International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(1s) 2026 pp. 1413-1421
https://doi.org/10.70917/ijcisim-2026-2469
Article

CYBER RISKS IN JORDANIAN PRIVATE HOSPITALS: A QUALITATIVE STUDY OF SOCIOTECHNICAL AND BEHAVIORAL BARRIERS TO STAFF SECURE PRACTICES

ABDALMOHADI ALRABABAH[1], HUDA IBRAHIM[2], ALAWIYAH ABD WAHAB[3]

[1]College of Arts and Sciences, School of Computing, Universiti Utara Malaysia
[2]College of Arts and Sciences, School of Computing, Universiti Utara Malaysia
[3]College of Arts and Sciences, School of Computing, Universiti Utara Malaysia
*Corresponding author: abd.alrababah@gmail.com

Abstract:

Background: Cyber risk threats to healthcare are escalating, with human behavior identified as a critical vulnerability. In Jordanian private hospitals, staff often bypass security protocols, yet no empirical study has systematically explored the sociotechnical and behavioral barriers in this resourceconstrained, culturally specific context.
Objective: To explore cyber risk challenges in Jordanian private hospitals, focusing on sociotechnical and behavioral barriers that impede staff engagement with secure practices.
Methods: Adopting an interpretivist paradigm, semistructured interviews were conducted with 18 IT professionals across five private hospitals in Jordan. Data were analyzed using thematic analysis following Graneheim and Lundman's framework. Trustworthiness was ensured through member checking, peer debriefing, audit trails, and reflexive journaling.
Results: Three overarching themes emerged: (1) technological infrastructure vulnerabilities (legacy systems, untested backups, password sharing), (2) operational risks (system downtime, diagnostic disruption, surgical cancellations, emergency diversion), and (3) systemic challenges (clinicalsecurity paradox, cascading failure chains, dual role of patient trust). Insecure behaviors were confirmed as instrumental adaptations to productivity pressure and fatigue, not careless errors.
Conclusion: Cyber risk vulnerabilities in Jordanian private hospitals are fundamentally systemic. Interventions must address technology, human behavior, organizational culture, and resource constraints simultaneously, shifting from preventioncentric to resiliencebased approaches.

Keywords: cyber risk; healthcare; sociotechnical barriers; resilience; Jordan; staff behavior; qualitative study

1. INTRODUCTION

Cyberattacks on healthcare systems are escalating globally, with the sector accounting for 24% of all cyber incidents in 2019 alone [1]. Between 2014 and 2016, 90% of hospitals reported at least one data breach, and nearly half experienced five or more [2]. Financial gain remains the primary driver [3,4], motivating 91% of data breaches [5]. Compromised medical data is highly valuable on black markets, enabling ransomware, extortion, and identity theft [6]. The average cost of a healthcare data breach reached USD $10.93 million in 2023 – the highest of any industry [7].

While technical safeguards such as firewalls, antivirus software, and encryption are essential, they are insufficient. Research consistently demonstrates that human behavior is a critical determinant of cybersecurity outcomes [8,9]. Healthcare professionals, operating under intense time pressure, fatigue, and a primary focus on

patient care, often engage in insecure practices – password sharing, use of unverified USB devices, and falling for phishing emails – not out of negligence but as instrumental responses to poorly designed workflows [10,11]. The healthcare environment thus presents a unique sociotechnical challenge, where clinical imperatives routinely override security protocols, creating what has been termed the "clinicalsecurity paradox" [12].

The cyberattack on the Jordanian Ministry of Health, as highlighted in the 2024 National Cybersecurity Report, marks a significant breach. Notably, while 7% of documented cyberattacks targeted the Ministry, none were reported to have targeted public or private hospitals directly – an omission that is critical given the potentially profound impact on healthcare institutions [13]. Preliminary evidence indicates that security concerns are a major barrier to electronic health record (EHR) adoption in Jordan, with staff reporting minimal security training [14].

Despite extensive research in Western contexts, the cybersecurity behaviors and barriers specific to Middle Eastern healthcare systems remain underexplored. No empirical study has systematically identified the sociotechnical and behavioral barriers within Jordanian private hospitals. This study addresses that gap.

2. PROBLEM STATEMENT

While technical safeguards against cyberattacks in healthcare are widely implemented, a critical and persistent vulnerability lies in the sociotechnical domain. Healthcare staff routinely bypass security protocols – sharing passwords, using unverified USB devices, and ignoring phishing simulations – as instrumental responses to productivity pressure, fatigue, and poorly designed security workflows [10,11]. In Jordanian private hospitals, no empirical study has systematically investigated the specific sociotechnical and behavioral barriers that lead to these insecure practices. The 2024 National Cybersecurity Report documented a major breach of the Jordanian Ministry of Health, yet attacks on hospitals remain underreported, and the underlying barriers to secure staff behavior in Jordanian private hospitals remain unknown [13]. Consequently, the prevailing preventioncentric cybersecurity model continues to be applied without adaptation to the local context, leaving hospitals exposed to ransomware, data breaches, and operational paralysis that directly threaten patient safety.

3. RESEARCH QUESTION AND OBJECTIVES

3.1 Research Question

Primary research question: What are the key sociotechnical and behavioral barriers perceived by healthcare staff that impede the implementation of effective cyber risk practices in Jordanian private hospitals?

3.2 Research Objectives

The objectives of this study are:

1. To explore the technological infrastructure vulnerabilities that contribute to cyber risks in Jordanian private hospitals.
2. To identify the operational risks arising from insecure staff behaviors and system design flaws.
3. To examine the systemic characteristics of healthcare delivery that perpetuate cyber risk vulnerabilities, including the clinicalsecurity paradox and cascading failure chains.
4. To generate evidencebased recommendations for resiliencefocused interventions tailored to the Jordanian private hospital context.

4. LITERATURE REVIEW

The escalating frequency and sophistication of cyberattacks on the global healthcare sector are well documented, with the average cost of a healthcare data breach reaching $10.93 million – the highest of any industry [7]. While technical safeguards are essential, a significant body of literature identifies human behavior as a critical determinant of cybersecurity effectiveness. Traditional research has often characterized users as the "weakest link" [15]; however, contemporary scholarship advocates a paradigm shift toward viewing staff as potential "human firewalls" when adequately supported [8].

The healthcare environment presents unique sociotechnical challenges that differentiate it from other sectors. The primacy of patient care frequently creates tension with security protocols, leading clinicians to adopt "workarounds" – instrumental behaviors designed to streamline workflows but which inadvertently introduce

vulnerabilities [16,17]. Furthermore, psychosocial factors including high stress, burnout, and fatigue significantly increase the likelihood of cybersecurity noncompliance among healthcare workers [18,19]. Specific risky practices documented in the literature include password sharing and reuse [20], elevated phishing susceptibility among clinical staff [21], unsafe USB device usage [22], and inadequate security practices associated with personal device usage [23]. Compounding these issues, cybersecurity training interventions often demonstrate limited lasting impact, as onetime awareness programs fail to address the underlying motivations driving insecure behaviors [24].

Despite extensive research in Western contexts, a significant gap exists regarding the Jordanian healthcare system. Preliminary evidence indicates that security concerns are a major barrier to EHR adoption in Jordan, with staff reporting minimal security training [14]. The 2024 National Cybersecurity Report documented a significant breach targeting the Jordanian Ministry of Health, yet attacks on hospitals remain underreported [13]. This study addresses that gap by employing qualitative methods to explore the contextual barriers and motivations shaping cybersecurity behaviors among healthcare staff in Jordanian hospitals.

5. METHODOLOGY

5.1 Study Design and Paradigm

This study adopted an interpretivist paradigm to explore the complex phenomenon of cyberattacks on healthcare information systems, particularly electronic health records (EHRs). A qualitative research design was employed to gain an indepth understanding of participants' experiences and perspectives regarding vulnerabilities, threats, and risks confronting private hospitals in Jordan. The objective was not to generate generalizable statistical data but to identify patterns of experience and perception that illuminate the contextual realities of cybersecurity in hospital settings.

5.2 Setting

The study was conducted across five private hospitals in Jordan. Hospitals were selected based on their willingness to participate and the presence of an established IT department.

5.3 Participants and Sampling

The target population comprised IT staff, IT managers, and information systems managers. Participants were selected using purposive sampling to ensure relevant expertise. Inclusion criteria required a minimum of five years of experience working with health information systems. Recruitment was conducted through telephone, email, and inperson invitations.

A total of 18 IT professionals participated. The sample consisted of 11 males (61.1%) and 7 females (38.9%). All participants held a bachelor's degree in information technology (n=12, 66.7%) or computer science (n=6, 33.3%). Professional experience ranged from 5 to 17 years (mean = 9.8 years, SD = 3.2). Participants held various roles: IT managers (n=5), system administrators (n=7), network security officers (n=3), and health information system coordinators (n=3). Table 1 summarizes the demographic characteristics.

Table 1. Demographic characteristics of participants

Characteristic	Category	n (%)
Gender	Male	11 (61.1%)
	Female	7 (38.9%)
Education	Bachelor's in IT	12 (66.7%)
	Bachelor's in Computer Science	6 (33.3%)
Role	IT Manager	5 (27.8%)
	System Administrator	7 (38.9%)
	Network Security Officer	3 (16.7%)
	HIS Coordinator	3 (16.7%)
Experience	5–9 years	10 (55.6%)
	10–14 years	6 (33.3%)
	15–17 years	2 (11.1%)

5.4 Data Collection Procedures

Data were collected through semistructured interviews conducted between August and December 2025. An interview guide was developed to ensure alignment with the research objectives, focusing on key areas including cyber vulnerabilities, cyberattacks, and associated risks. Interviews were conducted facetoface in participants' offices, with each session lasting approximately 25–35 minutes. The interviews were carried out in Arabic to facilitate clear communication. Field notes were taken to capture contextual information and support data interpretation. All interviews were digitally recorded with participants' consent and subsequently transcribed verbatim. Data collection continued until data saturation was achieved, defined as the point at which no new codes or themes emerged and previously identified codes were consistently repeated. Saturation was reached by the eleventh interview, and four additional interviews were conducted to confirm the adequacy of the sample.

5.5 Data Analysis

Following data collection, the interviews were systematically analyzed using thematic analysis, facilitated by NVivo software (version 13) to organize and manage the data efficiently. Data analysis was conducted concurrently with data collection, guided by the fivestep qualitative content analysis framework proposed by Graneheim and Lundman [25]. The analytical process comprised the following stages: (a) verbatim transcription of each interview; (b) division of the transcribed text into condensed meaning units; (c) abstraction and coding of these condensed meaning units; (d) sorting codes into subcategories and categories based on similarities and differences; and (e) development of main categories reflecting the core content of the data. Throughout the analysis, codes and themes were continuously reviewed, compared, and refined to ensure accuracy and consistency.

5.6 Trustworthiness

Given the interpretivist paradigm, measures to ensure trustworthiness were rigorously implemented in accordance with the framework established by Lincoln and Guba [26]. Credibility was established through member checking, enabling participants to validate the accuracy of the data collected. Additionally, peer debriefing sessions with colleagues and health information experts were undertaken during the thematic development phase. Dependability was ensured through comprehensive documentation of the research process, including data collection and analytical procedures, and the maintenance of a detailed audit trail. Confirmability was addressed by actively

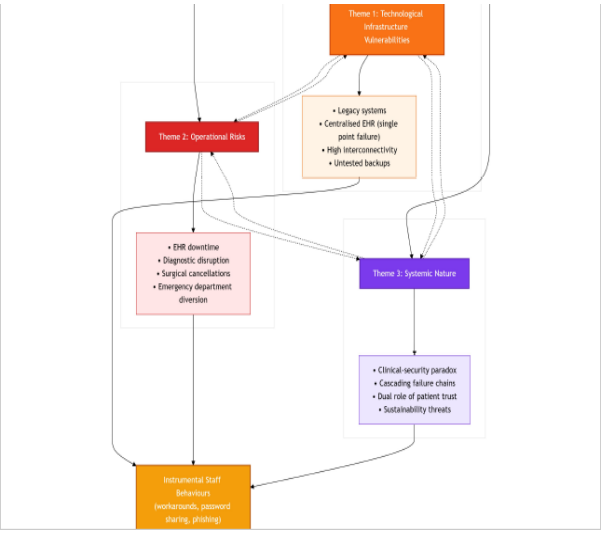
seeking participant feedback on emergent themes, ensuring that findings authentically represent participant perspectives. Transferability was facilitated through thick descriptive accounts of participant demographics, research context, and methodological approach. To mitigate interpretive bias, the researcher maintained a reflexive journal throughout the study.

6. RESULTS

6.1 Overview

Through the data analysis process, three main themes emerged: (a) technological infrastructure vulnerabilities, (b) operational risks, and (c) systemic nature of healthcare cyber vulnerabilities. Each theme was subsequently divided into subthemes and corresponding categories as in diagram 1.

Diagram 1. the data analysis process



6.2 Theme 1: Technological Infrastructure Vulnerabilities

Participants consistently described the technological infrastructure of modern hospitals as a complex and inherently vulnerable ecosystem, distinguished from other sectors by its fundamental prioritisation of clinical functionality and continuous operations over security considerations [27].

Legacy systems. A primary vulnerability was the pervasive reliance on legacy systems – unsupported software and hardware that remain in service for decades, accumulating "technical debt" that exposes hospitals to unpatched vulnerabilities due to prohibitive replacement costs and unacceptable clinical disruption. One IT manager stated: "We have a radiology system from 2012. The vendor no longer provides updates, but replacing it would shut down the department for two weeks – we cannot do that."

Centralisation of EHR systems. The centralisation of patient data within EHR systems creates a critical single point of failure. Participants noted that ransomware attacks can encrypt entire databases, paralysing hospital operations, yet affected systems cannot be simply shut down without endangering patients. A system administrator explained: "If the EHR goes down, doctors cannot access patient histories, allergies, or medication lists. They revert to paper, and errors increase."

Interconnectivity. The high interconnectivity of administrative, clinical, and diagnostic platforms enables attacks to cascade from lesssecure to critical systems, such as PACS and patient monitoring equipment, creating organizationwide crises. One participant observed: "An attack started in the billing department – a simple phishing email – and within hours, the MRI scheduling system was offline."

Backup system inadequacies. Backup systems were frequently compromised by design flaws, including storage on the same network segment as production systems and a lack of regular testing, rendering them nonfunctional at the moment of greatest need. An IT coordinator admitted: "We have backups, but we have never tested a full restore. I am not sure they would work."

6.3 Theme 2: Operational Risks

Operational risks represented the most immediate and visible consequences of cyber incidents, manifesting as direct disruptions to core clinical and administrative functions.

EHR system downtime. Ransomware attacks disable critical systems, forcing clinicians to revert to slower, errorprone paperbased processes and reliance on memory and verbal communication. A network security officer described: "During our last incident, nurses had to write medication orders by hand. It took three times longer, and we almost had a dosing error."

Diagnostic service disruption. Attacks targeting specialised systems such as PACS, LIS, and RIS created immediate bottlenecks in patient assessment and treatment planning, delaying test results and prolonging hospital stays. One participant stated: "When the lab information system goes down, we cannot receive blood test results electronically. Patients wait hours longer for discharge."

Surgical and procedure cancellations. Compromised clinical information systems prevented safe progression with scheduled procedures, leading to uncollected fees and postponed necessary interventions. An IT manager reported: "We had to cancel three elective surgeries last year because the preoperative checklist system was locked by ransomware."

Emergency department diversion. Paralyzed emergency services forced ambulances to redirect to other facilities, delaying critical care for timesensitive conditions. One participant noted: "Our ED was closed for six hours during an attack. An incoming stroke patient had to go to a hospital 15 kilometres away."

6.4 Theme 3: Systemic Nature of Healthcare Cyber Vulnerabilities

Participants revealed that cyber vulnerabilities are not isolated technical deficiencies but systemic characteristics arising from the fundamental nature of healthcare delivery itself.

Clinicalsecurity paradox. The very features that enable effective patient care – rapid information access, system integration, multiple users, external data sources, and continuous operations – are the same features that create cybersecurity vulnerabilities. As one participant explained: "We cannot put multifactor authentication on every workstation because nurses need to log in within seconds during a code blue. Security and care are in constant tension."

Cascading failure chains. A single weakness could precipitate organizationwide crisis. Compromise spreads from legacy systems to network entry points, enabling lateral movement to encrypt electronic health records, disrupt diagnostic platforms, force surgical cancellations, generate revenue loss, and erode patient trust. An IT manager stated: "One unpatched device in the waiting room became the entry point for an attack that shut down our entire hospital for two days."

Dual role of patient trust. Patient trust functions simultaneously as a vulnerability, a risk, and a protective factor. The high trust expectations that patients place in healthcare institutions make breaches particularly damaging to reputation. A participant observed: "After news of a breach, patients started asking whether their records were exposed. Some said they would not return." Yet trust also enables the open information sharing essential for effective clinical decisionmaking.

Sustainability implications. Smaller and resourceconstrained institutions face identical threats as larger organisations but with fewer resources. Cumulative financial, reputational, and operational impacts threaten longterm organizational viability. One network security officer from a small hospital lamented: "We cannot afford a dedicated security team. Meanwhile, the same ransomware attacking large hospitals is also attacking us."

6.5. Interconnections Among the Three Themes

The three themes are not isolated but dynamically interrelated. Technological infrastructure vulnerabilities (e.g., legacy systems, untested backups, centralised EHRs) create the preconditions for operational risks – a single unpatched device can trigger EHR downtime, diagnostic disruption, surgical cancellations, or emergency department diversion. These operational consequences are then amplified by systemic factors: the clinical-security paradox forces staff to adopt workarounds, cascading failure chains spread the impact across interconnected platforms, and eroded patient trust undermines long-term organizational sustainability. Conversely, systemic characteristics

perpetuate technological weaknesses (e.g., the imperative for continuous operation discourages legacy system replacement). Thus, each theme reinforces the others, forming a self-sustaining cycle of vulnerability.

7. DISCUSSION

This study aimed to explore the sociotechnical and behavioral barriers to secure cybersecurity practices in Jordanian private hospitals. The findings confirm that vulnerabilities are fundamentally systemic rather than isolated technical issues. Three interconnected themes emerged: technological infrastructure vulnerabilities (legacy systems, untested backups, password sharing), operational risks (downtime, workarounds, diagnostic disruption), and systemic challenges (clinicalsecurity paradox, cascading failure chains, dual role of patient trust).

A critical finding is that healthcare staff engage in insecure behaviors – password sharing, USB workarounds, ignoring phishing simulations – not out of negligence but as **instrumental responses** to productivity pressure, fatigue, and poorly designed security protocols. This aligns with Carboni et al. [10] and Mizrak et al. [11], who documented similar patterns in other healthcare contexts. However, this study provides the first empirical evidence from Jordanian private hospitals, a resourceconstrained, culturally distinct setting.

The clinicalsecurity paradox identified in this study – the inherent tension between patient care imperatives and security protocols – has been theorised but rarely documented through direct participant accounts in a Middle Eastern context [12,27]. Participants vividly described how the need for rapid logins, uninterrupted workflows, and continuous operations directly contradicts standard security recommendations, leading to unavoidable workarounds.

8. Limitations of the study must be acknowledged. First, the qualitative sample included only IT professionals; clinical staff (nurses, physicians, administrators) were not directly interviewed. Their perspectives on barriers and workarounds may differ. Second, the study was conducted in five private hospitals in Amman; findings may not be transferable to public hospitals or hospitals in other regions of Jordan. Third, social desirability bias may have influenced participants' reports of their own security practices. Fourth, the study did not include direct observation of staff behaviors, relying instead on selfreported and perceived barriers. Future research should include clinical staff perspectives, direct observation, and comparative studies across public and private sectors.

Implications for practice. The findings suggest that traditional preventioncentric cybersecurity models are mismatched to the healthcare context. Interventions must shift toward **resiliencebased approaches** that acknowledge that perfect security is unattainable. Key priorities include: (a) implementing regularly tested, segmented backup systems; (b) designing security protocols that accommodate clinical workflows (e.g., fast biometric logins); (c) moving from onetime training to repeated microsimulations with nonpunitive feedback; and (d) establishing anonymous reporting channels through which staff can flag security barriers without fear of retaliation.

9. CONCLUSION

This qualitative study explored cybersecurity challenges in Jordanian private hospitals through semistructured interviews with 18 IT professionals. The findings confirm that vulnerabilities are fundamentally systemic, embedded within technological infrastructure, operational processes, and the inherent characteristics of healthcare delivery. Three overarching themes emerged: technological infrastructure vulnerabilities (legacy systems, EHR centralisation, interconnectivity, backup inadequacies), operational risks (system downtime, diagnostic disruption, surgical cancellations, emergency diversion), and systemic challenges (clinicalsecurity paradox, cascading failure chains, dual role of patient trust). Critically, healthcare staff engage in insecure behaviors not out of negligence but as instrumental responses to productivity pressure, fatigue, and poorly designed security protocols.

Effective cybersecurity in Jordanian private hospitals cannot be solved by technology alone. It requires integrated sociotechnical approaches that address human behavior, organizational culture, workflow realities, and resource constraints simultaneously, with the goal of building resilience rather than achieving perfect security.

10. FUTURE RESEARCH

Based on these findings, six priority areas for future research emerge:

1. Clinical staff perspectives – Nurses, physicians, and administrative staff should be included as primary participants to capture their unique barriers and workarounds.

2. Intervention development – Design and test a lowcost, resiliencebased intervention targeting the specific barriers identified (e.g., automated backup verification, biometric logins, phishing microsimulations, anonymous reporting channels).
3. Comparative studies – Compare cybersecurity barriers across public vs. private hospitals and across different regions of Jordan.
4. Longitudinal observation – Direct observation of staff behavior's over time to document how workarounds evolve and how security policies are actually enacted.
5. Patient trust dynamics – Mixedmethods research exploring how actual or hypothetical breaches affect patient willingness to share sensitive information.
6. Integration with national policy – How can findings inform Jordan's National Cybersecurity Center reporting framework and healthcare sector regulations?

REFERENCES

1. Martignani C. Cybersecurity in cardiac implantable electronic devices. Expert Rev Med Devices. 2019;16(6):437-44.
2. Ponemon Institute. Sixth annual benchmark study on privacy & security of healthcare data. 2016.
3. Coventry L, Branley D. Cybersecurity in healthcare: a narrative review. Maturitas. 2018;113:48-52.
4. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems. Technol Health Care. 2016;24(1):1-9.
5. Bassett G, Hylender CD, Langlois P, Pinto A, Widup S. DBIR: 2021 data breach investigations report. Verizon. 2021.
6. Healthcare Information and Management Systems Society. 2020 HIMSS cybersecurity survey. 2020.
7. IBM Security. Cost of a data breach report 2023. IBM Corporation. 2023.
8. Zimmermann V, Renaud K. Moving from a "humanasproblem" to a "humanassolution" cybersecurity mindset. Int J Hum Comput Stud. 2019;131:169-87.
9. Hedström K, Karlsson F, Kolkowska E. Social action theory for understanding information security noncompliance in hospitals. Inf Manag Comput Secur. 2013;21(4):266-85.
10. Carboni C, Brightwell C, Halpern O, Freyer O, Gilbert S. Reconciling security and care in digital medicine. npj Digit Med. 2025;8(1):261.
11. Mizrak F, Demirel HG, Yaşar O, Karakaya T. Digital detox: exploring cybersecurity fatigue. Discov Ment Health. 2025;5(1):25.
12. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review. Technol Health Care. 2017;25(1):1-10.
13. Jordanian National Cybersecurity Center. National Cybersecurity Report 2024. Amman: NCC; 2024.
14. AlDwairi R, Tubaishat A. Factors affecting the adoption of electronic health records in Jordanian hospitals. Inform Med Unlocked. 2020;21:100459.
15. Schneier B. Secrets and lies: digital security in a networked world. New York: Wiley; 2000.
16. Koppel R, Metlay JP, Cohen A, et al. Role of computerized physician order entry systems in facilitating medication errors. JAMA. 2005;293(10):1197-203.
17. HadjiJanev M, Bogdanoski M. Cyber security in healthcare: a textbook. NATO Science for Peace and Security Programme; 2020.
18. Shanafelt TD, Hasan O, Dyrbye LN, et al. Changes in burnout and satisfaction with worklife balance in physicians. Mayo Clin Proc. 2015;90(12):1600-13.
19. Nobles C. Stress, burnout, and security fatigue in healthcare. J Cybersecur Res. 2022;7(1):42-58.
20. Inglesant PG, Sasse MA. The true cost of unusable password policies. In: Proc SIGCHI Conf Hum Factors Comput Syst. 2010:383-92.

21. Gordon WJ, Wright A, Aiyagari R, Landman A. Assessment of employee susceptibility to phishing attacks. JAMA Netw Open. 2019;2(3):e190393.

22. Clark R. USB devices as vectors for healthcare malware. J Med Syst. 2015;39(10):1-7.

23. Hovav A, Putri FF. Employees' compliance with BYOD security policy. Pervasive Mob Comput. 2016;32:35-49.

24. Bada M, Sasse AM, Nurse JR. Cyber security awareness campaigns: why do they fail to change behaviour? In: Proc Int Conf Cyber Secur Sustainable Soc. 2019:118-31.

25. Graneheim UH, Lundman B. Qualitative content analysis in nursing research. Nurse Educ Today. 2004;24(2):105-12.

26. Lincoln YS, Guba EE. Research, evaluation, and policy analysis. Rev Policy Res. 1986;5(3):546-65.

27. Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices. Med Devices (Auckl). 2015;8:305-16.

28. Sittig DF, Singh H. A sociotechnical approach to ransomware attacks. Appl Clin Inform. 2016;7(2):624-32.

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