International Journal For Quality In Health Care, 2020, 00(00), 1–4
doi:10.1093/intqhc/mzaa117
Advance Access Publication Date: 27 September 2020
Frontiers of Improvement

Frontiers of Improvement

Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health

Ms MENAKA MUTHUPPALANIAPPAN LLB[1] AND Dr KERRIE STEVENSON MBChB BMedSci (Hons) FHEA[2]

[1]Marsh JLT Specialty, 8 Marina View, Asia Square Tower 1, 018960 Singapore and [2]Faculty of Public Health and Policy, London School of Hygiene and Tropical Medicine, 15-17 Tavistock Place, London WC1H 9SH, UK

Address reprint requests to: Kerrie Stevenson, Faculty of Public Health and Policy, London School of Hygiene and Tropical Medicine, 15-17 Tavistock Place, London, UK. E-mail: kerrie.stevenson@lshtm.ac.uk

Received 8 June 2020; Editorial Decision 7 September 2020; Revised 12 August 2020; Accepted 18 September 2020

Abstract

The Coronavirus Disease 2019 (COVID-19) pandemic has resulted in widespread disruption to the healthcare industry. Alongside complex issues relating to ensuring sufficient healthcare capacity and resourcing, healthcare organizations and universities are now also facing heightened cyber-security threats in the midst of the pandemic. Since the outbreak began, various healthcare providers and academic institutions across the world have been targeted in a variety of complex and coordinatized cyber-attacks. International and national regulatory bodies have stressed the urgent need for healthcare providers and universities to protect themselves against cyber-attacks during COVID-19, recognizing that a growing number of cyber-criminals are seeking to capitalize on the vulnerabilities of the healthcare sector during this period. This includes a desire to steal intellectual property such as data relating to COVID-19 vaccine development, modelling and experimental therapeutics. It is therefore essential that healthcare providers and universities ensure they are informed, protected and prepared to respond to any cyber-threat. This article outlines key COVID-19 cyber-security principles for both healthcare organizations and academic institutions.

Key words: COVID-19, cyber-security, healthcare, technology

Background

In April 2020, the International Criminal Police Organization (INTERPOL) published a report cautioning a global increase in the prevalence of cyber-attacks relating to the Coronavirus Disease 2019 (COVID-19) pandemic [1]. These attacks are targeting individuals as well as public and private companies, including those in the healthcare industry. Alongside many others, the healthcare industry has been severely impacted by COVID-19 due to significantly increased demand for clinical care, medical equipment and health technology. With the industry's increasing reliance on information technology (IT) to deliver patient care, to model the disease, create a vaccine and in healthcare governance, it's unsurprising that cyber-criminals are capitalizing on the crisis.

Recent attacks and the challenges of responding

Over the past months, these vulnerabilities have been exploited globally; (i) a cyber-attack that halted the network of a Czech hospital in March, (ii) a ransomware attack on a vaccine trial group in UK in March, (iii) an unspecified cyber-attack on the US Health Agency in March, (iv) an unspecified cyber-attack on the construction company building the UK's emergency COVID-19 hospitals in May, and (v) an alleged state-sponsored attack on UK, US and Canadian universities developing a COVID-19 vaccine in July (Table 1). The Czech hospital hosted one of the country's biggest COVID-19 testing laboratories, forcing its entire IT network to shut down. This resulted in significant diagnostic delays regionally that adversely impacted patient care. In recent weeks, INTERPOL have also reported hos-

© The Author(s) 2020. Published by Oxford University Press on behalf of International Society for Quality in Health Care. All rights reserved.
For permissions, please e-mail: journals.permissions@oup.com

Downloaded from https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483 by guest on 16 June 2022

Table 1 Summary of reported cyber-attacks/data breaches in healthcare and academic organisations during the COVID-19 outbreak

Date of Cyber-Attack	Country/Institution	Reported Details
13 March 2020	Brno University Hospital, Czech Republic	Shut down of the IT network that caused postponement of urgent surgeries and compromised emergency medical care (https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/).
13 March 2020	World Health Organization (WHO)	Creation of a malicious site mimicking the WHO internal email system which aimed to steal employee passwords (https://tech.newstatesman.com/security/who-cyber-attack-covid19).
14 March 2020	Hammersmith Medicines Research Group, UK (COVID-19 Vaccine Trial Group)	Ransomware attack resulting in the publication of personal details of former patients, and a failed attempt to disable the network (https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus).
16 March 2020	United States Health and Human Services (HHS) Department	Unspecified attack on the HHS servers (https://tech.newstatesman.com/security/us-health-human-services-department-cyber-attack).
22 March 2020	Paris Hospital Authority (AP-HP), France	Unspecified attack on AP-HP servers (https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says).
4 April 2020	UK and Spanish Healthcare Workers	Ransomware attack attempting to deactivate anti-virus software (https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware; https://www.digitalhealth.net/2020/04/neither-covid-19-nor-cyber-criminals-care-who-gets-infected-and-suffers/).
13 May 2020	UK's ARCHER Academic High-Performance Computing (HPC) network	Exploitation of login nodes forcing rewriting on all user passwords (https://www.theregister.com/2020/05/13/uk_archer_supercomputer_cyberattack/).
13 May 2020	Bam Construct and Interserve (Companies who helped construct temporary COVID-19 hospitals for the UK's National Health Service)	Unspecified attack (https://www.constructionnews.co.uk/contractors/bam-construct/bam-construct-hit-by-cyber-attack-13-05-2020/).
10 June 2020	Babylon Health (Appointment and video-conferencing software for NHS doctors)	Data breach due to software error (https://www.mobihealthnews.com/news/europe/babylon-health-admits-gp-hand-app-data-breach-caused-software-issue).
16 July 2020	US, UK and Canadian authorities	Alleged unspecified state-sponsored cyber-attacks on institutions working on COVID-19 vaccines (https://www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers).

pitals and universities being threatened with being held ransom by cyber-criminals [2].

Alongside frontline health services, other parts of the healthcare industry supply chain are also vulnerable to attacks, including medical manufacturers working to meet the overwhelming global demand for COVID-19 essential goods. Increasingly, intellectual property belonging to research institutions working on novel treatments, diagnostics and vaccines are being targeted. Early in May 2020, the UK's National Cyber-Security Centre announced a significant increase in cyber-attacks perpetrated by hostile states and cyber-criminals targeting British universities and institutions working on COVID-19 research [3]. In response to this and other attacks, the UK's Health Secretary gave the UK's intelligence service access and oversight to the NHS IT network in May.

Unfortunately, healthcare organizations and universities often lack resources to protect against cyber-attacks and can be badly affected by the cost and long-term impacts of security breaches. The 2018 WannaCry ransomware attack which affected an estimated 40% of global healthcare institutions cost the UK's National Health Service an estimated £92 million due to a combination of ransoms paid and activity cancelled [4]. As such, in both this and in future pandemics, it is imperative that healthcare organizations and academic institutions are actively working to prevent and mitigate the impact of these attacks.

Key COVID-19 cyber-security principles for healthcare and academic organizations

Crucial to any mitigating action is investment in modern IT infrastructure with effective patch management and malware protection in both healthcare and academic settings [5]. Alongside this, institutions should ensure all staff are aware of common cyber-attacks including; (i) luring victims into downloading malicious apps, (ii) phishing emails disguised as official outbreak updates which distribute malware via attachments or links, and (iii) embedded spyware or malware in publicly available interactive COVID-19 maps and websites [5]. Secondly, good 'cyber-hygiene' should be incorporated

Downloaded from https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483 by guest on 16 June 2022

into everyday working patterns for staff. This includes; (i) use of strong passwords, (ii) avoiding opening unknown emails and links, (iii) enablement of firewall protection at work and home, and (iv) delivery of effective staff training [6].

Healthcare institutions should be aware that they face additional risks in the context of any cyber-attack and ensure these are appropriately managed [6]. Under-investment in cyber-security in healthcare institutions means some are particularly vulnerable to ransomware attacks, particularly during the COVID-19 pandemic. Cyber-criminals can shut down devices, servers or whole networks and demand a ransom to rectify the encryption. This may cause disruption to patient records, imaging and surgical services, medical devices and appointment systems. As medical devices become increasingly 'connected', cyber-criminals may hack devices such as cardiac pacemakers [7]. Healthcare institutions should remember that any cyber-security breach can result in disclosure of personally identifiable medical information and can severely interrupt clinical services, including emergency or life-saving care, potentially resulting in loss of life. Institutions should be prepared to handle the short- and long-term impacts of any attack, bearing in mind the economic and legal implications, and must have robust business continuity plans in place. Alongside this, they should establish a 'security culture' amongst staff by ensuring cyber-security training for all employees. A highly trained and responsive cyber-security team should be readily available, and organizations should ensure meticulous auditing of who is accessing health record systems. All mobile devices containing personal medical information should be protected with encryption, and software should not be installed by staff without prior consent. Staff working on remote devices should be enabled to connect to a virtual private network (VPN) to maintain a secure connection over unsecured internet infrastructure [8].

Academic institutions also face a series of unique threats including disclosure of secure research data or confidential patient trial data. This may be particularly dangerous for medical academic institutions involved in the development of highly coveted COVID-19 vaccines or novel treatments. State-sponsored espionage may aim to access trial information and exploit any imminent commercial opportunities. COVID-19 has also raised the public profile of many individual researchers meaning some are at risk of being personally targeted by hackers seeking to gather sensitive data relating to medical trials [9]. Universities should ensure all staff and students are familiar with key cyber-security principles, as well as where to report any suspicious activity. The diverse nature of users accessing university networks means it is challenging to ensure access is only available when necessary, but this is key to ensuring attackers are not able to regularly use authentic user credentials to access the network. Staff and students accessing the internal network on remote devices on campus or at home should connect to a VPN. This ensures secure and encrypted access to the internal network which vastly reduces the risk of a security breach. University networks often contain a collection of smaller networks which serve departments, laboratories and individual faculties. When maintained with minimal oversight, these networks are vulnerable to breaches. However, when managed well, these smaller networks can be used to store sensitive data and apply a higher level of protection without impacting the accessibility of the whole network [10].

Both healthcare and academic organizations should urgently assess the risks presented by a cyber-attack in the context of COVID-19 and develop a detailed incident response plan, remembering that attacks are likely to interrupt all aspects of delivery including current supply chains. In the event of an attack, organizations will need substantial support to respond effectively including forensic services, data breach expertise and enhanced public relations capabilities [6].

Conclusion

This pandemic has significantly affected healthcare delivery globally and is likely to do so for the foreseeable future. In the scramble to strengthen frontline medical services and find new treatments, healthcare organizations and academic institutions must not neglect the imminent threat of cyber-criminality; lives, novel treatments and a vaccine could depend upon it.

Acknowledgements

There are no acknowledgments.

Funding

The work was supported by an Academic Clinical Fellowship in Public Health from the UK's National Institute for Health Research [to KS].

Authors' Contributions

Both authors contributed equally to the manuscript.

Conflicts of Interest

MM is an insurance broker working for Marsh JLT Specialty that advises on cyber-risk insurance to organizations in Asia. She previously held a similar role in JLT Specialty, London. KS has no conflicts of interest to declare.

Data Availability Statement

No new data were generated or analysed in support of this research.

References

1. Preventing crime and protecting police: INTERPOL's COVID-19 Global Threat Assessment. *International Criminal Police Organisation*: https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment (May 2020, date last accessed).
2. INTERPOL launches awareness campaign on COVID-19 cyberthreats. *International Criminal Police Organisation*: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-launches-awareness-campaign-on-COVID-19-cyberthreats (July 2020, date last accessed).
3. Grierson J, Devlin H Hostile states trying to steal coronavirus research. *The Guardian*. https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency (May 2020, date last accessed)
4. *Two Years In and WannaCry is Still Unmanageable, Armis Security*. https://www.armis.com/resources/iot-security-blog/wannacry/ (May 2020, date last accessed).
5. Pandemic profiteering: how criminals exploit the COVID-19 crisis. *European Union Agency for Law Enforcement Cooperation*. https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (May 2020, date last accessed).
6. *Healthcare Information Security: Best Practices for Healthcare. Information Security Institute*. https://resources.infosecinstitute.com/catego-

Downloaded from https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483 by guest on 16 June 2022

ry/healthcare-information-security/is-best-practices-for-healthcare/ (May 2020, date last accessed).

7. *Cybersecurity: How can it be Improved in Healthcare?* Chicago: University of Illinois. https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/ (July 2020, date last accessed).
8. Bhuyan SS, Kabir U, Escareno JM, *et al*. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *J Med Syst* 2020;**44**: 10.1007/s10916-019-1507-y
9. Muncaster P State hackers target UK Universities s for COVID19 vaccine research. *Info-security Magazine*. https://www.infosecurity-magazine.com/news/state-hackers-uk-unis-covid19 (July 2020, date last accessed).
10. *The Cyber Threat to Universities: Assessing the Cyber Security Threat to UK Universities*. UK National Cyber-Security Centre. https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities (July 2020, date last accessed).

Downloaded from https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483 by guest on 16 June 2022