Disaster Medicine and Public Health Preparedness

www.cambridge.org/dmp

The EDIT Survey: Identifying Emergency Department Information Technology Knowledge and Training Gaps

Daniel Kollek BSc MD, CCFP (EM)[1], David Barrera B.Eng[2], Elizabeth Stobert MA, PhD[2] and Valérie Homier MD, MSc, DM, FRCPC[3]

[1]Division of Emergency Medicine, McMaster University, Hamilton, ON, Canada; [2]School of Computer Science, Carleton University, Ottawa, ON, Canada and [3]Department of Emergency Medicine, McGill University, Montreal, PQ, Canada

Original Research

Cite this article: Kollek D, Barrera D, Stobert E, Homier V (2022) The EDIT survey: identifying emergency department information technology knowledge and training gaps. *Disaster Med Public Health Prep* **16**: 1007–1012. doi: https://doi.org/10.1017/dmp.2020.474.

First published online: 15 March 2021

Keywords:
disaster medicine; disaster preparedness; information technology; ransomware; cybersecurity, EMR

Corresponding author:
Daniel Kollek,
Email: kollekd@mcmaster.ca.

Abstract

Objective: To review Emergency Department internet connectivity, cyber risk factors, perception of risks and preparedness, security policies, training and mitigation strategies.

Methods: A validated targeted survey was sent to Canadian ED physicians and nurses between March 5, 2019 and April 28, 2019.

Results: There were 349 responses, with physicians making up 84% of the respondents (59% urban teaching, 35% community teaching, 6% community non-teaching hospitals). All had multiple passwords, 93% had more than 1 user account, over 90% had to log repeatedly each workday, 52% had to change their passwords every 3 months, 75% had multiple methods of authentication and 53% reported using a terminal where someone else was already logged in. Passwords were used to review laboratory and radiology data, access medical records and manage patient flow. Majority of the respondents (51%) did not know if they worked with internet linked devices. Only 7% identified an 'air gapped' computer in their facility and 76% used personal devices for patient care, with less than a third of those allowing the IT department to review their device. A total of 26 respondents received no cyber security training.

Conclusion: This paper revealed significant computer-human interface dysfunctionality and readiness gaps in the event of an IT failure. These stemmed from poor system design, poor planning and lack of training. The paper identified areas with technical or training solutions and suggested mitigation strategies.

Introduction

Computer networks are mission critical components of care delivery in modern hospitals. Hospitals, and in fact entire health care systems, have been rendered incapable of delivering care when their IT framework was compromised. This information is not new and neither are the events rare. Specialized essential medical equipment belonging to Hollywood Presbyterian Medical Center was infected with the Locky ransomware on February 5, 2016. Despite the assistance of law enforcement and reputable security vendors, after almost 2 weeks of stunted operations, Hollywood Presbyterian Medical Center paid a ransom of $17000 in Bitcoin to release their systems.[1] Locky was 1 of 31 different ransomware attack types identified since 1989,[2] targeting hundreds of millions of networked systems[3] with a frequency of up to 4000 per day.[4] On May 12, 2017 the WannaCry ransomware compromised 200,000 devices in 150 countries.[5]

Recent years have seen an increased frequency of attacks.[6] Furthermore, ransomware is increasingly expensive with (across all cyber-attack events) the average ransom increasing from USD $294 to USD $1077 in 2016.[7] In Canada, an October 2019 hack of Life Labs, the country's largest provider of medical lab diagnostic services, exposed the sensitive personal information of an estimated 15 million Canadians.

Apart from data management services in hospitals, devices that connect directly to the patient such as IV pumps are increasingly networked to enable remote control and monitoring. Network capabilities add to device complexity which increases the risk of malfunction.[8] These control points are designed for care providers and vendors, but can also be used by attackers.

Aside from patient data and active medical devices, targets can be any area that involves automation or data management including the hospital building itself. As proof of concept, hackers took control of a building's thermostats. The entire effort took a weekend.[9] Attackers can hack hospital refrigerators to cause blood and drug spoilage, alter climate-controlled transport or storage of organs to corrupt organs etc. In general, attackers will look for an entry point into the network, typically through a poorly secured device that is already on

SDMPH
SOCIETY FOR DISASTER MEDICINE & PUBLIC HEALTH

the network, and use this device to launch further attacks.[10] Despite all these high probability/high impact risks to mission critical systems, there has been almost no research into methods of cyber-disaster risk reduction.

Research Question

The goal of this study was to identify risk factors in Canadian Emergency Department's IT systems and identify possible risk reduction solutions. In attempting to identify areas of system vulnerability, the study collected quantitative data on the degree of network use and internet connectivity in the ED, existing security training, and the way that ED physicians and nurses understand the IT risks and perceive their level of preparedness for IT failures.

Methods

Design

A survey was developed based on expert medical and computer science opinion and after discussion with stakeholders. Ethics approval was obtained via McGill University's Faculty of Medicine Institutional Review Board (Study A02-E15-19A). The survey was hosted on a website and validated with a small sample, edited post trial and all test data was purged. The survey reviewed the clinical tasks in which electronic data is used, the devices being used to access or deliver data, the security measures to protect data, the general (anonymous) profiles of the respondents and the type of facility. Respondents were only exposed to questions relevant to their practice. The survey was available in French and in English and was open between March 5, 2019 and April 28, 2019. Recipients received an original email invitation and 2 follow-up reminders. There was no financial or other type of reward provided after survey completion. Participants were assured that participation in the research study was voluntary and if they decided not to participate, or withdraw from participating they would not be penalized. Anonymous data was collated and stored on secure servers with access only available to the research team.

Population

The resulting Emergency Department Information Technology (EDIT) survey was disseminated by email to 1076 members of the Canadian Association of Emergency Physicians (CAEP), 516 members of the Association des Medecins d'Urgence du Quebec (AMUQ), 193 members of l'Association des specialistes en médecine d'urgence du Québec, an estimated 350 members of l'Association des infirmières et infirmiers du Québec (AIIUQ), 1200 members of the National Emergency Nursing Association (NENA), 270 members of the Emergency Nurses Association of Ontario (ENAO), and 413 members of the Centre for Excellence in Emergency Preparedness (CEEP). It is difficult to accurately determine the denominator because many recipients belong to more than 1 mailing list; However, the research team estimates that at least 2500 discrete recipients received the survey. The survey targeted physicians and nurses working in a Canadian Emergency Department at the time of survey completion. Other professions such as pharmacist or patient care attendant were excluded as well as retired nurses or doctors not currently working in a Canadian Emergency Department. Residents were also excluded because they were not usually at 1 specific site and thus were not regular users and on multiple systems. Emergency departments were chosen as a target audience because they work under the added stress of high flow-through and rapid decision making with limited prior knowledge of the patient, making the reliance on electronic systems and subsequent risk even higher.

Data Analysis

Data was entered into an Excel spreadsheet for tallying, comparison and graphic generation purposes. Data was analyzed using descriptive statistics (mean or median).

Results

There were 349 responses to the survey, of which 84% were physicians. 59% of respondents worked in urban teaching hospitals, 35% in community teaching hospitals and the remainder in community non-teaching hospitals. Demographics of responders are outlined in Table 1.

69% of respondents reported having between 1 and 4 hospital passwords, 26% of respondents reported having between 5 and 9 passwords, and the remaining respondents reported having 10 or more passwords. 52% had to change their password every 3 months. Passwords were primarily used to review laboratory data and radiology data followed by accessing medical records and managing patient flow as outlined in Figure 1.

A total of 93% of respondents reported having more than 1 hospital user account, with 59% having 3 or more. Over 90% had to log into multiple systems repeatedly during the workday. 53% of respondents reported using an open terminal where someone else was logged in but not present. 75% of respondents worked at sites that had other methods of authentication, of which the most common were radio frequency identification (RFID) tap cards (40%) and magnetic swipe cards (28%) as outlined in Figure 2. 51% of respondents did not know if they worked at sites with internet linked devices. Where known, device frequency is outlined in Figure 3.

76% of respondents use personal devices at work for patient care. Of those, 77% used the hospital Wi-Fi and 23% directly accessed patient records using their personal device. 22% of those users had their device reviewed by the IT department. The most common personal device use was consulting a medical application followed by communicating with colleagues. The different uses are outlined in Figure 4.

98% of respondents stated that their hospital computers are linked to the Internet however only 7% were able to identify an 'air gapped' computer (a computer that is neither connected to the internet nor connected to other systems that are connected to the internet and thus relatively immune to network based attacks) in their facility.[11,12]

Regarding training, RNs were more likely to receive training on hospitals' software (72% versus 53% of MDs) and MDs on maintaining patient privacy (53% versus 33% of RNs). A total of 26% of doctors and 20% of nurses received no cyber security training whatsoever from their hospitals.

In the event of an IT failure, depending on the type of care, 44% to 80% of the respondents were aware of plans to deliver some aspect of patient care. 65% of respondents believed the facility they work in could resume full IT function in less than 24 hours and 40% thought that it would take less than 6 hours.

https://doi.org/10.1017/dmp.2020.474 Published online by Cambridge University Press

Table 1. Respondent demographics

Profession												
MD			RN			Other						
289			51			6						
Years in practice												
<10			10-19			20-30			>30			
123			86			80			58			
Type of facility												
Urban Teaching			Community teaching			Community non-teaching			Walk in clinic			Other
191			113			17			1			0
Province												
N&L	NS	PEI	NB	PQ	ON	MB	Sask	NWT	AB	BC	Nun	YK
3	17	3	4	137	102	15	13	1	20	32	0	1

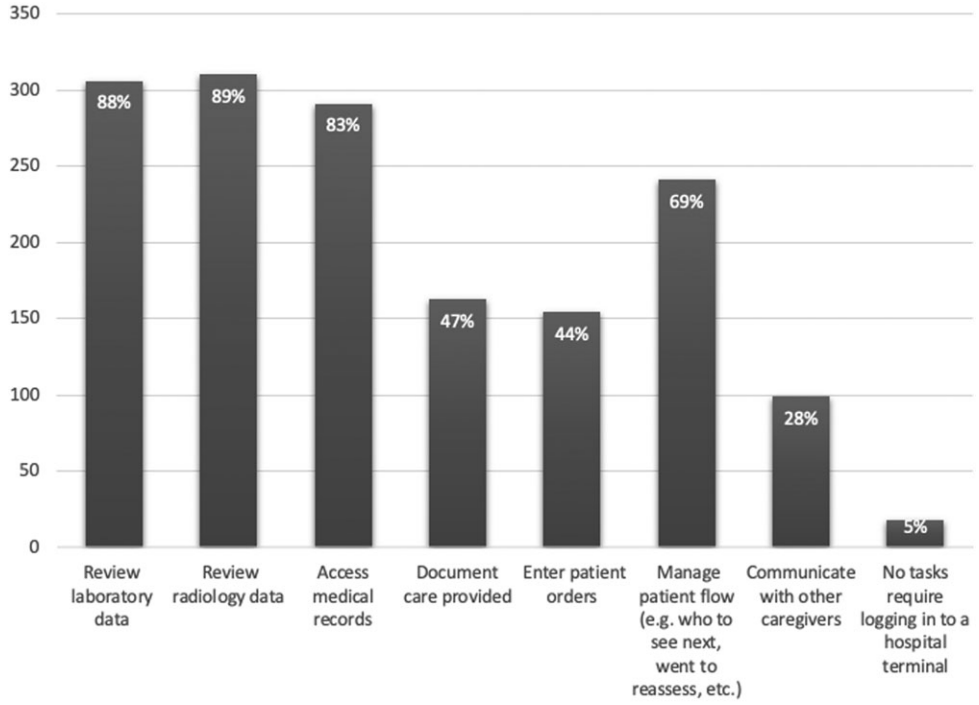

Figure 1. Common tasks requiring secure login.

Discussion

Prior studies

There are very limited studies on hospital cyber vulnerability and its clinical implications. Furthermore, despite the scant information available suggesting that there is a significant risk of cyber security breach in high intensity medical environments[13,14] there is no research on how to reduce this risk and avoid a disastrous failure of health care systems.

Interpretation

The most striking and unexpected findings of the study were the complexity of the network/caregiver interface, the degree to which it has become difficult to deliver any care without accessing a network, and the frequency of personal device use over hospital networks. All of these findings reinforced the need to protect hospital IT systems and have a response in place should the system collapse as a result of malicious activity or accident.

Regarding the caregiver interface with the computer networks, the paper identified a pervasive requirement to repeatedly log in to multiple software platforms. Health care providers' surveys reported that respondents used multiple accounts per shift in order to deliver care; This is clearly a dysfunctional and overly complex barrier to service delivery. Faced with the need to log in to multiple systems repeatedly, and adding the further complication of needing to change passwords on average every 3 months, it is no surprise that more than half of the respondents reported that they bypassed the safeguards and used other caregivers' open terminals. It is ironic that the security benefit of periodic password changes turns out

https://doi.org/10.1017/dmp.2020.474 Published online by Cambridge University Press

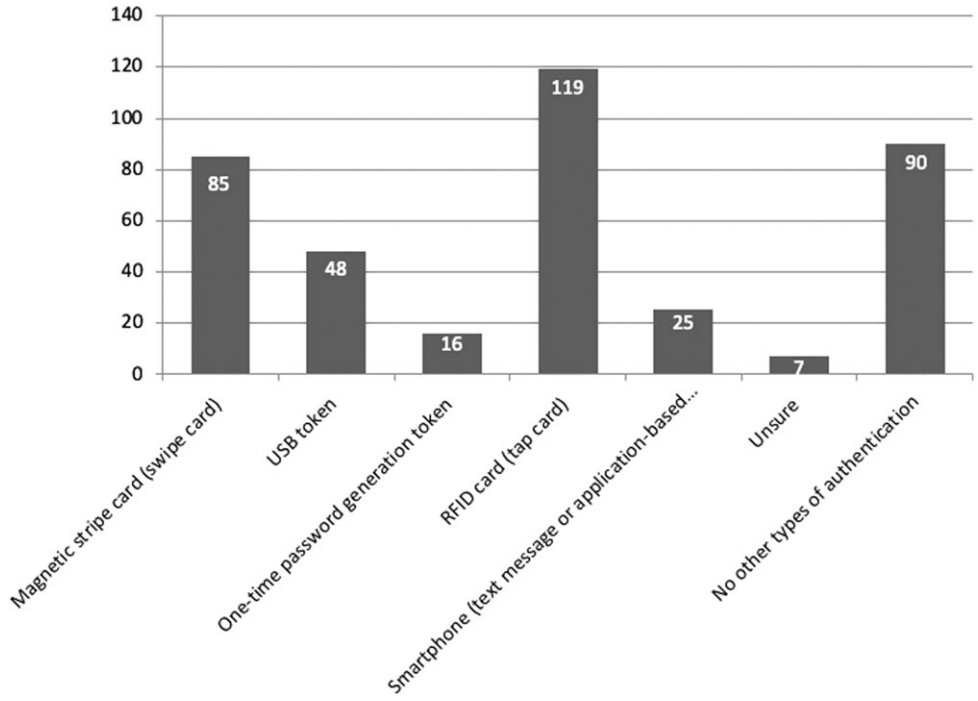

Figure 2. Other (non password) methods of authentication.

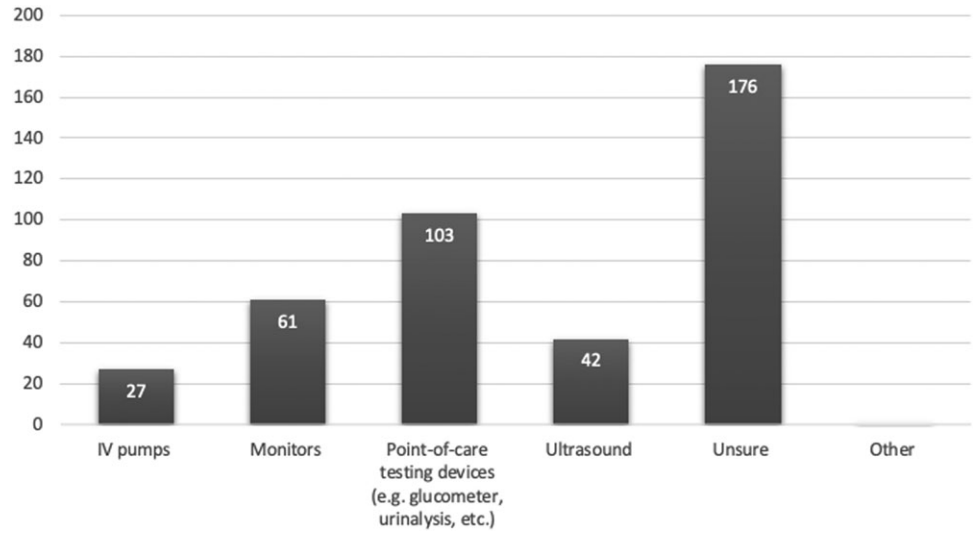

Figure 3. Networked devices.

to be weak at best.[15] In fact, when forced to change their password, people often choose a simple transformation of their previous password, making it no more difficult to guess.[16]

Login complexity leads to a perception by the user that security measures are a hindrance rather than a necessary evil and promotes poor computer hygiene. It is difficult to foster compliance with security measures if they become 1 more task that gets in my way of delivering care. The benefit of other forms of authentication such as RFID cards to minimize this behavior is minimal since amongst those using other forms of authentication, more than half still work around the security checks. Even if other authentication methods did provide more security, the underlying issue of complexity remains unaddressed.

These findings make it clear that in order to decrease the risks stemming from poor security compliance, there is a need for a secure, consistent, track-able, and ideally, uniform method of network access that does not require frequent changes by the end user and is equipped with safeguards in place to identify behavior that could stem from illegitimate access.

Regarding the use of personal devices, the vast majority of respondents use their personal devices to deliver some aspect of patient care, with the use of medical applications rating highest,

https://doi.org/10.1017/dmp.2020.474 Published online by Cambridge University Press

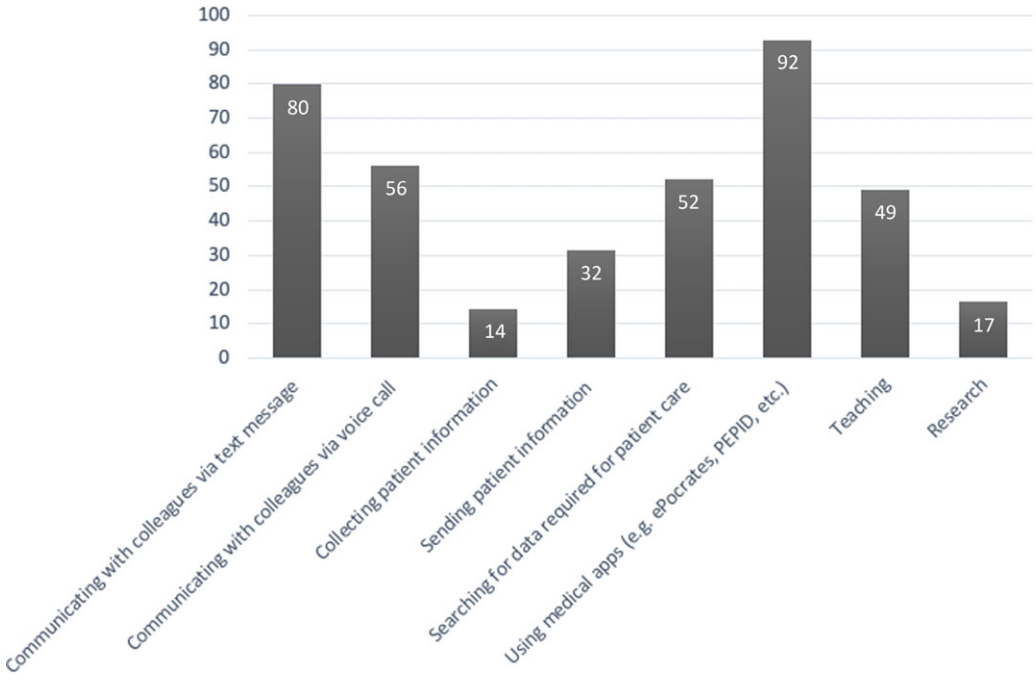

Figure 4. What tasks do you use your personal device for?

followed by communication with colleagues, and less frequently, directly accessing the patient medical record. Furthermore, 75% of respondents performed these tasks over the hospital's Wi-Fi network. Every external device that accesses the Wi-Fi network is a potential source of infection or infiltration of the hospital. A method that can be used to make external devices more secure is to install hospital software prior to allowing network access. Unfortunately, in this study less than a third of personal device users had their device reviewed by the IT department. Any attempt at risk reduction must include making this mandatory.

The study also identified end users' significant knowledge gaps that require remediation. 26% of respondents received no training from the hospital on best cyber security practices, while most respondents were unaware of an IT recovery plan, despite the fact that almost all sites had plans to deliver at least some aspect of care if their networked systems failed. These plans are useless if the end user is not aware of them. This topic should be mandatory in the context of hospital staff's overall disaster training. The variability in responses to this question (ranging from 44% to 80%) is a result of the question allowing 'yes' or 'no' answers to 7 components of a plan (for example a triage component, registration, accessing lab results etc.). Some sites were more aware of some components than others.

The almost total absence of 'air gapped' computers makes it unlikely EDs will be able to function during a system failure involving the EMR. This device can be periodically updated with an ED census through a removable storage device, allowing for a backup census of ED patients should there be an IT failure. During the collapse of the Glen site of McGill University Health Centre in Montréal on September 30, 2019 this proved very useful, and allowed the ED to continue providing care.[17] Air-gapped devices should be considered as a part of the hospital's cyber protection and response.

Most respondents did not know if they worked at sites with internet linked devices such as networked cardiac monitors and IV pumps. As far as the monitoring devices are concerned, they pose a potential data leak risk; the end-user has no control over the management of this data. The higher risk comes from the care delivery devices such as IV pumps,[18,19] that interface directly with the patient so that a disruption of their function can be immediately life-threatening. If caregivers are unaware that a device is liable to fail, in the event of a network failure they may miss a potentially life-threatening event. A hardcopy up to date list of networked devices should be immediately available in all departments providing patient care.

A final concern identified was the dispersal of patient data across multiple platforms and networks. This can lead to interference with marrying data to appropriate EMRs, posing the risk, albeit low in periods of normal function, of attributing data to the wrong patient. During periods after network shutdown, planned or unplanned in whole or in part, the different components will not reboot simultaneously. This could lead to mismatches of data from one rebooted software platform and another that is still not fully functional.

Strengths, Limitations, and Research Implications

This is the first study of its kind in Canada–a key strength that may open the field to further research. As with all surveys, sample size is a potential limitation. This is mitigated by common trends across much of the data which would indicate that there is validity and generalizability of the results. Another possible limitation is the reach of the survey as it was dependent on organizational membership and would not include responses from unaffiliated caregivers. Finally it is possible that some respondents submitted multiple responses but the authors feel this is highly unlikely as it would

https://doi.org/10.1017/dmp.2020.474 Published online by Cambridge University Press

require deliberately and maliciously ignoring the instruction to only reply to this survey once and only regarding 1 site.

Conclusion

The findings of this paper highlight the mission-critical importance of computer networks in healthcare coupled with significant knowledge, training and technical gaps. The recommendations of this paper are in 2 categories: the technical and the educational.

From the technical aspect, despite the importance of computer networks for the delivery of care in Canadian hospitals, this survey suggests that the existing systems are overly complex, dysfunctional, and incomplete, promote non-compliance with security measures and ultimately do not protect Canadian health care facilities from cyber events. Some of the findings, such as the multiplicity of passwords and logins and the absence of air-gapped backup computers, need to be addressed on a technical level. Other technical concerns, though only minimally addressed in this paper, are the inability of the end-user to assess the accuracy and validity of EMR data presented to caregivers and the inability to monitor actual performance of direct patient care devices.

From the educational aspect it is clear that there is room for further training regarding network vulnerability and fallibility, the need for and application of security measures, the use of personal devices, and the existence of recovery plans. Furthermore, if caregivers are aware of what networked devices in their hospital provide direct patient care, they may be prepared to respond if, and when these devices fail. Regular table top exercises and multidisciplinary simulations using test or training versions of the software used to deliver patient care could improve health care providers' preparedness for IT failures. Finally, since 75% of caregivers surveyed used their devices in providing care, it is unreasonable to not have hospital guidelines, training and software to ensure the safety and reliability of these devices.

Conflict of Interest. None of the authors have competing interests.

References

1. **Scott J, Spaniel D.** Combating the Ransomware Blitzkrieg. http://icitech.org/wp-content/uploads/2016/04/ICIT-Brief-Combatting-the-Ransomware-Blitzkrieg2.pdf. Accessed April 15, 2018.
2. **Yaqooba I, Ahmed E, Habib ur Rehman M**, *et al*. The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*. https://www.researchgate.net/publication/319527564_The_rise_of_ransomware_and_emerging_security_challenges_in_the_Internet_of_Things/citation/download. Accessed September 6, 2017.
3. **IBM**. *IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005*. IBM website. https://www-03.ibm.com/press/us/en/pressrelease/7815.wss. Accessed March 10, 2018.
4. **Ayala L.** Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention. Springer Science + Business Media New York. ISBN-13 (pbk): 978-1-4842-2154-9 ISBN-13 (electronic): 978-1-4842-2155-6.
5. **Alder S.** 40% of Healthcare Delivery Organizations Attacked with WannaCry Ransomware in the Past 6 Months. *HIPAA Journal*. https://www.hipaajournal.com/40-of-healthcare-delivery-organizations-attacked-with-wannacry-ransomware-in-the-past-6-months/. Accessed January 10, 2020.
6. **Ivanov A, Emm D, Sinitsyn F, Pontiroli S.** The ransomware revolution. *Kaspersky Security Bulletin*. 2016. https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/. Accessed April 7, 2018.
7. **Symantec Internet Security**. *Symantec Internet Security Threat Report – Volume 22, April 2016*. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. Accessed April 7, 2018.
8. **Alemzadeh H, Iyer RK, Kalbarczyk Z, Raman J.** Analysis of safety-critical computer failures in medical devices. *IEEE Security & Privacy*. 2013; 11(4):14–26.
9. **PenTest**. Thermostat Ransomware: a lesson in IoT security. PenTest Partners website. https://www.pentestpartners.com/security-blog/thermostat-ransomware-a-lesson-in-iot-security/. Accessed April 7, 2018.
10. **van Oorschot PC.** Computer Security and the Internet: Tools and Jewels. 2020, Springer, New York. Chapter 6, pages 174-175.
11. **Zetter K.** Hacker Lexicon: What is an air gap? https://www.wired.com/2014/12/hacker-lexicon-air-gap/. Retrieved October 2, 2020.
12. **Lemos R.** NSA attempting to design crack-proof computer. ZDNet News. CBS Interactive, Inc. Accessed October 2, 2020.
13. **Albarrak AI.** Information Security Behavior among Nurses in an Academic Hospital, *HealthMED*. 2012;6(7)2349–2354. https://www.researchgate.net/profile/Ahmed_Albarrak/publication/289103603_Information_Security_Behavior_among_Nurses_in_an_Academic_Hospital/links/5dc07322299bf1a47b153e07/Information-Security-Behavior-among-Nurses-in-an-Academic-Hospital.pdf Accessed March 9, 2020.
14. **Koppel R, Smith S, Blythe J, Kothari V.** Workarounds to computer access in healthcare organizations: You want my password or a dead patient? *Stud Health Technol Inform*. 2015;208:215–220.
15. **Chiasson S, van Oorschot PC.** Quantifying the Security Advantage of Password Expiration Policies. *Designs, Codes and Cryptography*. 2015;77(2): 401–408.
16. **Zhang Y, Monrose F, Reiter M.** The security of modern password expiration: An algorithmic framework and empirical analysis. Proceedings of the ACM Conference on Computer and Communications Security. 2010;176-186.
17. **Marc Beique**. Update: Computer system failure, McGill University Heath Care website https://muhc.ca/news-and-patient-stories/news/update-computer-system-failure Accessed July 8, 2020.
18. **Perry SJ, Wears RL, Cook RI.** The role of automation in complex system failures. *J Patient Saf Risk Manag*. 2005;1(1):56–61.
19. **Bagalio SA.** When systems fail: Improving care through technology can create risk. *J Healthc Risk Manag*. 27(4):13–18.