AAHC President's Council on Cybersecurity

Readiness | *Response* | *Recovery*

Cybersecurity at Academic Health Centers

Selected Readings for CEOs and C-Suite Leaders

Association of Academic Health Centers®
Leading institutions that serve society

aahcdc.org

Table of Contents

Clarke R, Youngstein T. Cyberattack on Britain's National Health Service—a wake-up call for modern medicine. N Engl J Med. 2017;377(5):409-11.

A 3-page Perspective article that highlights the 2017 WannaCry hack of the British National Health Service (NHS). This Perspective describes some of the major pitfalls from the attack and how the on-the-ground medical and IT staff handled the situation.

Access: https://www.nejm.org/doi/full/10.1056/NEJMp1706754 *(subscription required)*

Ghafur S, Grass E, Jennings NA, Darzi A. The challenges of cybersecurity in health care: the UK National Health Service as a case study. Lancet Digit Health. 2019;1(1):e10-2.

A 3-page Comment that uses the UK NHS as a case study for describing how other countries might consider their approach to cybersecurity. In addition to addressing the NHS, this article also describes cyber events in Singapore, Estonia, and the US.

Access: thelancet.com/journals/landig/article/PIIS2589-7500(19)30005-6/fulltext

Gordon WJ, Fairhall A, Landman A. Threats to information security—public health implications. N Engl J Med. 2017;377(8):707-9.

A 2-page Perspective article that inventories threats to information security in health centers, including hacking, ransomware, attacks on medical devices, denial of service attacks, and phishing. Provides an overview of major cyberattacks (e.g., WannaCry, Petya).

Access: https://www.nejm.org/doi/full/10.1056/NEJMp1707212 *(subscription required)*

Gordon WJ, Wright A, Aiyagari R, et. al. Assessment of employee susceptibility to phishing attacks at US health care institutions. JAMA Netw Open. 2019;2(3):e190393.

A 9-page Original Investigation that describes a phishing simulation conducted at six US healthcare centers, which involved distributing over two million phishing emails. Results indicated that the rate of employees opening these simulated emails was high and provides information on characteristics of institutions, including their efforts to raise awareness and train their employees, that can impact the click-through rate on infected emails.

Freely accessible at: https://jamanetwork.com/journals/jamanetworkopen/article-abstract/2727270

Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Int Res. 2018;20(5):e10059.

A 17-page article from MIT researchers based on interviews with C-Suite level health IT experts that attempts to lay out the systematic and organizational perspective for studying (1) the dynamics of cybersecurity capability development at hospitals and (2) how these internal organizational dynamics interact to form a system of hospital cybersecurity in the US. This article tackles some of the added complexity of having a medical center plus an academic entity, such as the need to accommodate trainee and researcher needs.

Freely accessible at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/

Jarrett MP. Cybersecurity—a serious patient care concern. JAMA. 2017;318(14):1319-20.

A 2-page Viewpoint that succinctly describes cybersecurity risks in relation to recent attacks. The major thrust of the article is to introduce, in an easily digestible format, the 2017 Health Care Industry Cybersecurity Task Force report on improving cybersecurity in the health care industry.

Access to article: https://jamanetwork.com/journals/jama/article-abstract/2654933 *(subscription required)*

Free access to related government report: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in Healthcare: a systematic review of modern threats and trends. Technol Health Care. 2017;25(1):1-0.

A 10-page systematic review of cybersecurity threats and potential solutions based on suggestions from the 31 included studies.

Freely accessible at: https://content.iospress.com/articles/technology-and-health-care/thc1263

Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we?. BMJ. 2017;358:j3179.

A 3-page Perspective focused on the UK, but applicable broadly. Includes a helpful box on key steps to improving cybersecurity and resilience. A quick, accessible introduction to the topic. This is paired with a brief, freely-accessible podcast featuring the authors.

Access: https://www.bmj.com/content/358/bmj.j3179 *(subscription required)*

Milliard WB. Where Bits and Bytes Meet Flesh and Blood: hospital responses to malware attacks. Ann Emerg Med. 2017;70(3):A17-21.

A 5-page Perspective on the 2017 cyberattack in Buffalo, New York that provides additional details about some of the steps taken by the hospital and IT departments before, during, and after the cyberattack.

Freely accessible at: https://www.annemergmed.com/article/S0196-0644(17)30891-0/fulltext

Ronquillo JG, Erik Winterholler J, Cwikla K, Szymanski R, Levy C. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. JAMIA Open. 2018;1(1):15-9.

A 4-page retrospective observational study of all available reported medical data breaches in the US from 2013 to 2017, downloaded from a publicly available federal regulatory database. This article provides an overview of the magnitude and characteristics of the problem (1,512 breaches affecting 154M patient records) in the last five years.

Freely accessible at: https://doi.org/10.1093/jamiaopen/ooy019