Conti cyber attack on the HSE

Independent Post Incident Review - Executive Summary and Learnings for Other Organisations

Commissioned by the HSE Board in conjunction
with the CEO and Executive Management Team

03 December 2021

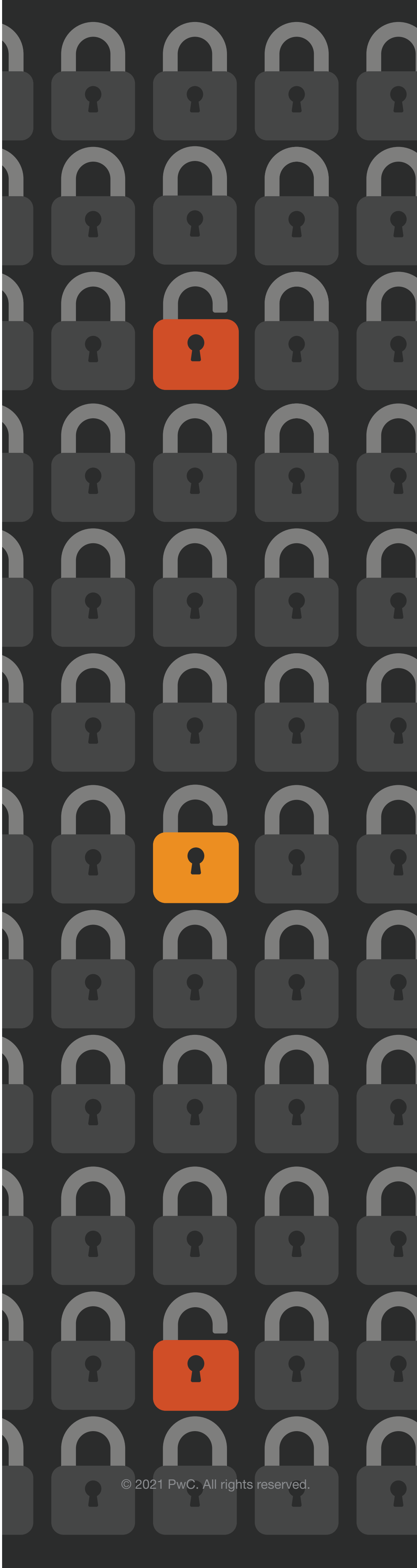
Redacted

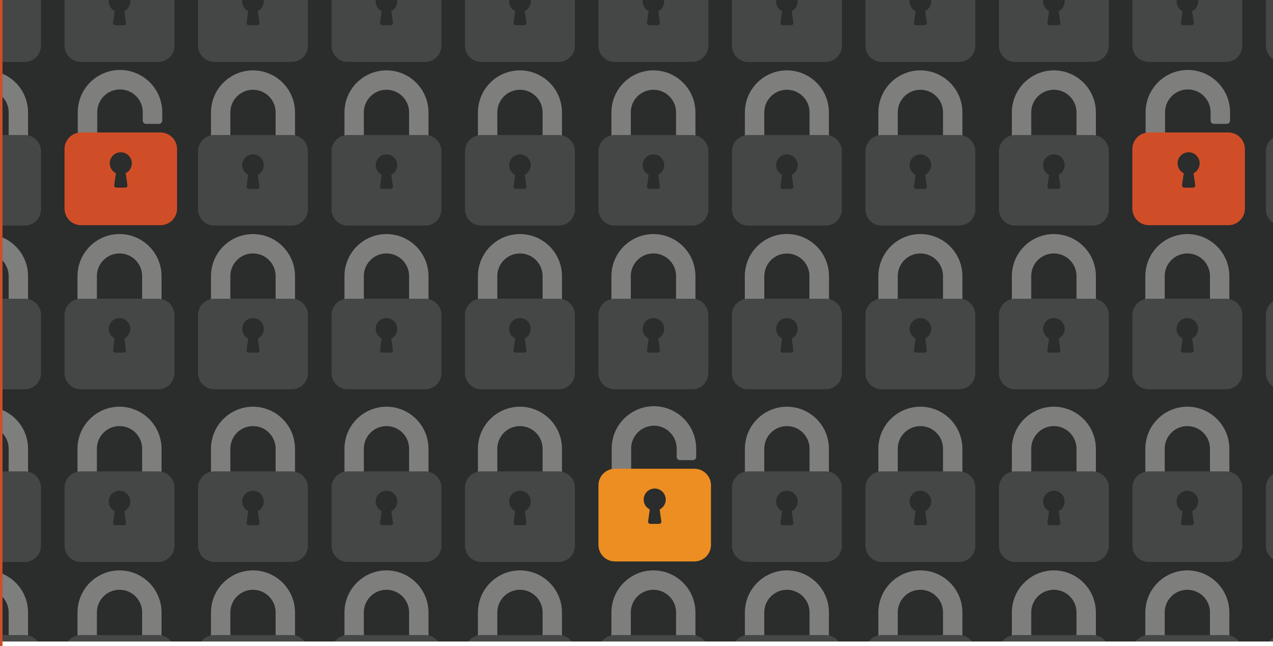
Important Notice

This document has been prepared only for the Health Services Executive ("HSE") and solely for the purpose and on the terms agreed with the HSE in our engagement letter dated 21 June 2021, as amended on 6 August 2021. We accept no liability (including for negligence) to anyone else in connection with this document.

The scope of our work was limited to a review of documentary evidence made available to us and interviews with selected HSE personnel, CHOs, hospitals and third parties relevant to the review. We have taken reasonable steps to check the accuracy of information provided to us but we have not independently verified all of the information provided to us relating to the services.

A significant volume of documentation was provided to us throughout the course of the review. We have limited our review to those documents that we consider relevant to our Terms of Reference. We cannot guarantee that we have had sight of all relevant documentation or information that may be in existence and therefore cannot comment on the completeness of the documentation or information made available to us. Any documentation or information brought to our attention subsequent to the date of this report may require us to adjust our report accordingly.





Contents

Redacted for security purposes.

The Board,
HSE,
Dr Steevens' Hospital,
Dublin 8, Ireland

03 December 2021

Subject : Post Incident Review into the Ransomware Cyber Attack

Dear Chair,

The Board of the Health Service Executive ("HSE") in conjunction with the Chief Executive Office ("CEO") and the Executive Management Team ("EMT") have requested an independent review into the recent ransomware cyber attack (the "Incident") and the circumstances surrounding this exfiltration of data from the HSE's Information Technology ("IT") systems. The purpose of the review is to:

- Urgently establish the facts in relation to the current preparedness of the HSE in terms of both its technical preparedness (Information and Communications Technology ("ICT") systems, cyber and information protections) and its operational preparedness (including Business Continuity Management planning) for a strategic risk of this nature.

- Identify the learnings from this Incident to identify improvements to the HSE's preparedness for and response to other major risks including immediate risks and incidents that cause major business disruption.

- Share those learnings within the HSE and externally with State and non-State organisations to inform their future preparedness.

Save as described in our contract or as expressly agreed by us in writing, we accept no liability (including for negligence) to anyone else or for any other purpose in connection with this report.

The subject matter and volume of information we reviewed as part of this process has been complex and significant in nature. Similarly, the timeline against which the review has been conducted has been challenging and has only been achieved with the cooperation of the many stakeholders involved, for which we are appreciative.

Yours faithfully,

PricewaterhouseCoopers

Executive summary

Background

The Health Service Executive ("HSE") is a large geographically spread organisation which provides all of Ireland's public health services through hospitals and communities across the country. The HSE consists of approximately 4,000 locations, 54 acute hospitals and over 70,000 devices (PCs, laptops, etc). Services are provided through both community delivered care and care provided through the hospital system as well as the national ambulance service. Corporate services and other services that support healthcare delivery are provided through the national centre.

The HSE is the largest employer in the Irish state, with over 130,000 staff including direct employees and those employed by organisations funded by the HSE[1]. It therefore comprises an extensive community who are increasingly dependent on connected and reliable Information Technology ("IT") solutions and varying levels of IT support from the HSE national centre to deliver clinical services. This includes the HSE's national IT infrastructure. The HSE is classified as a critical infrastructure operator under the EU Network and Information Security Directive ("NISD")[2], also known as an Operator of Essential Services ("OES").

Introduction to the Incident

In the early hours of Friday 14 May 2021, the HSE was subjected to a serious cyber attack, through the criminal infiltration of their IT systems (PCs, servers, etc.) using Conti ransomware. The HSE invoked its Critical Incident Process, which began a sequence of events leading to the decision to switch off all HSE IT systems and disconnect the National Healthcare Network ("NHN") from the internet, in order to attempt to contain and assess the impact of the cyber attack[3]. These actions removed the threat actor's (the "Attacker") access to the HSE's environment.

This immediately resulted in healthcare professionals losing access to all HSE provided IT systems - including patient information systems, clinical care systems and laboratory systems. Non-clinical systems such as financial systems, payroll and procurement systems were also lost. Significant disruption immediately occurred and many healthcare professionals had to revert to pen and paper to continue patient care. Healthcare services across the country were severely disrupted with real and immediate consequences for the thousands of people who require health services every day.

Normal communication channels, both at HSE's national centre and within operational services were also immediately lost. This included email and networked phone lines. Staff switched to communicating using mobile and analogue phones; fax; and face to face meetings.

The aim of the Attacker was to disrupt health services and IT systems, steal data, and demand a ransom for the non-publication of stolen data and provision of a tool to restore access to data they had encrypted.

The HSE initially requested the assistance of the Garda National Cyber Crime Bureau, the International Criminal Police Organisation ("Interpol") and the National Cyber Security Centre ("NCSC") to support the response. The ransomware created ransom notes with instructions on how to contact the Attacker. The Attacker also posted a message on an internet chat room on the dark web, with a link to several samples of data reportedly stolen from the HSE. The HSE and the Irish Government confirmed on the day of the attack that they would not pay a ransom[4].

The Incident had a far greater and more protracted impact on the HSE than initially expected, with recovery efforts continuing for over four months.[5]

Growing threat of cyber attacks

Cybercrime is increasing in frequency, magnitude and sophistication, with cybercriminals easily operating across jurisdictions and country borders. These incidents can cause major damage to safety and the economy[6]. As outlined in Ireland's National Cyber Security Strategy, 2019-2024, *"recent years have seen the development and regular use of very advanced tools for cyber enabled attacks and espionage, and, likely for the first time, the physical destruction of Critical National Infrastructure by cyber enabled means"*[7]. In April 2020, Interpol, warned that cybercriminals were targeting critical healthcare institutions with ransomware[8].

[1] Health Service Employment Report: August 2021

[2] This occurred in July 2016. See NIS Compliance Guidelines for Operators of Essential Service

[3] Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021

[4] https://www2.hse.ie/services/cyber-attack/how-it-may-affect-you.html

[5] Weekly Brief, 21 September 2021

[6] https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94

[7] National_Cyber_Security_Strategy.pdf

[8] https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

Ransomware attacks have risen significantly over the last few years. Whilst precise figures on the number of ransomware victims are not available, there are statistics that indicate the rate of growth of these attacks. For example, the US agency FinCEN's[9] analysis of ransomware-related Suspicious Activity Reports (SARs) filed during the first half of 2021 indicates that $590 million[10] was paid in ransomware-related transactions (likely representing payments originating from the US to ransomware groups), which exceeds the value reported for the entirety of 2020 ($416 million).

Despite claims by ransomware groups that they would not seek to harm people, there are several recent examples of attacks against healthcare providers. Hospitals including St. Lawrence Health System (USA), Sonoma Valley Hospital (USA), and Sky Lakes Medical Center (USA), all reported that they were impacted by ransomware attacks in 2020. On 20 May 2021, the Federal Bureau of Investigation ("FBI") identified at least 16 Conti ransomware attacks targeting US healthcare[11]. Healthcare organisations that have been the target of similar attacks this year include, Waikato District Health Board, New Zealand (May 2021), Eskenazi Health, USA (August 2021), Memorial Health System, USA (August 2021) and Macquarie Health Corporation, Australia (October 2021). More recently, much of the provincial healthcare system in Newfoundland was impacted by a cyber attack (November 2021). The ransomware attack against the HSE would appear to be the first occurrence of an entire national health service being impacted by such an attack.

Scope of our review

In June 2021, PwC was commissioned by the Board of the HSE, in conjunction with the Chief Executive Officer ("CEO") and the Executive Management Team ("EMT"), to conduct an independent post incident review ("PIR") to urgently establish the facts in relation to the HSE's technical and operational preparedness for an incident of this nature; and to identify the learnings from this Incident both for the HSE and for State and non-State organisations to inform their future preparedness. We initially undertook a scoping phase, to develop our understanding of the Incident and our approach to the review, followed by the PIR engagement which was conducted over a 14 week period.

We took a sample approach to review the involvement of the hospitals and Community Healthcare Organisations ("CHO") within the HSE's community, focusing on how the HSE's strategy was implemented at tactical levels and the effectiveness of the HSE's coordination of efforts.

This is a complex PIR. In recognition of this complexity, we brought together an experienced multi-disciplinary team of international cybersecurity and crisis management specialists. Our team included forensic investigation and response, IT / cybersecurity, crisis management, culture and behaviour, and regulatory experts with extensive experience in cybersecurity PIRs.

Timeline of the Incident

On 18 March 2021, the source of the cyber-attack[12] originated from a malicious software ("Malware") infection on a HSE workstation (the "Patient Zero Workstation"). The Malware infection was the result of the user of the Patient Zero Workstation clicking and opening a malicious Microsoft Excel file that was attached to a phishing email sent to the user on 16 March 2021.

After gaining unauthorised access to the HSE's IT environment on 18 March 2021, the Attacker continued to operate in the environment over an eight week period until the detonation of the Conti ransomware on 14 May 2021. This included compromising and abusing a significant number of accounts with high levels of privileges (typically required for performing administrative tasks), compromising a significant number of servers, exfiltrating data and moving laterally to statutory and voluntary hospitals.

The Incident was not identified and contained until after the detonation of the Conti ransomware on 14 May 2021, which caused widespread IT disruption. There were several detections of the Attacker's activity prior to 14 May 2021, but these did not result in a cybersecurity incident and investigation initiated by the HSE and as a result opportunities to prevent the successful detonation of the ransomware were missed. The key events from 18 March 2021 to 14 May 2021 are set out in the diagram overleaf.

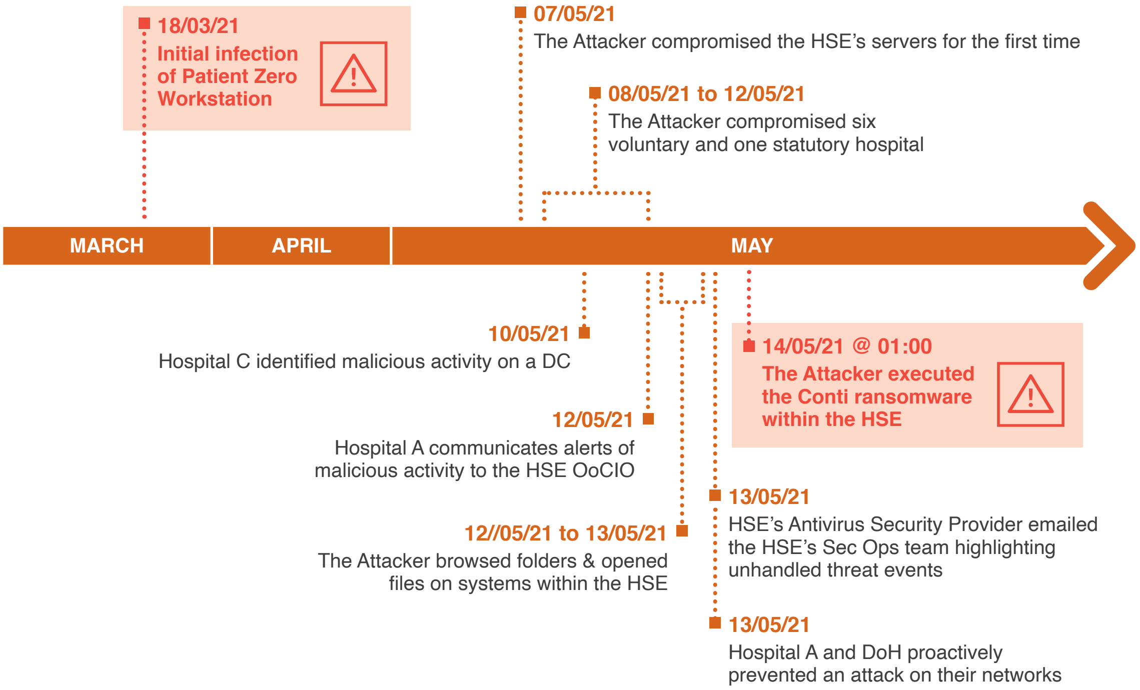
[9] www.fincen.gov

[10] https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

[11] https://www.ic3.gov/Media/News/2021/210521.pdf

[12] HSE's Incident Response provider Intrusion Investigation Report, September 2021

Figure 1: Summary Timeline 18 March - 14 May 2021



18/03/21
Initial infection of Patient Zero Workstation

07/05/21
The Attacker compromised the HSE's servers for the first time

08/05/21 to 12/05/21
The Attacker compromised six voluntary and one statutory hospital

10/05/21
Hospital C identified malicious activity on a DC

12/05/21
Hospital A communicates alerts of malicious activity to the HSE OoCIO

12//05/21 to 13/05/21
The Attacker browsed folders & opened files on systems within the HSE

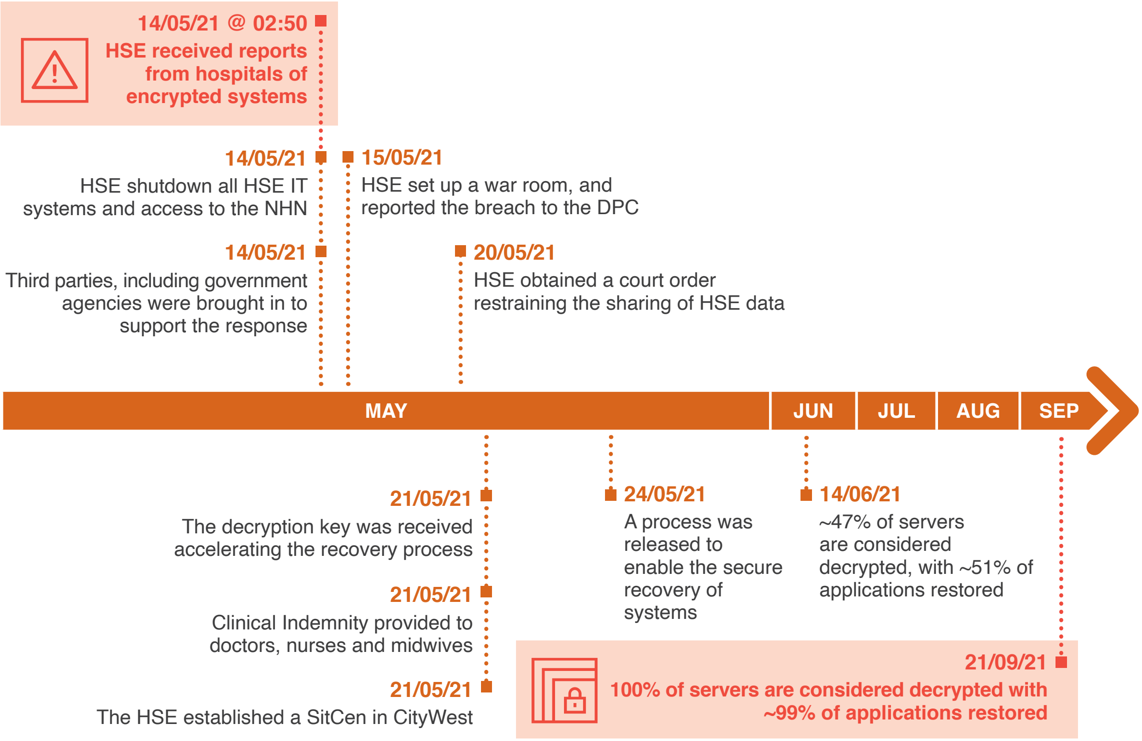
14/05/21 @ 01:00
The Attacker executed the Conti ransomware within the HSE

13/05/21
HSE's Antivirus Security Provider emailed the HSE's Sec Ops team highlighting unhandled threat events

13/05/21
Hospital A and DoH proactively prevented an attack on their networks

In the early hours of 14 May 2021, the HSE identified that they had been a victim of a cyberattack and they began to mobilise a response, drawing on their experiences from previous crises, including COVID-19. The key response and recovery events from 14 May 2021 are set out in the diagram below.

Figure 2: Summary Timeline 14 May - 21 September 2021



14/05/21 @ 02:50
HSE received reports from hospitals of encrypted systems

14/05/21
HSE shutdown all HSE IT systems and access to the NHN

14/05/21
Third parties, including government agencies were brought in to support the response

15/05/21
HSE set up a war room, and reported the breach to the DPC

20/05/21
HSE obtained a court order restraining the sharing of HSE data

21/05/21
The decryption key was received accelerating the recovery process

21/05/21
Clinical Indemnity provided to doctors, nurses and midwives

21/05/21
The HSE established a SitCen in CityWest

24/05/21
A process was released to enable the secure recovery of systems

14/06/21
~47% of servers are considered decrypted, with ~51% of applications restored

21/09/21
100% of servers are considered decrypted with ~99% of applications restored

The HSE was assisted by the Defence Forces and the NCSC as well as third parties in the early weeks of the Incident, to provide structure to the response activities. The response teams could not initially focus on the highest priority response and recovery tasks due to the lack of preparedness for a widespread disruptive IT event e.g. through not having a pre-prepared list of prioritised clinical systems and applications to focus their efforts.

On 15 May 2021, the HSE senior management set up a war room at a third party's office building on Molesworth Street. On 20 May 2021, the Defence Forces attended Molesworth Street for further discussions around the level of support that was required by the HSE during the response and recovery phases of the Incident and on 21 May 2021, the HSE set up a physical situation centre ("SitCen") in CityWest to manage the response and recovery. The HSE engaged a third party Incident Response organisation ("HSE's Incident Response provider") to investigate the cyber attack.

On 20 May 2021, the HSE secured a High Court injunction[13] restraining any sharing, processing, selling or publishing of data stolen from its computer systems. On the same day, the Attacker posted a link to a key that would decrypt files encrypted by the Conti ransomware. The HSE's Incident Response provider validated that the decryption key worked on 21 May 2021 and provided it to the HSE, allowing them to gain access to the data that had been encrypted by the Conti ransomware. Without the decryption key, it is unknown whether systems could have been recovered fully or how long it would have taken to recover systems from backups, but it is highly likely that the recovery timeframe would have been considerably longer.

From 22 May 2021 onward, the HSE Information and Communications Technology ("ICT") team moved from the response phase into the recovery phase, where they focused their efforts on decrypting systems, cleansing workstations, restoring systems and the recovery of applications. The HSE recovered their primary identity systems ([redacted] Active Directory ("AD") domain) within days of the Incident, but decryption of servers and acute and community services applications took place largely over the following three months. By 21 September 2021, the HSE had recovered all servers and 1,075 applications, out of a total of 1,087 applications[14].

At the time of issuing this report, the HSE had notified the Data Protection Commissioner ("DPC") in relation to the Incident, however, they have not made any data subject notifications for personal data exposure or exfiltration. The HSE's Legal and Data workstream continues to work closely with the DPC in relation to this matter.

Mitigating factors impacting on the Incident

There were a number of mitigating factors which had a considerable effect in reducing the severity and impact of the Incident.

Relative simplicity of the attack and the release of the decryption key

Based on the forensic examination of the Attacker's activity, it would appear that the Attacker used relatively well-known techniques and software to execute their attack. A more sophisticated attack may have involved gathering intelligence in advance, before it could be successfully and subtly exploited. The impact of the Incident on the HSE and health services could have been significantly greater, with far more severe clinical impact. Some examples of this include, but are not limited to:

- if there had been intent by the Attacker to target specific devices within the HSE environment (e.g. medical devices);
- if the ransomware took actions to destroy data at scale;
- if the ransomware had auto-propagation and persistence capabilities, for example by using an exploit to propagate across domains and trust-boundaries to medical devices (e.g. the EternalBlue exploit used by the WannaCry and NotPetya[15] attacks);
- if cloud systems had also been encrypted such as the COVID-19 vaccination system.

An additional mitigating factor was the release of the decryption key by the Attackers on 20 May 2021, which allowed for an accelerated recovery process. It is unclear how much data would have been unrecoverable if a decryption key had not become available as the HSE's backup infrastructure was only periodically backed up to offline tape. Therefore it is highly likely that segments of data for backup would have remained encrypted, resulting in significant data loss. It is also likely to have taken considerably longer to recover systems without the decryption key.

[13] https://www.hse.ie/eng/services/publications/order-perfected-20-may-2021.pdf
[14] Weekly Brief, 21 September 2021
[15] https://us-cert.cisa.gov/ncas/alerts/TA17-181A

Significant 'in-the moment' efforts in response to the Incident

A recurring theme observed throughout the PIR was the dedication and effort observed at all levels during the response to the Incident. This included individuals from across the HSE, impacted hospitals, CHOs, and third parties all going "above and beyond" in their call of duty. This illustrates that, in times of significant challenge or emergencies, staff in the health services are resilient, respond quickly, and have an ability to implement actions and workarounds to maintain even a basic continuity of service to their patients.

National support

The impact of the Incident was at a national scale which encouraged support and presence from other state agencies and third parties, who provided structure, governance, technical expertise and resources to assist the response and recovery.

Lessons learned from COVID-19 and previous IT disruptions

Whilst the HSE had not previously encountered an incident of this scale, they have been exposed to other significant incidents both directly (e.g COVID-19) and through observations of ransomware attacks on other healthcare organisations globally (e.g WannaCry ransomware attack) over the past five years. Each of these incidents highlighted key learnings that have led to an improved level of crisis management maturity within the HSE.

Strategic recommendations and findings

The Incident demonstrated that the HSE and organisations connected to the NHN are vulnerable to common cyber attacks that can cause significant impact to the provision of health services. Transformational change is required across the technology foundation for provision of health services and its associated cybersecurity, that will need to be executed over the coming years.

In order to deliver a significant and sustainable change in the exposure to cybersecurity risk, four areas of strategic focus are required across the HSE and other parties connected to the NHN. There are dependencies across these four areas and they need to be progressed in parallel. They are summarised below, with further detail provided in Section 4.1. More detailed findings and recommendations are provided in Section 5.

1. Implement an enhanced governance structure over IT and cybersecurity that will provide appropriate focus, attention and oversight.

1.1 Establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, share health data or access shared health services. Establish a 'code of connection' that sets minimum cybersecurity requirements for all parties and develop an assurance mechanism to ensure adherence.

One of the challenges faced by the HSE is that cybersecurity risk materialises as a 'common risk' to all organisations connected to the NHN given the interconnected nature of the IT systems. Under the governance constructs of the health service, organisations have varying levels of autonomy over IT and cybersecurity decision making, yet the risk is shared - with organisations dependent on each other for cybersecurity. There is no 'code of connection' for all parties that connect to the NHN, share health data or use shared services in order to set a minimum baseline of security standards.

1.2 Establish an executive level cybersecurity oversight committee to drive continuous assessment of cybersecurity risk and a cybersecurity transformation programme across the provision of health services.

Within the HSE, there is no dedicated executive oversight committee that provides direction and oversight to cybersecurity, both within the HSE and all organisations connected to the NHN. A known low level of cybersecurity maturity, including critical issues with cybersecurity capability, has persisted. It is important that the cybersecurity oversight committee includes participation from user groups, so that culturally cybersecurity moves from being perceived as an IT challenge, to being perceived as 'how we work'. The cybersecurity oversight committee should be accountable for ensuring compliance with the evolving requirements of the EU NISD for essential services across the health service.

1.3 Establish an executive level oversight committee for IT.

With a fragmented set of decision rights over IT development and support across the provision of health services, a necessary enabler for driving transformational change will be the establishment of an executive level committee, chaired by the Chief Technology and Transformation Officer (see Recommendation 2 below), that can agree the priorities for IT development and investment, and align all interested parties behind a clear vision, strategy and plan. Critical to its success will be the participation of IT leaders from across the health service.

1.4 Establish a board committee (or repurpose an existing one) to oversee the transformation of IT and cybersecurity to deliver a future-fit, resilient technology base for provision of digitally-enabled health services, and ensure that IT and cybersecurity risks remain within a defined risk appetite. Consider the inclusion of further specialist non-executive members of the committee in order to provide additional expertise and insight to the committee.

Cybersecurity was recorded as a 'High' risk in the Corporate Risk Register in Q1 2019.[16] At the time of the Incident, the risk rating for cybersecurity on the Corporate Risk Register was 16, based on a likelihood scoring of 4 (likely, with a 75% probability) and an impact scoring of 'Major'.[17] The HSE's risk assessment tool is described in Appendix H.

Risks on the Register are subject to a quarterly review process and the quarterly reports are reviewed by the relevant Board Committee. The Performance and Delivery Committee of the Board reviewed the cyber risk with management in September 2020[18] and this was followed by a revised mitigation plan. The Committee includes two experienced IT leaders in large organisations, although they are not cybersecurity specialists. This revised mitigation plan had a number of actions due to be completed post the date of the Incident. The actions completed prior to the Incident did not materially impact the risk faced in this area.

The HSE's IT-related risks had been presented at Board level on a number of occasions. However, the gravity of cybersecurity exposure was not fully articulated to the Board, given the HSE's level of vulnerability to a cyber attack, or assessed against a defined risk appetite. Known issues with cybersecurity capability have made limited progress over the course of several years.

Given the scale of change required across the provision of health services, it is recommended that a focused committee of the board is established, with relevant training provided. Consideration should be given to appointing additional individuals to that committee with specialist skills to act in a non-executive capacity and enhance the ability for the committee to support and oversee the IT and cybersecurity transformation. A key role for the committee will be to ensure that HSE requests for government funding (e.g. to the Department of Public Expenditure and Reform ("DPER")) to invest in addressing IT and cybersecurity issues are clearly articulated, and the risks associated with lack of investment are communicated and understood.

2. Establish a transformational Chief Technology & Transformation Officer ("CTTO") and office to create a vision and architecture for a resilient and future-fit technology capability; to lead the delivery of the significant transformation programme that is required, and to build the increased function that will be necessary to execute such a scale of IT change.

The national health service is operating on a frail IT estate with an architecture that has evolved rather than be designed for resilience and security. The NHN is primarily an unsegmented (or undivided) network, and can be described as a "flat" network, to make it easy for staff to access the IT applications they require. However, this design exposes the HSE to the risk of cyber attacks from other organisations connected to the NHN, as well as exposing other organisations to cyber attacks originating from the HSE. This network architecture, coupled with a complex and unmapped set of permissions for systems administrators to access systems across the NHN, enabled the Attacker to access a multitude of systems across many organisations connected to the NHN and create the large-scale impact that they did.

The parts of the health service that were arguably best-equipped to maintain clinical services in the face of prolonged IT outages were those that rely on paper records for patient services. Whilst this was a positive feature in managing the Incident, it highlights the extent to which modernisation is required across the health service to enable the adoption of digital health services.

Reducing cybersecurity risk requires both a transformation in cybersecurity capability (see recommendation 3) and IT transformation, to address the issues of a legacy IT estate and build cybersecurity and resilience into the IT architecture.

2.1 Appoint a permanent CTTO with the mandate and authority to develop and execute a multi-year technology transformation, build an appropriate level of IT resource for an organisation the scale of the HSE and oversee the running of technology services.

The HSE has operated since the end of 2018 with an interim Chief Information Officer with limited

[16] Q1, 2019 CRR COMBINED Document for April LT meeting.pdf
[17] CRR Q4 2020 Full Report post EMT meeting February 2021 v0.1 09 02 21.pdf
[18] Minutes-hse-performance-and-delivery-committee-18-september-2020.pdf

practical mandate, authority and resources to effect change across all organisations connected to the NHN. The level of resourcing in critical IT functions is significantly lower than we would expect for an organisation of this size.

The CTTO should assume responsibility for all capabilities that currently sit within the Office of the Chief Information Officer ("OoCIO"), as well as a broadened capability to drive rapid transformation. The CTTO should be a member of the EMT reporting to the CEO.

2.2 Under the office of the CTTO, develop an IT strategy to achieve a secure, resilient and future-fit IT architecture, required for the scale of the HSE organisation.

The HSE has had a plan for the development of IT that has been used to secure funding for individual projects. However it has not been tied to a vision, strategy and architecture that is deliverable over a period of years and that provides the necessary level of resilience through investment in enabling IT architecture and fallback solutions in the event of core technology failure. Many interviewees expressed frustration with an apparent approach of investing in 'new projects' or 'new features' rather than the holistic delivery and maintenance of a technology foundation for health service provision.

In order to deliver the transformation required, a clear strategy is required that can be used to secure commitment to execution across all organisations involved in the provision of health services, and the significant funding that will be required over many years.

3. Appoint a Chief Information Security Officer ("CISO") and establish a suitably resourced and skilled cybersecurity function. Develop and drive the implementation of a cybersecurity transformation programme.

The HSE has a very low level of cybersecurity maturity (Section 5.3 of this report gives an evaluation of maturity against the industry standard "NIST CSF" framework). Examples of the lack of cybersecurity controls in place at the time of the Incident include:

- The IT environment did not have many of the cybersecurity controls that are most effective at detecting and preventing human-operated ransomware attacks;
- There was no security monitoring capability that was able to effectively detect, investigate and respond to security alerts across HSE's IT environment or the wider NHN;
- There was a lack of effective patching (updates, bug fixes etc.) across the IT estate that is connected to the NHN; and
- Reliance was placed on a single antivirus product that was not monitored or effectively maintained with updates across the estate. For example, the workstation on which the Attacker gained their initial foothold did not have antivirus signatures updated for over a year.

The low level of cybersecurity maturity, combined with the frailty of the IT estate, enabled the Attacker in this Incident to achieve their objectives with relative ease. The Attacker was able to use well-known and simple attack techniques to move around the NHN, extract data and deploy ransomware software over large parts of the estate, without detection.

3.1 Appoint a CISO and establish a suitably resourced and skilled cybersecurity function

The HSE does not have a single responsible owner for cybersecurity at either senior executive or management level to provide leadership and direction. This is highly unusual for an organisation of the HSE's size and complexity with reliance on technology for delivering critical operations and handling large amounts of sensitive data. As a consequence, there was no senior cybersecurity specialist able to ensure recognition of the risks that the organisation faced due to its cybersecurity posture and the growing threat environment.

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. Whilst recruitment of a permanent CISO may take some time, appointment of an interim CISO should be considered in the short term.

The HSE also had only circa 15[19] full-time equivalent ("FTE") staff in cybersecurity roles, and they did not possess the expertise and experience to perform the tasks expected of them.

[19] 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.

A critical requirement for the HSE to begin to develop the ability to prevent and detect a similar incident in the future is the appointment of senior cybersecurity leadership and the development of a suitably skilled and resourced cybersecurity function. These skilled resources are currently scarce and the HSE may need to consider co-sourcing arrangements to support resource requirements in this area.

3.2 Develop and drive the execution of a multi-year cybersecurity transformation programme to deliver an acceptable level of cybersecurity capability for a national health service.

A multi-year programme to transform cybersecurity capability in a holistic way is required to be led by the CISO, to ensure that the provision of health services in Ireland, and the data that those health services handle, becomes less vulnerable to cyber attacks. This programme will include the formalisation of cybersecurity training and awareness.

Implement a clinical and services continuity transformation programme reporting to the National Director for Governance and Risk, and enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT.

4.1 Implement a clinical and services continuity transformation programme reporting to the National Director for Governance and Risk. Establish an Operational Resilience Policy and Resilience Steering Committee to drive integration between resilience-related disciplines, and an overarching approach to resilience.

The HSE has recognised that clinical and services continuity (business continuity) as a risk discipline has not developed at the pace needed with executive oversight and focus. A National Director for Governance and Risk (equivalent to a Chief Risk Officer) was appointed on 14 June 2021, and assigned responsibility for establishing a clinical and services continuity framework, through which risk management and continuity plans will be reviewed, maintained and validated. Responsibility for clinical and service continuity under the HSE's accountability structure will remain with operational and functional managers. A programme and resource is required to develop the consistency and breadth of planning across the health service, including establishing clear requirements for disaster recovery capability to be implemented by the IT transformation programme, and the mapping of clinical processes to IT systems and data.

The HSE should establish an Operational Resilience Policy and Steering Committee to drive integration between resilience-related disciplines across the organisation, such as incident management, crisis management, clinical and services continuity and enterprise risk management plus disciplines that can impact on resilience such as cybersecurity and physical security.

4.2 Enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT.

The HSE has extensive experience in managing crises, for example in the critical role it has fulfilled for the nation in navigating the COVID-19 crisis. This has resulted in some effective mechanisms for crisis management not just being designed, but regularly used.

However, the nature of the crisis resulting from the ransomware attack was different, and required elements of capability that have not previously been required. For example: communicating with all staff in the health service without internal emails or other IT collaboration tools; establishing a wide variety of communication channels and forums to gather information and feedback to prioritise recovery of systems, and issuing clear guidance to all parties impacted by the Incident that was relevant to their localised situation.

The nature of a ransomware attack, resulting in effectively total loss of IT, makes it particularly challenging to manage with a unique set of issues to be navigated. Investment is required in crisis management planning, resourcing and tools and processes in the HSE and associated organisations in order to be prepared to manage this kind of crisis in the future.

Tactical recommendations

Given the high risk of exposure at present, below are tactical recommendations which require immediate attention to achieve urgent impact and to contribute to the development and implementation of the strategic recommendations. These recommendations are described in more detail in Section 4.2 of this report. Further detail of key findings and recommendations are included in Section 5 of this report.

1. Response to the Incident

1.1. Complete the ongoing work being performed by the Legal and Data workstream and continue to work closely with the Data Protection Commissioner (DPC).

1.2. Continue to reconcile medical data stored and managed through interim processes post the ransomware attack and place centralised governance over these activities.

1.3. Collate and manage artefacts created in response to the Incident, including initial production of an asset register.

1.4. Appoint an interim senior leader for cybersecurity (a CISO) to be responsible for driving forward tactical cybersecurity improvements, managing third-parties that provide cybersecurity services and leading the cybersecurity response to cyber incidents.

1.5. Formalise a programme and governance to respond to tactical recommendations arising from the Incident Response investigation and provide assurance over their implementation.

2. Security monitoring

2.1. Ensure that the HSE's Incident Response provider's managed defence service or an equivalent is maintained to detect and respond to incidents on endpoints (i.e. laptops, desktops, servers etc.) to provide protection to the entirety of the NHN.

2.2. Establish an initial cybersecurity incident monitoring and response capability to drive immediate improvement to the ability to detect and respond to cybersecurity events.

3. Ability to respond to a similar incident in the near future

3.1. Review the process for managing internal crisis communications including resources.

3.2. Develop a plan for response and management of an NHN-wide similar incident taking recent learnings into account.

3.3. Establish retainers with appropriate service level agreements ("SLAs") for third party incident and crisis management response support, together with processes and sufficient internal expertise to direct and manage the third-parties

4. IT environment

4.1. Implement an upgrade to National Integrated Medical Imaging System ("NIMIS") to allow Windows 10 upgrade, thereby addressing known vulnerabilities and support issues associated with current wide deployment of Windows 7.

4.2. Formalise existing roles and responsibilities for IT across the entities accessing the NHN and establish SLAs for centrally-provided services, while also ensuring information security policies align with those responsibilities.

Next Steps

The seriousness of the deficiencies identified persist and necessitate transformational change in the HSE as well as immediate tactical actions. We recommend that the HSE improve their cybersecurity, IT and operational resilience governance, leadership and capability, to allow them to stand up a remediation programme to address our recommendations.

In 2021, the HSE had a combined revenue and capital budget of nearly €22 billion, which included an IT operating budget of €82 million and IT capital budget of €120 million (including €25 million for Covid-19 capital spend)[20]. The HSE is currently estimating its IT operating budget will increase to €140m and its IT capital budget will increase to €130m in 2022. Whilst it is outside the scope of the PIR to quantify the incremental cost to the HSE of implementing the recommendations set out in this report, it is clear that it will require a very significant investment on an immediate and sustained basis.

The HSE will need to develop an investment case for this remediation programme, as the successful implementation of the strategic and tactical recommendations will be dependent on a well resourced plan, against which funding will need to be secured and progress tracked. This will be a complex programme, with interdependencies between our recommendations, and the programme will also need to be highly integrated with existing project delivery and business as usual operations. The investment case will be complex to develop due to for example: i) it can be challenging to segregate core IT spend and cybersecurity investment (e.g. upgrading to Windows 10 or Individual Health Identifier); ii) costs to release and backfill service staff i.e. clinical and operational subject matter experts who are critical to complex e-health projects, will be a relevant cost of the remediation programme and this will need to be incorporated into the investment commitment; and iii) a significant number of cybersecurity and clinical and service continuity resources need to be put in place, to deliver on the execution of the plan.

[20] HSE National Service Plan 2021

The cost of the remediation programme, in addition to underlying technology and operational resilience costs, is likely to be a multiple of the HSE's current capital and operating expenditure in these areas over several years. Our recommendations need to be developed into a prioritised plan, with tactical recommendations implemented on an accelerated basis. On the basis of this plan, cost estimates for year one can be established with a reasonable level of accuracy. Subsequently, within the first year, high level cost estimates for years 2-5 can be estimated (possibly over a longer duration, depending on interdependencies with other change programmes).

Learnings for other organisations

A number of the vulnerabilities that the ransomware attack highlighted are not unique to the HSE, and issues identified in this report will be found in other organisations. All organisations therefore need to consider the extent to which they are protected from a major cyber incident, and be prepared to respond and recover should they experience such an event. We have outlined these recommendations in Section 1 of this report.

Conclusion

While reviews of this nature tend to focus on what went wrong to identify learnings, it is also important to recognise that the Incident was caused by an Attacker and the HSE was the victim of a cybercrime. There was a considerable effort made by personnel, including IT and operations personnel in HSE centre, the hospitals and CHOs, and healthcare professionals in all areas, to respond to the Incident, to recover from the Incident and to continue to provide patient care throughout the Incident. If this significant effort had not been made by these people, the impact of the Incident on the Irish public healthcare system would certainly have been much worse.

The HSE is operating on a frail IT estate that has lacked the investment over many years required to maintain a secure, resilient, modern IT infrastructure. It does not possess the required cybersecurity capabilities to protect the operation of the health services and the data they process, from the cyber attacks that all organisations face today. It does not have sufficient subject matter expertise, resources or appropriate security tooling to detect, prevent or respond to a cyber attack of this scale. There were several missed opportunities to detect malicious activity, prior to the detonation phase of the ransomware.

The relative disadvantage in this Incident for organisations who have greater dependency on technology services, illustrates the critical need for resiliency to be built into the IT architecture and systems, to foster the confidence required to enable future migration to more digital provision of health services.

Emergency and crisis planning at the HSE previously focused on scenarios such as adverse weather, pandemic, serious accidents and terrorist action, which generate a temporary surge in demand for acute services. The assumption was that all critical infrastructure and processes would remain available to support the response. Similar to many other organisations, the HSE did not conduct contingency planning for a cyber attack or any other scenario involving the complete loss of infrastructure, people, or facilities. Clinical and services continuity has not been a corporate priority in the HSE until recently. In order to maximise the learnings from the response to the Incident, the HSE must expand upon initiatives already started, and implement a coherent operational resilience capability, including clinical and services continuity and crisis management, across the organisation.

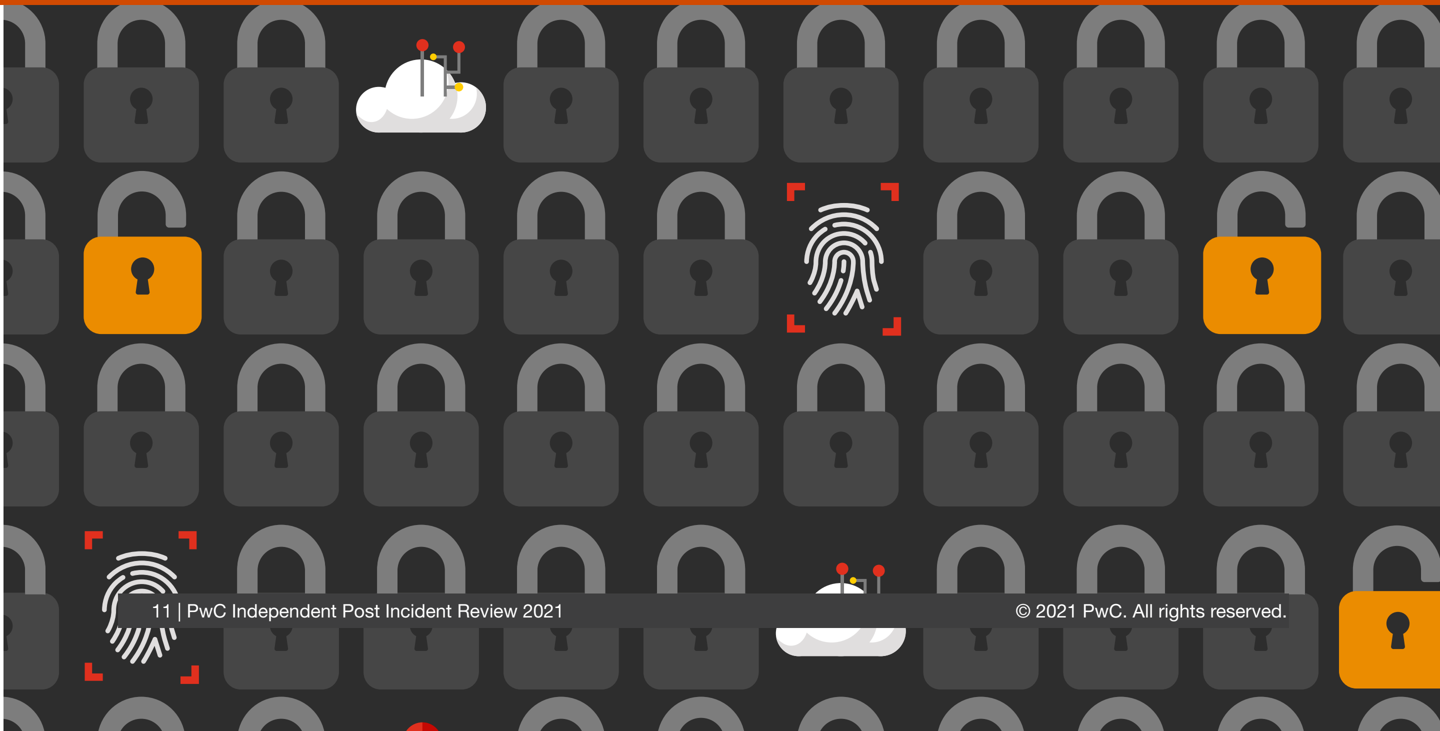
Reducing cybersecurity risk requires both a transformation in cybersecurity capability and IT transformation, to address the issues of a legacy and complex IT estate and build cybersecurity and resilience into the IT architecture. Whilst this will need to be executed over a period of several years, there is an imperative for the HSE to act with urgency to ensure that the necessary plans, vision, leadership, committed investment and resourcing are in place to drive this significant change to build a secure, resilient and future-fit technology foundation for provision of national healthcare services. The required investment commitment is likely to be a multiple of the HSE's current expenditure on technology and operational resilience, but is essential to protect the HSE against future attacks which are inevitable and have the potential to be even more damaging.

The HSE, the State and non-State organisations now have an opportunity to take the key lessons from this major Incident to build a more robust and resilient cyber frontier nationally.

The HSE remains vulnerable to cyber attacks similar to that experienced in the Incident, or cyber attacks that may have an even greater impact.

1 Learnings

Whilst the purpose of this report is to highlight recommendations and findings specific to the HSE to be taken from the Incident, there are a number of recommendations and key learnings that can be applied to all organisations.



As dependency on technology deepens across society, the impact of destructive cyber attacks such as ransomware will undoubtedly grow even further. Investing in cybersecurity needs to be a priority even for organisations that previously have not considered cyber attacks as a threat to their operations. A number of the vulnerabilities that the ransomware attack highlighted are not unique to the HSE, and issues identified in this report will also be found in many other organisations. All organisations therefore need to consider the extent to which they are protected from a major cyber incident, and be prepared to respond and recover should they experience such an event.

The points below are presented as recommendations that all organisations should consider in the light of the experience of the HSE, in order to learn lessons from this Incident more broadly. They are not intended to be exhaustive, but act as an instructive set of learnings to consider in response to this Incident.

Governance and cybersecurity leadership

1. Understanding of technology dependency and governance of technology risk

Boards and executive leadership of organisations should ensure that they understand the extent to which their critical operations are dependent on technology. Governance must ensure that risks associated with technology are properly understood and actively managed, including the resiliency of the organisation to widespread technology failure or compromise from an attack (which may occur indirectly through the supply chain). Governance over technology should ensure that sufficient investment is focused on: maintenance of robust foundational technology infrastructure; realising opportunities from new technology (such as infrastructure and applications in the cloud) to manage risks in a new way, and managing risks that arise from new application of technology.

2. Cybersecurity strategy and leadership

Organisations should ensure they have a cybersecurity strategy that defines the key cybersecurity risks to the organisation, how those risks are being mitigated and the resourcing and investment to execute the strategy. Organisations should have a single accountable senior leader responsible for delivering the strategy. An element of the strategy should be consideration of the cyber risk posed by legacy IT, how this risk can be mitigated in the short-term, and how technology modernisation will address the root-cause issue.

Effective cybersecurity capability

3. Ransomware-specific assessment

Organisations should perform a cybersecurity assessment specific to the threat of ransomware, given the heightened threat posed by ransomware attacks. This will highlight the extent to which the organisation's cybersecurity controls are appropriate and effective to defend against this threat, and identify areas that may require urgent investment.

Key examples of cybersecurity controls that should be assessed include: sufficiency of security monitoring to detect and contain ransomware attacks in the early stages, ability to prevent and detect the compromise of 'privileged' (e.g. systems administrator) accounts, and the robustness of user authentication.

Several organisations that provide ransomware-response services can provide such assessments, and publicly available frameworks and guidance are available from organisations such as the Cybersecurity & Infrastructure Security Agency ("CISA") in the USA.

4. Effective cybersecurity monitoring and response

Organisations must possess an effective security monitoring capability that can detect and respond to the tools and techniques used by human-operated ransomware groups. This should include deploying a capable 'Endpoint Detection & Response' tool to detect and prevent malicious activity on workstations (fed by current cyber threat intelligence) and ensuring the development of skilled resources and processes so that security alerts are rapidly triaged, investigated and responded to.

5. Testing of cybersecurity capability through simulated attacks

Testing of cybersecurity capability through the use of ethical hackers simulating end-to-end attack techniques (i.e. 'red team' testing) is essential to provide a threat- based perspective of an organisation's vulnerability to ransomware and other types of attacks. This can be used to rapidly identify and prioritise key security improvement areas and ensure that the organisation can effectively detect common attacker tools, with the necessary people and processes are in place to investigate and respond to alerts.

Preparedness to respond and recover

6. Cybersecurity-specific incident response and crisis management plans

Organisations should develop and exercise cybersecurity-specific incident response and crisis management plans that define how a response should be led, managed and coordinated. These should be challenged to ensure they are effective in a catastrophic ransomware scenario where all IT platforms, cybersecurity tools and usual communication channels are unavailable, and recovery efforts may have to be sustained for weeks or months.

7. Business continuity planning and IT disaster recovery planning for a ransomware scenario

Organisations should prioritise business continuity planning and disaster recovery planning that would ensure provision for continuity of critical operations and the ability to recover in the face of a ransomware attack that results in total loss of IT and associated data.

Business continuity planning should be based on rigorous 'Business Impact Analysis', and ensure that workarounds are defined for the scenario of total loss of IT for up to several weeks.

Organisations' IT disaster recovery plans should be based on a prioritised list of applications and systems to recover, should the technology base of the organisation have to be rebuilt or recovered, informed by an up-to-date asset register and mapping of critical operations to technology. Offline backups (or backups that are verified as inaccessible to attackers with full control of production IT) must be available for all critical systems, data and infrastructure, including core IT infrastructure such as Active Directory ("AD"), with a well-defined and tested restore procedure that includes verification of ability to recover all systems to a common point-in-time.

8. Retained incident and crisis support

Organisations should establish contractual retainers with key third parties that may be required to support a crisis response. Third party support that may likely be required during an incident include: forensic and technical incident response; crisis response; external legal counsel, and public relations.

Retainers should include: service level agreements; specification of third party roles and responsibilities; reviews of the technical preparedness of the organisation for incident response (by forensic and technical incident response providers), and pre-agreed legal requirements (such as non-disclosure agreements). These will ensure that partners can be engaged to support, and be integrated into, a response immediately and scale to the size of the response required.