Commentary

DIGITAL HEALTH

Digital Health
Volume 8: 1–3

DOI: 10.1177/20552076221104665
journals.sagepub.com/home/dhj
SAGE

Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that

O'Brien Niki[1], Ghafur Saira[1], Sivaramakrishnan Arvind[2] and Durkin Mike[1]

Abstract

Cyber-attacks on healthcare institutions have increased in recent years and have made headlines through the COVID-19 pandemic. With the fallout of attacks increasingly reported in academic research and in the media, there is a real urgency to address cyber-threats that must be augmented across and within health systems. Until now, clinical healthcare professionals have considered cyber-attacks on healthcare organisations a predominantly information and communication technology issue, but this perception is no longer fit-for-purpose. This commentary provides insights into the scale of cyber-attacks and their impact on staff wellbeing, arguing that cybersecurity education for all staff in healthcare organisations must be improved through online resources, simulation, and gaming. The role of national educators, policymakers, and multilateral organisations in achieving this is outlined alongside implications for future policy and practice.

Keywords

Education, online, technology, health informatics, health communications

Submission date: 21 March 2022; Acceptance date: 14 May 2022

Cybersecurity in healthcare is not a duty or an obligation but an act of responsibility. When patients and families entrust their lives to the health system and its professionals, their complete commitment to excellence in delivery is a basic expectation.

The increase in cyber-attacks on healthcare institutions has made headlines through the COVID-19 pandemic.[1,2] A ransomware attack on the Irish health system in May 2021 was a reminder of how much disruption cyber-attacks can cause healthcare services.[2] However, this threat to healthcare organisations and patient safety is not new; cyber-attacks have intensified with the increased use of digital technology in healthcare.

We know that clinical healthcare professionals have previously considered cyber-attacks on healthcare organisations a predominantly information and communication technology (ICT) issue, but the nature and increased frequency of attacks is turning that dichotomy on its head. Table 1 outlines the two most common types of attacks, and recent examples from healthcare, according to findings from the 2021 HIMSS Healthcare Cybersecurity Survey.[3] Clinical staff are at the eye of the storm, but are often not provided the tools and education to address these challenges.

When hackers rendered the Dusseldorf University Hospital computer system inoperable in November 2020, this resulted in the shutdown of services forcing a patient to be transferred to a hospital 60 km away.[1] Consider the experience of clinicians caring for the 78-year-old woman who subsequently died on route. They were not to blame for the attack and its outcome (the Health Minister of North Rhine-Westphalia was warned of weaknesses within healthcare IT systems in the weeks prior), but in general, loss of life undoubtedly weighs on clinical staff, including medical students.[8]

Sensitising students to digital health technologies is rightfully now increasing in academia and healthcare.[9] Cybersecurity is an integral component of safe and effective health technology use, as well as patient safety in the modern era, and must be core to this conversation and subsequent planning. As part of this, all future healthcare

[1]Institute of Global Health Innovation, Imperial College London, London, UK
[2]Apollo Hospitals Enterprise Ltd, Chennai, TN, India

Corresponding author:
O'Brien Niki, Institute of Global Health Innovation, Imperial College London, Room 1035/7, QEQM Wing, St Mary's Campus, London W2 1NY, UK.
Email: n.obrien@imperial.ac.uk

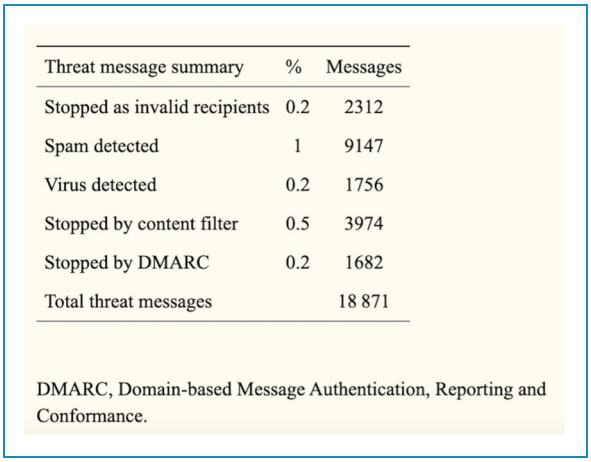
Table 1. Common types of cyber-attacks and recent examples from healthcare.

Type of attack		Example from the health sector
Phishing attack	Phishing describes a particular type of scam where an attacker sends a fraudulent email or text message from a seemingly trusted individual or organisation. The aim of a phishing attack is to trick the recipient into clicking an attachment which allows the attacker to do something the recipient may not be aware of (e.g. the stealing of credentials/ passwords).[4]	In March 2020, a phishing attack on the World Health Organization was identified. A group of cyber-attackers launched a malicious website mimicking the WHO's internal email system with the intention of stealing passwords from WHO staff.[5] The attack was unsuccessful but highlighted the level of sophistication of some phishing attacks targeting healthcare organisations.
Ransomware attack	Ransomware is a type of malicious software (malware) that makes systems unusable until the victim makes a payment.[4] Ransomware uses encryption to disable an organisation's access to its own critical data, including databases and file servers. Access of only granted following the payment of a ransom to the cyber-attackers.	In May 2021, a Conti ransomware attack on the Irish health system affected more than 80% of its IT infrastructure, stealing data, and locking healthcare staff out of systems essential for healthcare delivery, as well as non-clinical systems like finance and procurement.[6] The attack stemmed from a staff member opening a malware compromised spreadsheet sent to them via email.[7] It took the service 4 months to fully recover.

professionals, as the regular users of digital health technologies, gatekeepers of patient information, and most importantly, frontline providers of care to patients, must be made aware of cyber risks and threats towards the development of a 'human firewall' as staff engage increasingly effectively in cybersecurity.[10,11] This is the first step to enable them to prepare both practically for threats they can mitigate, and psychologically for those they cannot.[12] Yet current academic literature on teaching cybersecurity to students and medical professionals focuses on cybersecurity as an element of training on complex digital health technologies, such as artificial intelligence.[13] But have we missed a step, or more importantly, how many opportunities have we missed during their educational experience?

The value of strong cybersecurity in novel digital health technologies is clear. Yet these areas of health technology are in their infancy at the global level. Across health systems, the majority of cybersecurity breaches stem from phishing emails, negligence or inappropriate accessing of data,[14] rather than attacks on complex technologies. The huge scale of these simple attacks is known: staff at one UK NHS institution received 18,871 email phishing threats in a 1-month period, 2.2% of all emails received.[15] The system is often complicit in the ergonomics of clinical error, which becomes highly relevant when we consider that healthcare workers with a high workload are significantly more likely to open a phishing email (Figure 1).[16]

Cybersecurity should not be an add-on to ICT training, yet it has been noted that there are no widespread educational techniques to train clinical staff to identify and manage cyberattacks in the clinical realm (e.g. attacks on medical devices),[17] nor their role in larger scale cyber-attacks on their organisation. Educating students across healthcare disciplines on the basics of cybersecurity, types of attacks, where and how cyber-attackers are most likely to target individuals, their role in maintaining security, and the connection between cybersecurity and patient safety,[18] are fundamentals that are being overlooked alongside greater efforts to build a culture of responsibility around cybersecurity. The challenges of organisational hierarchies, poor reporting cultures, and fear of speaking up must also be discussed openly in the context of a suspected cyber-attack.



Threat message summary	%	Messages
Stopped as invalid recipients	0.2	2312
Spam detected	1	9147
Virus detected	0.2	1756
Stopped by content filter	0.5	3974
Stopped by DMARC	0.2	1682
Total threat messages		18 871

DMARC, Domain-based Message Authentication, Reporting and Conformance.

Figure 1. Summary of threat message activity during a 1-month period reported by Priestman et al.[15] Reproduced under licence: CC BY-NC.

A range of tools or concepts can be utilised or built upon to aid the teaching of cybersecurity. For example, Health Education England offers NHS staff access to short, online learning programmes, including a programme entitled 'Data security awareness', as part of the Technology Enhanced Learning: Digital education programme.[19] The need to make such education fun and easy to assimilate calls for simulation and gaming techniques to be employed more often in the teaching–learning process. As the simulation is already widely used in medical education, its use in cybersecurity training lends itself to incorporation within clinical training activities.[17] National educators and policymakers can explore other areas of patient safety education to develop tools. Multilateral organisations should aid efforts through the creation of educational tools at the global level.

The COVID-19 pandemic has ushered in a new era of digital health expansion but has brought the lucrativeness of cyber-attacks on healthcare organisations into view for malicious actors. Cyber-attacks are a permanent and substantial threat to health systems. It is not solely the responsibility of the ICT sector or ICT departments to respond. All medical education programmes must advance curriculums and priorities to train clinical staff to prepare for, and address, cybersecurity threats as they would any other element of patient safety. Well prepared students will support and advance safer health systems in the long term.

Acknowledgements: This work has not been previously published.

Author contributions: NO and MD conceptualised the manuscript. NO and MD led in the writing of the original draft manuscript, with input from SG and AS. All authors (NO, SG, AS, MD) equally contributed to the writing, reviewing, and editing to develop the final draft. All authors approved the version submitted for publication.

Declaration of conflicting interests: The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Ethical approval: Not applicable.

Funding: The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Infrastructure support for this work was provided by the NIHR Imperial Biomedical Research Centre.

Guarantor: No.

ORCID iD: O'Brien Niki https://orcid.org/0000-0002-8389-1448

References

1. Crossland D. Woman dies after hackers hit A&E in Düsseldorf. The Times, https://www.thetimes.co.uk/article/woman-dies-after-hackers-hit-a-amp-e-in-duesseldorf-s5gr62ctj (2020, accessed 5 December 2021).
2. Perlroth N and Satariano A. Irish hospitals are latest to be hit by Ransomware attacks. The New York Times, https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html (2021, accessed 5 December 2021).
3. HIMSS. 2021 HIMSS healthcare cybersecurity survey: HIMSS, https://www.himss.org/resources/himss-healthcare-cybersecurity-survey (2021).
4. Ghafur S, Fontana G, Martin G, et al. Improving cyber security in the NHS, 2019.
5. Satter R, Stubbs J and Bing C. Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike. Reuters, https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN (2021, accessed 10 March 2022).
6. PwC. Conti cyber attack on the HSE: Independent Post Incident Review: PwC, https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf (2021).
7. Corera G. Irish health cyber-attack could have been even worse, report says. BBC, https://www.bbc.co.uk/news/technology-59612917 (2021, accessed 10 March 2022).
8. Batley NJ, Bakhti R, Chami A, et al. The effect of patient death on medical students in the emergency department. *BMC Med Educ* 2017; 17: 110.
9. Keane PA and Topol EJ. AI-facilitated health care requires education of clinicians. *The Lancet* 2021; 397: 1254.
10. O'Brien N, Grass E, Martin G, et al. Developing a globally applicable cybersecurity framework for healthcare: a Delphi consensus study. *BMJ Innov* 2021; 7: 199.
11. Coventry L and Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas* 2018; 113: 48–52.
12. Kamerer JL and McDermott D. Cybersecurity: nurses on the front line of prevention and education. *J Nurs Regul* 2020; 10: 48–53.
13. Paranjape K, Schinkel M, Nannan Panday R, et al. Introducing artificial intelligence training in medical education. *JMIR Med Educ* 2019; 5: e16048.
14. Ghafur S, Grass E, Jennings NR, et al. The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet Digital Health* 2019; 1: e10–e12.
15. Priestman W, Anstis T, Sebire IG, et al. Phishing in healthcare organisations: threats, mitigation and approaches. *BMJ Health Care Inform* 2019; 26: e100031.
16. He Y, Aliyu A, Evans M, et al. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. *J Med Internet Res* 2021; 23: e21747.
17. Dameff CJ, Selzer JA, Fisher J, et al. Clinical cybersecurity training through novel high-fidelity simulations. *J Emerg Med* 2019; 56: 233–238.
18. O'Brien N, Ghafur S and Durkin M. Cybersecurity in health is an urgent patient safety concern: we can learn from existing patient safety improvement strategies to address it. *J Patient Safety Risk Manag* 2021; 26: 5–10.
19. Health Education England. eLearning for healthcare: Programmes: Health Education England, https://www.e-lfh.org.uk/programmes/ (2021).