longer had the decryption key not been sourced, as the HSE would have had to rely on recovering applications and systems from backups. The HSE would likely have encountered significant difficulties with this approach as the backup infrastructure was primarily designed to recover single systems only and not to recover multiple systems at scale and pace.

The focus of the HSE's activities since the attack has been on implementing recommendations provided by third parties and to continue to recover systems. A finalised cybersecurity improvement plan does not exist and limited evidence has been provided to show planning that will significantly and sustainably reduce the HSE's exposure to future ransomware attacks.