ANZ Journal of Surgery

WILEY | Royal Australasian College of Surgeons

PERSPECTIVE

Cybersecurity Should be a Routine Component of Healthcare Provider Education

Benjamin Piotrowski[1,2] | Ishith Seth[3] | Joshua Kovoor[4] | Mathew Jacob[4] | Toby Gilbert[1,2]

[1]Lyell McEwin Hospital, Elizabeth, Australia | [2]Adelaide Medical School, The University of Adelaide, Adelaide, South Australia, Australia | [3]Faculty of Medicine and Surgery, Monash University, Clayton, Victoria, Australia | [4]Ballarat Base Hospital, Ballarat, Victoria, Australia

Correspondence: Benjamin Piotrowski (bpiotrowski21@gmail.com)

Received: 2 February 2025 | **Revised:** 6 July 2025 | **Accepted:** 8 July 2025

Keywords: artificial intelligence | curricula | cybersecurity | digital health | teaching

1 | Introduction

The rapid digitisation in the healthcare sector has heightened cybersecurity vulnerability. The real threat of novel technologies, including those posed by generative Artificial Intelligence (AI), necessitates concerted action by institutions and individuals. In the first half of 2024, Australian health service providers, under the mandatory Notifiable Data Breaches scheme, reported the highest number of data breaches, which involved a likely risk of harm to personal information [1]. While these risks are widely acknowledged, the responsibility for mitigating them, particularly through structured education, remains ill-defined across Australia and New Zealand [2]. The burgeoning popularity of digital tools, including procedural equipment such as surgical robots or cardiac pacemakers, can further increase patients' susceptibility to direct harm [3]. As surgeons, our responsibility to advocate for our patients and provide the best possible care should be supplemented with appropriate tools and education at an organisational level—to safeguard patients and administer safe care.

Cybersecurity in surgical practice requires a multifaceted approach that integrates proactive risk management with enhanced educational initiatives. An alarming 95% of breaches result from human error, including actions by clinicians [4]. Proactive measures to promote safe cybersecurity practices are crucial for mitigating threats, reducing patient information breaches, and improving clinician safety. However, the successful adoption of strategies by healthcare professionals largely depends on the tools hospitals and administrative bodies provide. Education is a core means to safer practices and more resilient healthcare systems [5]. This perspective piece focuses on clarifying responsibility for cybersecurity education, highlighting curriculum gaps, and advocating for tailored strategies across healthcare institutions, particularly in surgical settings [2].

2 | Concerns and Implications of Cyberattacks

Cyberattacks have critical repercussions, compromising patient data, affecting the continuity of critical infrastructure, and eroding public trust. A 2025 CyberCX report declares an "elevated" level of threat to Australian and New Zealand hospitals, with a high potential disruption to patient care [6]. The Australian Government's Cyber Security Report 2022 declares an increase in weekly cyberattacks from 2021 (largely using social engineering, basic web app attacks and system intrusion) by 69% to an average of 1387 [7]. In New Zealand 2021, five hospitals and 600 servers in the Waikato district health board were targeted by a phishing operation disrupting functionality for 6 months [8]. This resulted in diversion of cancer radiotherapy treatment, inaccessible data on treatment progress, and deferred elective surgery dependent on radiological and pathology services [8]. Correspondingly, in 2022, Medibank (an Australian private healthcare insurer) compromised 9.7 million customers' data in a phishing attack, costing $35 million in recovery costs [9].

Nine cyber breaches have resulted in poor patient outcomes, including extended hospital stays, procedure delays, and medical complications [10].

3 | Digital Vulnerabilities Within Healthcare Systems

The sophistication of cyberattacks utilizing audio, data, and visual synthesis, particularly those involving AI, warrants concern. AI use is widespread, and its imitation of authoritativeness, apparent authenticity, and circumvention techniques (e.g., phishing emails, malware, and human authentication spoofing) has surpassed basic security measures [11]. Various studies have highlighted the potential for harm unique to healthcare, including the misuse of AI for misclassifying medical abnormalities leading to incorrect diagnoses [12], facial recognition for authentication bypass [13], and CT scan tampering [14]. A lack of investment in digital infrastructure is a key element of vulnerabilities [15].

The most frequently identified causes of human error resulting in breaches include the transmission of personal information to the wrong recipient, unintended release/publication, and loss of data storage or paperwork [1]. Australia and New Zealand have a heterogeneous cohort of clinicians and various levels of information technology literacy. Given this, and the balkanisation of electronic health records, there is limited universal oversight for authenticating cyber education and data protection.

4 | Proactive Education in Cybersecurity

The National eHealth Security and Access Framework (NESAF) in Australia and the Health Information Security Framework (HISF) in New Zealand establish the current framework guiding health data protection and security; however, they have limited endorsement of a proactive cybersecurity culture and compliance [16]. A 2018 Australian cybersecurity report identified that 63.6% of respondents did not have or were unsure if their healthcare organisation had embedded cybersecurity awareness and training in its policies/procedures [17]. A United States healthcare institution's phishing campaign resulted in a nearly 50% reduction in click-through rates [18]. Preventative strategies included multifactor authentication (MFA), external email filters, and employee awareness and training [18]. Ultimately, organisational employee training with an emphasis on 'cyber hygiene' is noted to improve the understanding of risks and reduce the average financial burden of data breaches [5, 19, 20].

5 | Cybersecurity Education and Recommendations

Innovative approaches to cybersecurity education can amplify its impact on surgical practice. Simulation-based learning, a cornerstone of surgical training, can be adapted to include cybersecurity scenarios. Mandatory training focusing on cybersecurity (e.g., cyber hygiene, recognising breaches, and phishing) is highly recommended to be introduced into Australian healthcare institutions [21]. Medical graduates should be expected to achieve a certain level of cybersecurity competency, which should be incorporated into their formal curricula. Initiatives would be best established within medical colleges and reinforced during the foundational years of training, allowing surgical trainees to embody principles of cybersecurity safety while focusing on building surgical expertise.

Surgical leadership plays a pivotal role in adopting cybersecurity best practices. As leaders in multidisciplinary teams, surgeons are uniquely positioned to influence organizational policies and champion a culture of digital safety [1, 7]. This includes continuing to advocate for regular security audits, promoting transparency in reporting breaches, and collaborating with IT specialists to address vulnerabilities in surgical technologies. Moreover, surgical societies and professional

TABLE 1 | Recommendations for security tools and education.

Passwords	Password rotation policies Enforcing password structure policies (e.g., enhancing complexity by incorporating special characters and unique logins) MFA (e.g., using hospital tag sign-on) or trusted password managers. Further protection with phishing-resistant MFA will contribute additional security against sophisticated cyberattacks. Not sharing password details
Device use	Logging in as a personal user and not a domain administrator Logging off devices after use Secure remote access
Levels of access	Appropriate level of access based on roles and responsibilities. Reviewing requirements for access privileges. Removal of extended access when inessential.
Storage of data	Not storing sensitive surgical information or research on external devices (e.g., USB, laptops, phones).
Emails	Be mindful of unsolicited emails from purported individuals, including surgical device companies, especially when the spelling is unusual or the sender is unrecognised.
Reporting of breaches/misuse	Responsible for timely reporting of mistakes or unintentional disclosures.

TABLE 2 | Strategies for wider cybersecurity measures.

Education	Standardised and revised education on system vulnerabilities, cyber hygiene, and threat detection. Implementing features and education in line with the Australian Signals Directorate 'Essential Eight', which is designed to provide guidance to address "cyber intrusions (i.e., those executed by advanced persistent threats such as foreign intelligence services), ransomware and external adversaries with destructive intent, malicious insiders, 'business email compromise', and industrial control systems." [22]
Communication standards	Communicating with treating teams/professionals on a secure platform using de-identified data. For example, avoiding WhatsApp for inter-team communication. It would be suggested that a verified, deidentified, and encrypted portal/application be integrated into the electronic health records system. Implementing email filters that screen for phishing and suspicious emails and indicate emails from external senders.
Information standards	Avoid documenting and recording data using unencrypted services. For example, Google Sheets can record multidisciplinary team meetings or send surgical pictures via unencrypted methods.
Hospital devices	Promoting individual/team-shared devices.
Medical and surgical devices	Regular patchwork with hardware, firmware and software. Optimising safe use of video recording and training. Collaborating with vendors to reduce the risk of exploitation.
Software	Regular software updates and patches.
Auditing	Regular security auditing. Reviewing cybersecurity detection, incident response, recovery and continuity protocols.
Reporting systems	Reporting platforms and procedures for open disclosure reporting of breaches/misuse without repercussion. This would help compile evidence to guide policy/legislation improvements and reforms. Monitoring procedures for threat detection, response to incidents and suspicious activity.
Third party programs	Centralising third-party health programs via a safe hospital monitored system, such as accessible databases that allow monitoring and safe access to required resources (e.g., imaging providers, guidelines etc.)
Legislation	Legislative change to enforce uniform standards in education, policy and safety requirements.

bodies are well placed to support cybersecurity awareness by promoting practical education and reinforcing applicable standards through existing professional development frameworks [1, 7, 15]. Examples of such practical approaches are summarized in Tables 1 and 2 [1, 7, 15, 23].

6 | Conclusion

Cybersecurity education is not a novel concept, but its implementation in the Australasian healthcare setting remains fragmented and inconsistently prioritized. Rather than reiterating known risks, this paper identifies actionable gaps in responsibility, curriculum integration, and institutional accountability. A coordinated educational strategy, guided by medical colleges and health organizations across Australia and New Zealand, is urgently needed to embed cybersecurity as a standard competency for all healthcare professionals, particularly surgeons operating in digitally networked environments. Only through structured, role-specific education and robust institutional support can the surgical community uphold its obligation to deliver safe, digitally secure patient care.

Acknowledgements

Dr. Joshua Kovoor is a Fulbright Future Scholar, supported by the Australian-American Fulbright Commission.

Disclosure

The authors have nothing to report.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

1. Office of the Australian Information Commissioner (OAIC), "Notifiable Data Breaches Report: January to June 2024," 2024, Australian Government, https://www.oaic.gov.au/__data/assets/pdf_file/0013/242050/Notifiable-data-breaches-report-January-to-June-2024.pdf.

2. T. W. Hoffman and J. F. Baker, "Navigating Our Way Through a Hospital Ransomware Attack: Ethical Considerations in Delivering Acute Orthopaedic Care," *Journal of Medical Ethics* 49, no. 2 (2023): 121–124.

3. W. Gordon, N. Ikoma, H. Lyu, G. Jackson, and A. Landman, "Protecting Procedural Care—Cybersecurity Considerations for Robotic Surgery," *Npj Digital Medicine* 5, no. 1 (2022): 148.

4. N. Jerry-Egemba, "Safe and Sound: Strengthening Cybersecurity in Healthcare Through Robust Staff Educational Programs," *Health Management Forum* 37, no. 1 (2024): 21–25.

5. S. Nifakos, K. Chandramouli, C. K. Nikolaou, et al., "Influence of Human Factors on Cyber Security Within Healthcare Organisations: A Systematic Review," *Sensors* 21, no. 15 (2021): 5119.

6. CyberCX, "Diagnosing Cyber Threats in Healthcare 2025," (2025), https://connect.cybercx.com.au/cyber-threats-in-healthcare-2025.

7. Australian Digital Health Agency, "Cyber Security Report 2022," 2023 Level 25, 175 Liverpool Street, Sydney, NSW 2000: Australian Government; 2023, https://www.digitalhealth.gov.au/sites/default/files/documents/cyber-security-report-2022.pdf.

8. International Cyber Law: Interactive Toolkit Contributors, "Waikato Hospitals Ransomware Attack (2021): International Cyber Law: Interactive Toolkit," 2022, https://cyberlaw.ccdcoe.org/wiki/Waikato_Hospitals_ransomware_attack_(2021)?oldid=3411.

9. M. Dart and M. Ahmed, "Operational Shock: A Method for Estimating Cyber Security Incident Costs for Large Australian Healthcare Providers," *Journal of Cyber Security Technology* 8, no. 4 (2024): 260–285.

10. J. Tully, J. Selzer, J. P. Phillips, P. O'Connor, and C. Dameff, "Healthcare Challenges in the Era of Cybersecurity," *Health Security* 18, no. 3 (2020): 228–231.

11. C. Nobles, "The Weaponization of Artificial Intelligence in Cybersecurity: A Systematic Review," *Procedia Computer Science* 239 (2024): 547–555.

12. S. Finlayson, J. Bowers, J. Ito, J. Zittrain, A. Beam, and I. Kohane, "Adversarial Attacks on Medical Machine Learning," *Science* 363, no. 6433 (2019): 1287–1289.

13. A. Bose and P. Aarabi, "Adversarial Attacks on Face Detectors Using Neural Net Based Constrained Optimization," (2018), IEEE 20th International Workshop on Multimedia Signal Processing (MMSP); 2018 29–31.

14. Y. Mirsky, T. Mahler, I. Shelef, and Y. Elovici, "{CT-GAN}: Malicious Tampering of 3d Medical Imagery Using Deep Learning," 2019 28th USENIX Security Symposium (USENIX Security 19).

15. P. Ewoh and T. Vartiainen, "Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review," *Journal of Medical Internet Research* 26 (2024): e46904.

16. K. Offner, E. Sitnikova, K. Joiner, and C. MacIntyre, "Towards Understanding Cybersecurity Capability in Australian Healthcare Organisations: A Systematic Review of Recent Trends, Threats and Mitigation," *Intelligence and National Security* 35, no. 4 (2020): 556–585.

17. Cybersecurity Community of Practice (CCoP), "Cybersecurity Across the Australian Healthcare Sector|Final Report of a National Survey 85 Buckhurst Street, South Melbourne VIC 3205: Health Informatics Society of Australia; 2018," https://www.hisa.org.au/wp-content/uploads/2018/07/HISA-Healthcare-Cybersecurity-Report_June-2018.pdf.

18. W. Gordon, A. Wright, R. Aiyagari, et al., "Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions," *JAMA Network Open* 2, no. 3 (2019): e190393.

19. W. Priestman, T. Anstis, I. Sebire, S. Sridharan, and N. Sebire, "Phishing in Healthcare Organisations: Threats, Mitigation and Approaches," *BMJ Health Care Inform* 26, no. 1 (2019): e100031.

20. IBM, "Cost of a Data Breach Report 2024 2024," https://www.ibm.com/reports/data-breach.

21. R. Salama, C. Altrjman, and F. Al-Turjman, "Healthcare Cybersecurity Challenges: A Look at Current and Future Trends," in *Computational Intelligence and Blockchain in Complex Systems*, ed. F. Al-Turjman (Morgan Kaufmann, 2024), 97–111.

22. Australian Signals Directorate (ASD), "Strategies to Mitigate Cyber Security Incidents: Australian Government," 2010, https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20%28February%202017%29.pdf.

23. S. Muhammad and N. A. Mirjat, "Cybersecurity in Digital Healthcare: Strategies for Protecting EHRs Against Emerging Cyber Threats," *Journal of Multidisciplinary Research* 10, no. 1 (2024): 46–66.