Conti cyber attack on the HSE

Independent Post Incident Review

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

03 December 2021

pwc

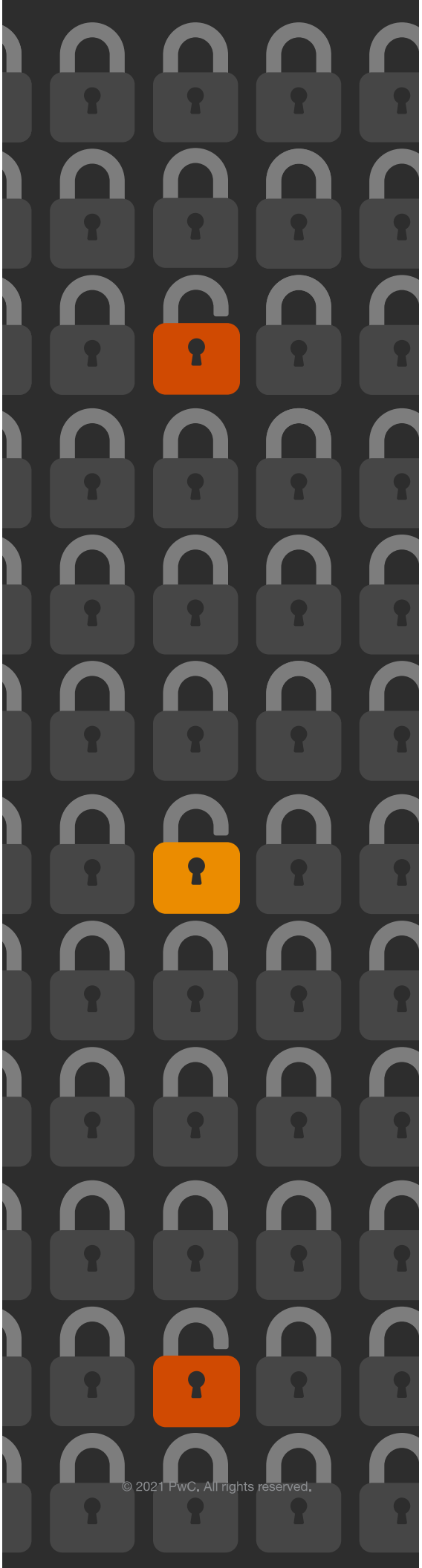
Redacted

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

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

PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 Ireland T: +353 (0) 1 792 6000, F: +353 (0) 1 792 6200, www.pwc.ie
Feargal O'Rourke (Managing Partner - PricewaterhouseCoopers Ireland)

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

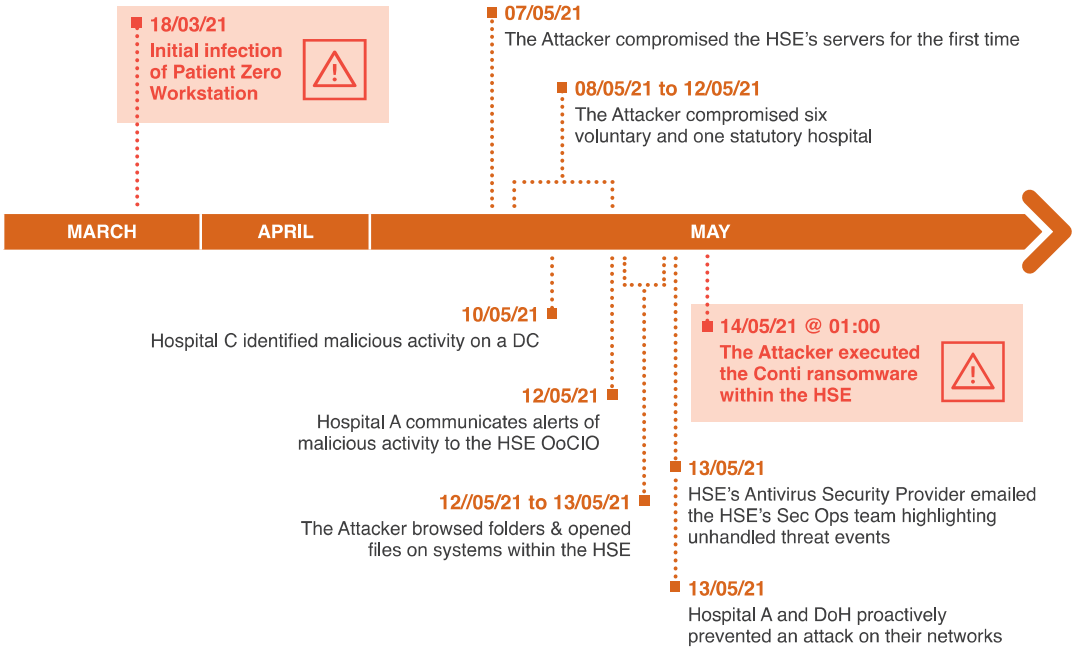
On 18 March 2021, the source of the cyber-attack[12] originated from a malicious software ("Malware") infection on a HSE workstation (the "Patient Zero Workstation"). The Malware infection was the result of the user of the Patient Zero Workstation clicking and opening a malicious Microsoft Excel file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



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