CYBERSECURITY, RANSOMWARE ATTACKS AND HEALTH: EXPLORING THE PUBLIC HEALTH IMPLICATIONS OF THE RECENT CYBERATTACK ON IRELAND'S HEALTH SERVICE

WINTERBURN Michael[1]*, HOUGHTON Frank[2]

[1]*Dept. of Information Technology, Limerick Institute of Technology, Moylish, Ireland.*

[2]*Dept. of Applied Social Sciences, Limerick Institute of Technology, Moylish, Ireland.*

Article submited: 02.05.2021; accepted: 10.07.2021

Abstract

In May 2021, Ireland's state healthcare system, the Health Services Executive, was the subject of a devastating ransomware attack called Conti. The malware uses a number of sophisticated tools and has effectively caused the healthcare system to go off-line for an extended period of time as the state has refused to pay the $19,999,000 ransom demand. Globally, ransomware is becoming a major issue for healthcare systems, with widespread attacks, even increasing in number during the Covid-19 pandemic. Healthcare systems may be being targeted for a number of reasons including that they are necessary to a population and may be vulnerable to compromise due to a lack of cybersecurity resources. To improve the security posture of healthcare systems a rebalancing may need to occur with potential impacts on resources available for healthcare provision and consequent impact on public health. Preventative measures regarding ransomware are presented, including what to do if an attack is discovered.

Keywords: cybersecurity, ransomware attacks and health: exploring the public health implications of the recent cyberattack on Ireland's Health Service

**Corresponding Author: Michael Winterburn; Michael.Winterburn@lit.ie*

In mid-May of 2021 the IT systems of Ireland's state health system, the Health Services Executive (HSE), was the subject of a sophisticated ransomware attack, with the criminal gang involved allegedly demanding $19,999,000 to restore access. Whilst many details of this cyberattack are not available yet, it is being called the Conti Ransomware attack [1]. The head of the Republic of Ireland's health service has described the impact of this attack as 'catastrophic'.

It should be noted that the history of ransomware is linked to healthcare. The first recorded case of this phenomenon was the 1989 AIDS Trojan (also known as PC Cyborg), in which 20,000 infected diskettes were sent to delegates attending a WHO conference on AIDS. Subsequently a Trojan software activated to hide directories and encrypt file names. Payment to an address in Panama was required to solve the issue [2].

This attack on Ireland's HSE is only the latest in a growing number of cyber-attacks on health systems. Other recent attacks include the Brno University Hospital in Czechia [3], and attempts by the PentaGuard group to target hospitals in Romania [4]. Perhaps the most well-known health system attack was against the Hollywood Presbyterian Medical Center in Los Angeles, California, which subsequently paid $17,000 to obtain a decryption key to regain access to their files. However, other major attacks include the targeting of the US health insurance company Anthem in 2015, the Australian Red Cross Blood Service in 2016, and the global WannaCry ransomware attack in 2017, which reportedly infected approximately 200,000 systems across more than 150 countries, including 50 hospitals in the UK [5].

It must be acknowledged that the healthcare sector is particularly vulnerable to cyberattacks [6]. There are many reasons for this, the greatest of which is probably a lack of IT security resources. Expenditure on IT systems in the health industry in many European countries is approximately a quarter of that spent on IT by other sectors of the economy, with many systems out of date or unsupported. Alongside this lack of resources is the shortage of experts in the field of cybersecurity employed in healthcare. Many healthcare systems are unable to recruit or retain such professionals as they struggle to match salaries available in other sectors. Other factors that make healthcare vulnerable include governance and culture. The governance issue is particularly problematic as healthcare in many countries is routinely provided by a myriad of different organisations and clear leadership and standards on this issue are often lacking. Cultural issues are also undoubtedly a problem, with healthcare providers focussing primarily on patient health and sharing information, rather than prioritising cyber security.

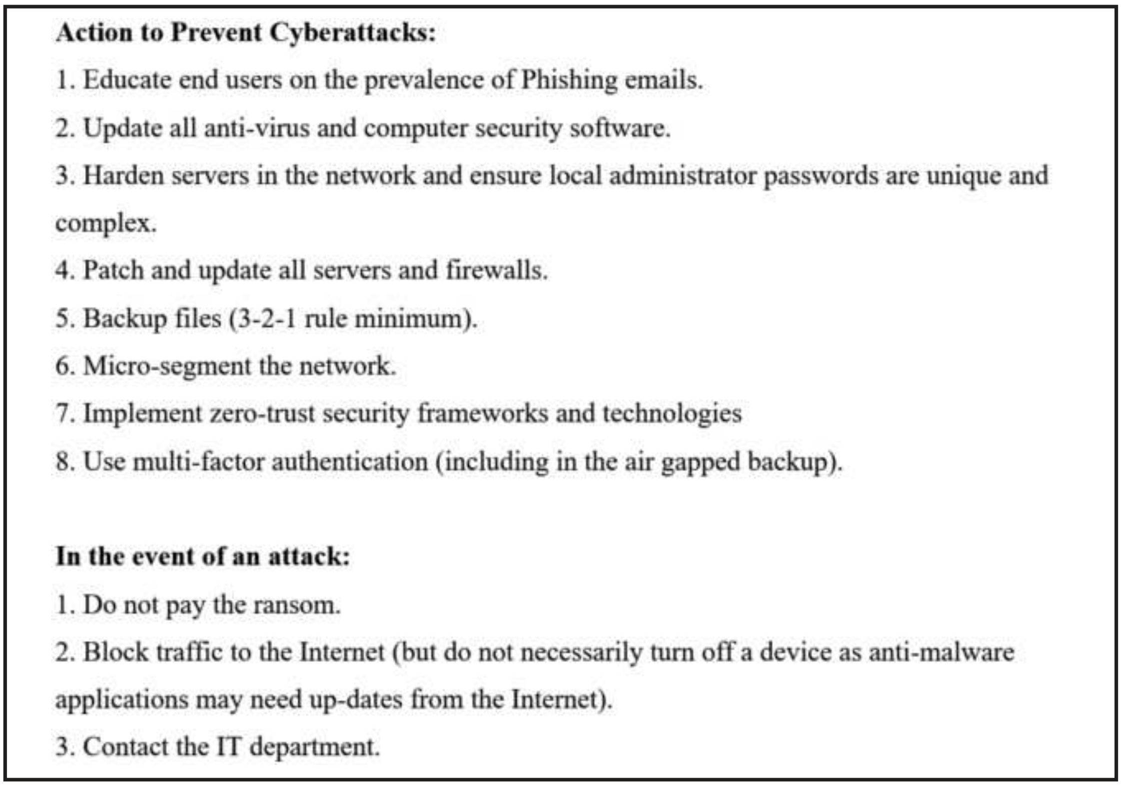
The impact of the COVID-19 pandemic is also a significant factor [7]. Health systems are over-stretched with staff stressed, worn-out, and struggling to adapt to recent wholescale expansions of online systems. The volume of cyber attacks on health systems has increased dramatically since the onset of the pandemic [8].

The Public Health implications of this attack are significant. The most obvious impact of the attack was that most state health services in Ireland effectively had to go off-line for an extended period, resulting in significant loss of services to patients. It should be remembered that this de facto shutdown occurred immediately following prolonged closures and restricted operation of many health services as a result of the COVID-19 pandemic. The potential adverse health impacts caused by the threatened or actual release of sensitive health data are significant. There can be no doubt that the personal and professional lives of many individuals will be negatively impacted into the future, whether it be as a result of blackmail, identity theft, fraud, or public censure from the publication of stolen data. Patient safety was also undoubtedly compromised as easy access to information on comorbidities, allergies, and existing prescriptions was lost.

The confidence of the public in health services is also a casualty of this attack. This widespread breach of confidentiality may have significant impacts into the future on the engagement of patients with sensitive and stigmatised health issues. This could include a range of services from testing for sexually transmitted diseases (STDs), and other reproductive health services, including fertility treatment and abortion, as well as engagement with mental health and domestic violence services.

Health providers that are subject to such cyberattacks may also be subject to legal action by patients, criminal proceedings for lack of due diligence, as well as compensation payments and regulatory fines. The reputational damage to health systems may have long term financial implications. These forms of cyberattacks may also weaken confidence in connected health, and hence significantly curtail moves towards increased telehealth, e-consultations, and mobile connected health devices [9]. Looking to the future, health services will have to re-examine the implications of information security of connected medical devices, and accessibility and utility to promote patient health and wellbeing. A final public health outcome of this attack will probably be the impact of the lost opportunity cost of this attack. Into the future, health systems will probably have to devote increasing amounts of scare resources to the issue of cybersecurity. It is highly likely that such diversion of funds will result in less resources for the provision of much needed health services elsewhere.

Although the cybercriminal group behind the attack in Ireland appear to have released the key to unlock the HSE's systems there are reports of confidential patient information appearing on the dark web, and already fraudulent attempts to obtain banking details have emerged, with criminals contacting former patients claiming that they were overcharged and offering refunds. Moving forward it is vital that all health service personnel prioritise cyber security, and understand how to prevent and respond to such attacks [10]. Basic steps in this process are outlined in Box bellow:



Action to Prevent Cyberattacks:

1. Educate end users on the prevalence of Phishing emails.
2. Update all anti-virus and computer security software.
3. Harden servers in the network and ensure local administrator passwords are unique and complex.
4. Patch and update all servers and firewalls.
5. Backup files (3-2-1 rule minimum).
6. Micro-segment the network.
7. Implement zero-trust security frameworks and technologies
8. Use multi-factor authentication (including in the air gapped backup).

In the event of an attack:

1. Do not pay the ransom.
2. Block traffic to the Internet (but do not necessarily turn off a device as anti-malware applications may need up-dates from the Internet).
3. Contact the IT department.

Resumo

En majo 2021, la ŝtata sansistemo de Irlando, la Health Services Executive, estis la celo de detrua atako per elaĉeta programaro nomita Conti. La fiprogramaro uzas kelkajn sofistikajn ilojn kaj efike kaŭzis, ke la sansistemo senretiĝis dum longa tempo, ĉar la ŝtato rifuzis pagi la rekompencan postulon de $ 19,999,000. Tutmonde elaĉeta programaro fariĝas grava afero por sanaj sistemoj, kun vastaj atakoj, eĉ pli multnombre dum la pandemio COVID-19. Kuracaj sistemoj eble estas celitaj pro multaj kialoj inkluzive de tio, ke ili estas necesaj por loĝantaro kaj povas esti facile damaĝeblaj pro manko de cibersekurecaj rimedoj. Por plibonigi la sintenon de sansistemoj rilate al sekureco, eble necesas reekvilibrigo kun eblaj efikoj al rimedoj haveblaj je la dispono de sanprizorgo kaj konsekvence efiko al publika sano. Preventaj rimedoj pri elaĉeta programaro estas prezentitaj, inkluzive kion fari se atako estas malkovrita.

References

1. National Cyber Security Centre. Ransomware Attack on Health Sector - UPDATE 2021-05-16. NCBC, Department of the Environment, Climate & Communications, Ireland.https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf (accessed: 28/05/2021)

2. Kruse CS, Frederick B, Jacobson T, Monticone DK. (2017) Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care 25 (2017) 1–10. DOI 10.3233/THC-161263

3. Porter S. Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak. HealthCareITNews. 2020. Mar 19. https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak (accessed: 28/05/2021)

4. ZDNet (2020) ZDNet. 15th May 2020. Hackers preparing to launch ransomware attacks against hospitals arrested in Romania. https://www.zdnet.com/article/hackers-preparing-to-launch-ransomware-attacks-against-hospitals-arrested-in-romania/ (accessed: 28/05/2021)

5. Millard WB. Where Bits and Bytes Meet Flesh and Blood. Ann Emerg Med. 2017; doi: 10.1016/j.annemergmed.2017.07.008

6. Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med Inform Decis Mak. 2019;19(1):10. Published 2019 Jan 11. doi:10.1186/s12911-018-0724-5

7. Williams CM, Chaturvedi R, Chakravarthy K. Cybersecurity Risks in a Pandemic. J Med Internet Res. 2020 Sep 17;22(9):e23692. doi: 10.2196/23692

8. He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review [published correction appears in J Med Internet Res. 2021 Apr 28;23(4):e29877]. J Med Internet Res. 2021;23(4):e21747. Published 2021 Apr 20. doi:10.2196/21747

9. Seh AH, Zarour M, Alenezi M, et al. Hea - lthcare Data Breaches: Insights and Implications. Healthcare (Basel). 2020;8(2):133. Published 2020 May 13. doi:10.3390/healthcare8020133

10. Australian Signals Directorate. Strategies to Mitigate Cyber Security Incidents – Mitigation Details. Australian Cyber Security Centre, AustralianGovernment. https://www.cyber.gov.au/sites/default/files/2019-03/Mitigation_Strategies_2017_Details_0.pdf (accessed: 28/05/2021)