Understanding Cybersecurity Practices in Emergency Departments

Elizabeth Stobert[*], **David Barrera**[*], **Valérie Homier**[†], **Daniel Kollek**[‡]
[*]School of Computer Science, Carleton University
[†]Department of Emergency Medicine, McGill University
[‡]Division of Emergency Medicine, McMaster University

ABSTRACT
Emergency departments (EDs) have unique operational requirements within hospitals. They have strong availability demands, are staffed by rotating personnel, and must provide services as quickly as possible. Modern EDs are also heavily computerized, and as such cybersecurity practices play a key role in meeting the expected operational standards. To better understand the cybersecurity challenges in EDs, we conducted a survey asking 347 ED personnel across Canada about their cybersecurity practices. The survey collected information relating to authentication and password management, use of personal devices for handling patient data, Internet connectivity on personal and hospital systems, and institutional security policies. Our results show that across multiple hospitals, deployed computer security systems fail to integrate with the requirements of staff and patients, leading to interruptions and inefficiencies.

Author Keywords
Security, Usability, Medicine, Hospitals

CCS Concepts
•**Security and privacy** → *Social aspects of security and privacy;*

INTRODUCTION
Hospitals and clinics worldwide are becoming increasingly connected. Patient records are digitized and accessible to staff across departments, lab results are transmitted and viewed remotely, and clinicians use hospital computers to look up information. The increased use of information technology (IT) in hospitals has many advantages, but with the increased dependence on IT, the risk of failure also grows.

In 2017, one in five hospitals in Canada reported falling victim to at least one cybersecurity incident [22]. These attacks disrupted access to hospital resources and services, interfering with patient care. In the United Kingdom, 80 hospitals were infected with the *WannaCry* ransomware in 2018, incurring downtime and patient data loss [20]. Analysis of these attacks revealed that hospitals were not being explicitly targeted, but were rather caught in the crossfire of large-scale untargeted cyberattacks looking for unpatched Internet-connected systems.

Prior work has investigated cybersecurity practices in hospitals [9, 11, 12, 2], finding that the ability to provide quick and effective care is often at odds with hospital IT policy. For example, integrating software from multiple vendors tends to require multiple distinct sets of user credentials which must be entered multiple times and on multiple systems. To achieve their primary task (patient care), healthcare professionals find workarounds to bypass these policies; systems are left permanently logged in, software updates are not applied, and in some cases default passwords are never changed (or set to a simple shared password) to facilitate multi-user use. These practices contribute to increased exposure to attacks.

The literature has confirmed that these cybersecurity practices are common across hospitals and clinics, but emergency departments specifically have received less attention. Emergency departments (ED) have unique operational requirements within hospitals, since they are the hospital's front line in the event of a disaster or outbreak. Moreover, EDs mostly treat new (unregistered and without appointment) patients that have a wide range of illnesses and conditions. The dynamics of an ED make it even more important for personnel to avoid downtime due to logins and system patching.

In this paper we report on a survey of cybersecurity practices in Canadian emergency departments. We were interested in whether the practices of doctors and nurses in the ED differed from those of staff in other departments. We were interested in coping strategies surrounding authentication tasks and use of personal devices, but also asked participants about data privacy and integrity. The paper also sheds light on cybersecurity practices in the Canadian healthcare system.

BACKGROUND
The integration of IT services into hospitals and other medical environments has been pervasive, and nearly all aspects of medical care have been computerized in some way. This includes computerization of medical records, diagnostic equipment (e.g. ultrasound), point-of-care testing devices (e.g. glucometers), patient monitors, and planning and management

CHI '20, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6708-0/20/04 ...$15.00.
http://dx.doi.org/10.1145/3313831.3376881

software for healthcare professionals. This move to digitization has raised significant usability issues, along with risks to cybersecurity and patient privacy.

The study of IT practices in medical environments has consistently found incompatibilities between healthcare workers' mental models and the use of IT infrastructure. Smith and Koppel [21] identified 45 scenarios where technology infrastructure failed to accurately support either clinicians' mental models or reality. In one example, a computer system allowed for input of very granular categories, and this (false) specificity was misguiding to clinicians.

Digital replacements for analogue tools can have subtle feature differences that greatly impact medical work. Pennathur et al. [16] noted flexible space for comments was lost when transitioning to an electronic ED patient status board, which impacted collaboration and communication. The Activity-based Computing (ABC) framework [5] suggests reorganizing digital medical work around activities, rather than workstations, to better support medical staff.

Timeliness is an important aspect of effectiveness in delivering, coordinating and managing medical care. As such, IT infrastructure for medical contexts must be designed to support temporal planning and coordination [3, 14] in both the short and long term. In addition to coordination and planning, temporal measures are often used to gauge the quality of team performance and care delivery. Kusonoki and Sarcevic [13] analyzed temporal awareness in a trauma centre and proposed an improved display that highlighted time-based information to provide increased visibility for staff.

When IT infrastructure and IT security policy interfere with the ability of a clinician to give care, the circumvention of the policy (or even the technology entirely) is common practice [6]. Koppel et al. [12] analyzed the circumvention of barcoded medication administration systems in hospitals, finding 15 types of workarounds caused by a variety of technical (e.g., failing batteries or WiFi loss) and non-technical reasons (e.g., emergencies, unreadable barcodes). In these situations, the observed workarounds could lead to wrong doses or medications delivered at the wrong time, despite users' good intentions.

AlKabani et al. [2] investigated the role of socio-organizational factors on the adoption of IT security compliance. Through a survey of 300 hospital staff in Oman, they concluded that successful deployment of IT policies depends on more than simply users' attitude and behaviour. Socio-technical factors such as training, management commitment, and accountability play a critical role in how policies are received and implemented. Hedström et al. identify the control-based compliance model as problematic in healthcare situations, and instead propose *value-based compliance* as a solution [10].

Cybersecurity and Authentication

Prior work examining authentication practices in medical environments shows disconnects between healthcare practitioners' attitudes toward authentication and their behaviour. Medical professionals engage in insecure authentication practices such as password and session sharing, but claim that these behaviours are necessary for accomplishing their tasks (i.e., delivering patient care) [11, 6]. A 2012 survey of 352 nurses at a teaching hospital in Saudi Arabia [1] found that while most respondents appeared to understand the importance of authentication for access control, many respondents still engaged in password- and session-sharing. A 2014 survey of 432 nurses in Japan [15] found that these nurses had a clear understanding of security goals, but limited understanding of how their actions might impact cybersecurity in the hospital.

Alternative approaches to authentication have also been examined in the medical context. Heckle [9] documented and analyzed the deployment lifecycle of a single sign-on (SSO) solution as part of a larger risk management program. Deploying the SSO solution proved challenging in many points, most of which were not technical; hospital staff had grown accustomed to circumventing authentication when necessary to focus on patient care, while the SSO solution required them to develop new mental models of the system. Adoption of the SSO solution ultimately required extensive training of employees to return to pre-SSO levels of productivity.

The design patterns inherent in traditional authentication paradigms can also be problematic in the context of the "nomadic, dynamic, interrupted, and cooperative" [4, p. 357] hospital environment. Bardram [4] and Savage [19] describe how the processes of logging-in and logging-out interrupt workflows, and give unauthorized users access to ongoing sessions when another user has not explicitly ended that session. Bardram [4] proposes using proximity-based computing to address this problem, but even with technological progress toward ubiquitous computing, these technologies have not been realized in practice.

Emergency Departments

Emergency Departments are responsible for providing initial treatment for patients (most often without prior appointment or registration) suffering from a wide range of illnesses. As such, they must operate 24/7 and must be able to handle bursts of patients (e.g., in case of outbreaks or disasters). In line with national and international trends, EDs in Canada are increasingly relying on IT infrastructure to provide service. Networked computers and devices are used throughout the patient flow from intake to discharge. Emergency medicine is a distinct sub-discipline in medicine, but it is unclear whether this distinction affects the cybersecurity risks affecting EDs. In this study, we investigate cybersecurity practices to better understand the challenges affecting Emergency Departments.

Healthcare in Canada

As mandated by the Canada Health Act [8], healthcare in Canada is publicly provided by provinces and territories. Healthcare in Canada is a single-payer system, where all patients are covered by the provincial insurance corresponding to their province of residence. Each province and territory operates a government-run health insurance plan that is funded by taxes. Physicians bill the province/territory directly, so patients do not pay for healthcare at the point of delivery. The majority of costs are covered by the provincial health insurance plans, with a few exceptions that vary by province, such as prescription drugs, dental care, and eye care.

Because healthcare is not privatized, most hospitals in Canada are teaching hospitals affiliated with universities and their staff includes residents and medical students. The public nature of Canadian hospitals affects their budgets, which in turn shapes the resources available for IT services, including security.

STUDY

Our goal in this work was to obtain an initial sense of the landscape of cybersecurity in Canadian Emergency Departments, and to do this, we chose to conduct a survey study. We had contacts in partner organizations who were willing to distribute a questionnaire, and we wanted to take advantage of the opportunity to obtain a broad sample of participants. A survey also allowed us to ask about a comparatively wide variety of topics relating to security in Emergency Departments.

Hospital Visits

As part of the background phase of the project, we toured Emergency Departments at three hospitals located in Quebec and Ontario, and were able to meet with hospital IT departments (including management) to discuss their security policies, practices, and concerns. During these tours, we were shown the technology in use in the EDs, and were able to informally chat with hospital staff about the security constraints and considerations in their work. Although we did not conduct formal interviews, these consultations shaped the questions we included in our survey.

Survey

We developed a survey instrument with 28 questions that asked about cybersecurity practices in Canadian Emergency Departments. The survey included general questions about passwords and authentication in the Emergency Department, the security policies in use on accounts, systems, and devices in the ED and hospital, the level of Internet connectedness in the ED, and about IT security training and preparedness. We also asked a few demographic questions. The full list of questions can be seen in Appendix A.

The length of the survey was restricted by the organizations through which we distributed the survey, so we kept our focus on high-level questions and issues that were likely to affect most or all of our respondents. Because we were targeting nurses and physicians (rather than hospital IT management), we asked questions about the day-to-day interactions with devices and policies, rather than the policies themselves. We were particularly interested in how much awareness of connectedness, policies, and security had filtered down to healthcare professionals who interact directly with patients. Compliance was not the main focus of our work, rather we were interested in respondents' awareness of security, and actual day-to-day practices and experiences. Our survey questions addressed issues likely to affect the ED, but were not ED-specific. We pilot tested the survey on a small group of ED staff, which led to clarifications in the wording of a few questions.

We deployed the survey from March to April 2019. We specifically recruited nurses and physicians actively working in a Canadian Emergency Department at the time of the survey. We excluded residents, paramedics, pharmacists, and patient care attendants, as well as retired nurses and doctors. The survey was advertised through the mailing lists of six Canadian professional organizations of emergency physicians and nurses[1]. Overlap across associations and mailing lists makes it challenging to know exactly how many people received the advertisement, but our conservative estimate is that over 1500 nurses and physicians received the invitation to participate.

The survey was translated and available in both official languages (i.e., English and French). We did not pay respondents, and there was no external incentive offered for participation in the survey. The survey was approved by the research ethics committees at our universities.

Participants

We received 347 completed surveys, of which 85% were completed in English, and the remaining 15% in French. Our sample was made up primarily of doctors: 83% of respondents identified themselves as MDs, 16% of respondents were nurses (either registered nurses or registered practical nurses), and the remaining respondents did not disclose their job category. We had responses from hospital personnel with all levels of experience, ranging from less than 10 years experience up to more than 30 years experience.

Our recruiting was biased by the organizations that were willing to distribute our survey link, and accordingly, most participants practiced in either Quebec (39%) or Ontario (29%). Quebec was over-represented in the survey sample, and British Columbia (9%) was underrepresented, but in general, the distribution of respondents was similar to that of the Canadian population. The overwhelming majority of our participants worked in teaching hospitals: 55% in urban teaching hospitals, and 32% in community teaching hospitals.

RESULTS

Passwords and Logging In

Authentication is one of the most ubiquitous security tasks, and the Emergency Department is no different. Figure 1 shows the distribution of number of hospital passwords for all participants. The vast majority of respondents (95%) had 9 or fewer passwords. Most respondents were allowed to choose their own passwords (73%), and 74% of respondents said that password reuse was allowed by their hospital IT systems. 46% of participants said that they were required to change passwords quarterly, and 30% of participants said that there was variability in how frequently they were required to change their passwords.

Passwords are not the only method of authentication used in the ED. Figure 2 shows the frequency of use of other forms of authentication. Card-based authentication (whether a magnetic swipe card (24%) or RFID proximity card (34%)) was the most frequently reported other means of authentication.

[1]The Canadian Association of Emergency Physicians (CAEP), the Association des Médecins d'Urgence du Québec (AMUQ), the Association des infirmières et infirmiers du Québec (AIIUQ), the National Emergency Nursing Association (NENA), the Emergency Nurses Association of Ontario (ENAO), and the Centre for Excellence in Emergency Preparedness (CEEP).

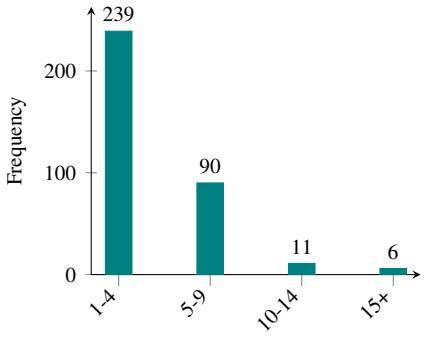

Figure 1: Number of reported hospital passwords.

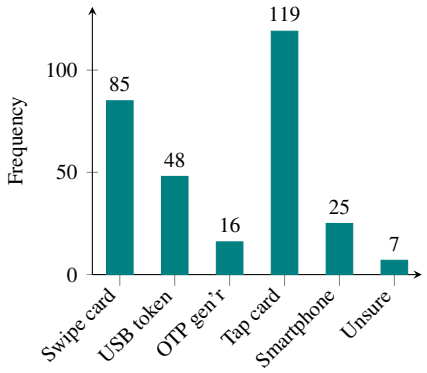

Figure 2: Additional types of authentication used in the ED.

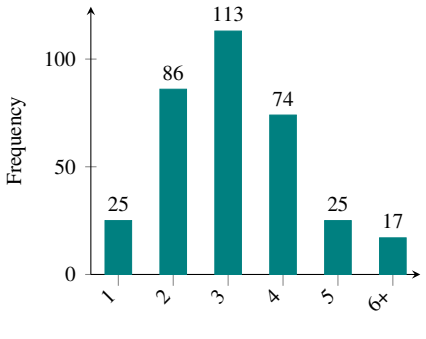

Figure 3: Number of accounts needed in a routine work day.

These authentications are used to log in to a variety of hospital IT systems. Participants most frequently reported having to log in to view patient data, such as radiology (89%) and laboratory data (88%), and to access medical records (84%). Hospital IT systems also typically require logins for managing patient flow (69%). Less frequently, doctors and nurses are required to log in to document care decisions (47%), enter patient orders (44%) and communicate with other caregivers (29%).

Not all accounts are used daily, and we were interested in how many accounts were used in a typical working day. 33% of respondents said they accessed three accounts in a usual workday (Figure 3). Of course, some accounts are used multiple times per shift: 90% of respondents said they had to log into at least some systems more than once per shift, and 43% said they had to log into all systems more than once per shift. Account logins are also frequently shared – 53% of users reported regularly using a system under another user's login.

The Connected Emergency Department

The vast majority of respondents (97%) said that they were able to access the Internet from computers in the Emergency Department. Connectedness is fast escaping the bounds of computers though, and medical IoT devices are replacing their offline counterparts. Respondents were most likely to say that their ED had connected point-of-care testing devices (e.g., glucometers or urinalysis) (30%), followed by monitors (18%), ultrasound (12%), and IV pumps (8%). However, 39% of respondents said that they were unsure about which devices in their ED were Internet-connected.

For EDs with both Internet-connected devices and offline devices, integrating all records into the electronic medical record (EMR) is an important issue for data availability and integrity. Of the respondents who said that this was an issue in their ED, 41% were unsure if such a protocol existed. 34% said that there was a protocol, and 21% said that there was no protocol. Data corruption in the EMR (e.g., results that contradict each other) can result from these integration procedures, but only 26% of respondents said that their ED had processes in place to detect these data corruptions.

Personal Devices in the ED

Many hospital personnel use personal devices at work, whether to look up information, communicate with colleagues, or other work-related tasks. The organizational structure of most Canadian hospitals, where doctors are independent contractors with one (or more) hospital affiliation(s) makes this situation even more relevant. BYOD (Bring Your Own Device) has been a significant topic in security for some time, and managing these devices can be a complex task for IT departments.

76% of the doctors and nurses who completed our survey said that they used a personal device (i.e., one not provided by the hospital) for assistance in providing care. Of those, the most frequently cited activities were using a medical app (93%) (e.g., ePocrates, PEPID), communicating with colleagues via text message (80%) or phone (56%), searching for information related to patient care (52%), and teaching-related tasks (49%). Respondents were less likely to use their personal device for collecting (14%) or transmitting (31%) patient information.

Nurses and physicians are well aware of the importance of patient privacy. When using personal devices, our respondents reported using a number of different strategies to protect their patients' privacy. Primarily, respondents said that they avoided sending any personally identifying information (77%), but also said that they relied on strategies such as deleting images (43%) and messages (38%). 23% said that they tried to combine out-of-band channels to dissociate patient identifiers from medical data (e.g., texting a photo to another physician, but calling on the phone to discuss). Participants were less likely to say that they rely on privacy tools such as private browsing mode (5%) or connecting to the hospital VPN (22%) to protect patients' privacy.

Of the respondents who said they used a personal device at work, 77% said that they were able to connect to the hospital WiFi. However, most people (69%) were not able to connect that device to the hospital network (allowing them to access internal resources such as patient data repositories). About 75% of participants said that their hospital IT department had no interaction with their device, including providing or installing software.

Training

The majority of respondents (75%) had received at least some kind of formal IT-related training from their hospital. Of the respondents who had received training, they were most likely to have been trained in the use of hospital software packages (75%) and protecting patient data (65%), and fewer participants (28%) said that they had received training directly related to cybersecurity. In our survey, nurses were slightly more likely to report training than physicians: 80% of nurses reported having received formal IT training, compared to 74% of doctors. However, fewer nurses (11%) reported having received cybersecurity training than doctors (22%).

DISCUSSION

We surveyed 347 Canadian doctors and nurses working in Emergency Departments about the cybersecurity practices, training, and connected devices in their hospitals. We found that our respondents handle many security tasks, including managing multiple passwords, other authentication tokens, and frequent password changes. They use multiple IT systems for a variety of work tasks, including viewing patient data, accessing medical records, and managing patient flow; and log into these systems multiple times in every shift. This results in circumventions of security: more than half of respondents admitted to using systems under another person's login.

Cybersecurity is undoubtedly an important concern for hospitals, and particularly for Emergency Departments, which serve as the front line in of the hospital in case of accidents or disasters. EDs need to maintain functionality, which includes keeping diagnostic and communication tools connected.

The results of our survey suggest that the security problems affecting Emergency Departments closely resemble problems in other hospital and medical contexts. ED personnel are overburdened with security tasks, which leads to circumvention [11, 6] and attendant cybersecurity risks. Although ED staff in our study seemed to recognize the importance of privacy and security, we found that security interrupts their ability to deliver patient care, and that they may inadvertently risk patient privacy through a lack of detailed understanding of technology. This speaks to the tension between security understanding and implementation found in similar studies [1, 15].

Securing the Canadian Emergency Department

Because the majority of Canadian hospitals are publicly funded, they typically are not especially affluent. IT departments are making do with a limited budget that must support keeping devices online and secure, training, and management of all other IT services. Solutions such as recommending that EDs be upgraded to the latest Internet-connected devices are not feasible, and the integration between connected and offline devices is likely to plague EDs for the foreseeable future. In addition to the tensions between users and security, the pragmatic challenges (such as financial impact) must be considered in evaluating potential security solutions for EDs.

Technological Awareness

Hospital personnel are well versed in the need for patient privacy. However, we were concerned by our respondents' lack of awareness of how patient data intersects with technology in the Emergency Department. More than a third of our respondents said that they were unsure which devices in their ED were connected to the Internet, and respondents frequently said that they shared patient data via their personal devices without using privacy tools.

One potential problem with data being shared on personal devices is that those devices may be vulnerable to security risks resulting from outdated operating systems. Google estimates that only 10% of Android devices are running up-to-date versions of the operating system [7]. Compelling users to update their devices is difficult in any situation, but it is particularly difficult for organizations to enforce security policies on unmanaged devices. The problem is compounded by the indirect relationship between doctors and hospitals.

The lack of awareness of how data is stored and transmitted also emerges in respondents' lack of awareness of how data is integrated into the medical record. Personnel who do not understand how data flows through the system create vulnerabilities when there is a potential for data to be inserted, corrupt data to go unnoticed, etc. Training might be one way to address this problem, but we speculate that EMR software could further highlight the relationship between data sources and provenance, and flag inconsistencies for remediation.

Data Deletion

We were taken aback by the finding that most practitioners do not use the privacy tools built into their devices, such as private browsing mode. Instead, it appeared that respondents were relying on manual deletion of files as a means of ensuring patient privacy. This carries significant security concerns, and highlights mismatches in mental models between users and devices. Data deleted via the user interface is generally not explicitly "erased" on the hard drive or storage media. Instead, the data location is simply marked as available to be rewritten with new data. However, there is no guarantee that this space will actually be rewritten; deleted information can often be recovered from nominally erased locations [18].

Another element of this problem is that data on mobile devices can be unwittingly shared via automatic cloud backups. Users are unlikely to change default settings, and it can be difficult to know exactly when copies of files are made, and where they are stored [17]. If identifiable patient information is saved in the cloud, it may not be deleted when users believe it is.

Technical solutions to the problem of secure deletion are limited, and one commonly recommended method of secure data deletion is to encrypt all data, making it undecipherable without with encryption key. However, encrypting data has its own usability challenges [23], and can lead to unintended data loss if the key is lost. From the perspective of BYOD, the challenge is to create different practices for different categories of photos/messages etc. One idea might be to create a secure messaging app designed for use by medical personnel, and recommend that doctors and nurses use that app when exchanging this type of information. The app could be designed to encrypt data, and prevent uploads to cloud servers, without impacting the configuration of other applications on the device.

Training

One finding of our survey was that comparatively few of our respondents had received any formal training on cybersecurity topics, and respondents were more likely to say that they had received training on other IT topics such as software packages than on cybersecurity. We are hesitant to recommend training as a panacea to security problems: poorly designed security software will always compel users to find workarounds, even if they have been properly trained, but we do think that hospitals should consider including training on IT security issues affecting the hospital.

The nurses in our sample were slightly more likely to say that they had received IT training, and this highlights one potential barrier to implementing training programs in the ED. Because doctors do not work for hospitals, hospitals have difficulty demanding compliance with IT standards such as training. This suggests that security training mandates might need to come from a higher body, such as the Provincial Colleges of Physicians and Surgeons.

CONCLUSION AND FUTURE WORK

In this paper we investigated cybersecurity practices in Canadian Emergency Departments. We found that doctors and nurses handle many security events in an average workday, which may detract from their primary medical tasks. We also identified circumventions of security policies such as shared logins or using personal devices for medical-related tasks. Our findings support what is seen in the literature about cybersecurity in hospital environments, and suggests that many of the same issues affecting IT security in hospitals also affect the Emergency Department.

One of our research questions was whether the characteristics of security in the Emergency Department differ from those seen in other medical contexts: while we do not have enough evidence to conclude that they are entirely the same, our results do suggest that many of the challenges are similar. A more in depth study of the ED could provide a more conclusive sense of similarities and differences.

This study took a high level approach, and the methodology used did not allow us to delve deeply into the details of participants' security practices. However, the results of our survey provide an initial overview that will help to fine tune areas of interest for future study. Particularly, we think there is an need for more detailed qualitative study of security in EDs, investigating more focused questions such as how personal device use affects patient privacy. As well, it would be interesting to triangulate the findings here with surveys of hospital IT departments, and contrast security practices, policies, and compliance to highlight the tensions in the system.

Cybersecurity is of increasing importance in the medical domain, and the Emergency Department is characterized partly by its nature as a socio-technical system. Security policy is only as effective as the way that people enact it. To create effective security that protects patients, keeps systems online, and delivers prompt care and results, it must be designed with the doctors and nurses that use it in mind.

ACKNOWLEDGEMENTS

We thank reviewers and our shepherd for their suggestions for improving this paper. We would also like to thank the clinical, administrative, and IT staff at the hospitals we visited for sharing their perspectives on security issues affecting Canadian hospitals.

REFERENCES

[1] Ahmed I. Albarrak. 2012. Information Security Behavior among Nurses. *HealthMED* 6, 7 (2012).

[2] Ahmed AlKalbani, Hepu Deng, and Booi Kam. 2015. Investigating the Role of Socio-organizational Factors in the Information Security Compliance in Organizations. In *Australasian Conference on Information Systems*.

[3] Jakob E. Bardram. 2000. Temporal Coordination - On Time and Coordination of Collaborative Activities at a Surgical Department. *Computer Supported Cooperative Work (CSCW)* 9, 2 (May 2000), 157–187. DOI: http://dx.doi.org/10.1023/A:1008748724225

[4] Jakob E. Bardram. 2005. The trouble with login: on usability and computer security in ubiquitous computing. *Personal and Ubiquitous Computing* 9, 6 (Nov. 2005), 357–367. DOI: http://dx.doi.org/10.1007/s00779-005-0347-6

[5] Jakob E. Bardram. 2009. Activity-based computing for medical work in hospitals. *ACM Transactions on Computer-Human Interaction* 16, 2 (June 2009), 1–36. DOI:http://dx.doi.org/10.1145/1534903.1534907

[6] Jim Blythe, Ross Koppel, and Sean W. Smith. 2013. Circumvention of Security: Good Users Do Bad Things. *IEEE Security & Privacy* 11, 5 (Sept. 2013), 80–83. DOI:http://dx.doi.org/10.1109/MSP.2013.110

[7] Google. 2019. Distribution Dashboard. (May 2019). https://developer.android.com/about/dashboards

[8] Government of Canada. 2018. Canada Health Act. (Dec. 2018). https://www.canada.ca/en/health-canada/services/health-care-system/canada-health-care-system-medicare/canada-health-act.html

[9] Rosa Heckle. 2011. Security Dilemma: Healthcare Clinicians at Work. *IEEE Security & Privacy* 9, 6 (Nov. 2011), 14–19. DOI: http://dx.doi.org/10.1109/MSP.2011.74

[10] Karin Hedström, Ella Kolkowska, Fredrik Karlsson, and J.P. Allen. 2011. Value conflicts for information security management. *The Journal of Strategic Information Systems* 20, 4 (Dec. 2011), 373–384. DOI: http://dx.doi.org/10.1016/j.jsis.2011.06.001

[11] Ross Koppel, Sean W Smith, Jim Blythe, and Vijay Kothari. 2015. Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient? *Studies in Health Technology and Informatics* (2015), 215–220. DOI: http://dx.doi.org/10.3233/978-1-61499-488-6-215

[12] Ross Koppel, T. Wetterneck, J. L. Telles, and B.-T. Karsh. 2008. Workarounds to Barcode Medication Administration Systems: Their Occurrences, Causes, and Threats to Patient Safety. *Journal of the American Medical Informatics Association* 15, 4 (July 2008), 408–423. DOI:http://dx.doi.org/10.1197/jamia.M2616

[13] Diana S. Kusunoki and Aleksandra Sarcevic. 2015. Designing for Temporal Awareness: The Role of Temporality in Time-Critical Medical Teamwork. In *ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW)*. 1465–1476. DOI: http://dx.doi.org/10.1145/2675133.2675279

[14] C.P. Nemeth, R.I. Cook, M. O'Connor, and P.A. Klock. 2004. Using Cognitive Artifacts to Understand Distributed Cognition. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 34, 6 (Nov. 2004), 726–735. DOI: http://dx.doi.org/10.1109/TSMCA.2004.836798

[15] Yukari Niimi and Katsumasa Ota. 2014. Privacy Recognition by Nurses and Necessity of Their Information Security Education. In *International Conference on Education Reform and Modern Management*. Atlantis Press. DOI: http://dx.doi.org/10.2991/ermm-14.2014.97

[16] Priyadarshini R. Pennathur, Ann M. Bisantz, Rollin J. Fairbanks, Shawna J. Perry, Frank Zwemer, and Robert L. Wears. 2007. Assessing the Impact of Computerization on Work Practice: Information Technology in Emergency Departments. In *Proceedings of the Human Factors and Ergonomics Society 51st Annual Meeting (4)*, Vol. 51. 377–381. DOI: http://dx.doi.org/10.1177/154193120705100448

[17] Kopo M. Ramokapane, Awais Rashid, and Jose M. Such. 2017. "I feel stupid I can't delete": A Study of Users' Cloud Deletion Practices and Coping Strategies. In *USENIX SOUPS*.

[18] J. Reardon, D. Basin, and S. Capkun. 2013. SoK: Secure Data Deletion. In *IEEE Symposium on Security and Privacy*. DOI:http://dx.doi.org/10.1109/SP.2013.28

[19] Beth Ann Savage. 2017. *A Qualitative Exploration of the Security Practices of Registered Nurses*. Ph.D. Thesis. Walden University.

[20] William Smart. 2018. *Lessons learned review of the WannaCry Ransomware Cyber Attack*. Technical Report. 42 pages. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

[21] Sean W Smith and Ross Koppel. 2014. Healthcare information technology's relativity problems: a typology of how patients' physical reality, clinicians' mental models, and healthcare information technology differ. *Journal of the American Medical Informatics Association* 21, 1 (Jan. 2014), 117–131. DOI: http://dx.doi.org/10.1136/amiajnl-2012-001419

[22] Statistics Canada. 2017. Canadian Survey of Cyber Security and Cybercrime (CSoCC). (Nov. 2017). http://www23.statcan.gc.ca/imdb/p2SV.pl?Function=getSurvey&Id=359489

[23] Alma Whitten and JD Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security*.

APPENDIX

SURVEY

Canadian Emergency Department IT Security and Preparedness Survey

Passwords

1. How many hospital passwords do you have? (1, 2, 3, 4, 5 to 9, 10 to 14, 15 or more)
2. How often are you required to change your hospital passwords? (Never, Every month, Every three months (quarterly), Every year (annually), Less than every year, Unsure, Varies by system)
3. At work, are you allowed to use the same password for different accounts? (Yes, No)
4. Are you forced to choose a unique password for every system, or does the system allow you to reuse passwords on multiple accounts? (Yes, No)
5. How many system-assigned passwords for hospital systems do you have? (0, 1, 2, 3, 4, 5 or more)
6. Which of the following tasks require you to log into a hospital computer network (including PACS) using a hospital terminal (as opposed to using a personal device)? (Review laboratory data, Review radiology data, Access medical records, Document care provided, Enter patient orders, Manage patient flow, Communicate with other caregivers, No tasks require logging in to a hospital terminal, Other)
7. How many different accounts (i.e. username/password combinations for systems such as patient tracking, radiology, lab etc.) do you need in a routine working day? (1, 2, 3, 4, 5, 6 or more)
8. Once you have logged in to a hospital system (e.g. EMR, PACS, etc.), do you need to log in again to the same system during your shift? (A single login lasts all shift, I have to log in to some systems multiple times, I have to log in to all systems multiple times)
9. Do you ever access hospital systems under someone else's login? (Yes, No)
10. Other than passwords, are there any additional authentication methods in use in your emergency department? (Magnetic stripe card (swipe card), USB token, One-time password generation token RFID card (tap card), Smartphone (text message or application-based two-factor authentication), Unsure, No other types of authentication are used, Other)

Internet Connectivity

1. Can the computers in your emergency department access the Internet? (Yes, No, Uncertain)
2. Are there any identified computers in your department that are "air-gapped" (isolated from the Internet and/or the hospital network) to protect them from system crashes or external attack? (Yes, No, Unsure)
3. Do any of the following devices in your department connect to the hospital network or to the Internet? (IV pumps, Monitors, Point-of-care testing devices (e.g. glucometer, urinalysis, etc.), Ultrasound, Unsure, Other)
4. For devices that provide point-of-care testing, is there a protocol to make sure that results are integrated into the electronic medical record? (Yes, No, Unsure, N/A)

Devices

1. Do you use a personal device (i.e. a device not provided by the hospital) to assist you in providing care? (Yes, No) If yes:
2. Has the hospital IT department:
   - Reviewed/authorized your device? (Yes, Uncertain, No)
   - Provided/installed software on the device? (Yes, Uncertain, No)
   - Reviewed/tracked your device usage?(Yes, Uncertain, No)
3. What tasks do you use this device for?
   - Communicating with colleagues via text message
   - Communicating with colleagues via voice call
   - Collecting patient information
   - Sending patient information
   - Searching for data required for patient care Using medical apps (e.g. ePocrates, PEPID, etc.)
   - Teaching
   - Research
   - Other
4. privacy: How do you protect patient privacy when using the device?
   - By turning on "private browsing mode" in the browser (sometimes called "incognito mode")
   - By connecting to the hospital VPN
   - By deleting text messages or emails
   - By deleting images
   - By avoiding sending identifying information
   - By using out-of-band communication channels to separate personal identifiers from medical data
   - Other
5. Does your device connect to the hospital wifi (wireless internet)? (Yes, No, Unsure)
6. Does your device connect to the hospital network, allowing you to access patient information? (Yes, No, Unsure)

Training and Preparedness

1. In which topics have you received formal training from your institution or hospital? (Use of hospital software packages, Protecting patient data, Cybersecurity (malware, virus avoidance, creating good passwords, etc.), I have not received any formal computer training related to my work environment, Other)
2. In the event of an IT failure, does your workplace have a plan for:
   - Order entry (Yes No Not applicable Unsure)
   - Patient triage (Yes No Not applicable Unsure)
   - Patient registration (Yes No Not applicable Unsure)
   - Retrieval of laboratory results (Yes No Not applicable Unsure)
   - Retrieval of imaging (Yes No Not applicable Unsure)
   - Documentation (Yes No Not applicable Unsure)
   - Dispensing medication (Yes No Not applicable Unsure)
   - Replacing other infrastructure and services that are dependent on the computer system (Yes No Not applicable Unsure)
3. In the event of an IT failure, how long do you think it would take your hospital to return to full functionality? (One hour or less, Between one and six hours, Between six and 24 hours, More than 24 hours, Unsure)
4. Does your workplace have processes in place to detect corrupt data? (Yes, No, Uncertain)

Demographics

1. How many years have you been in practice? (Less than 10 years, 10 to 19 years, 20 to 29 years, 30 or more years)
2. In what type of facility do you practice? (Urban teaching, Community teaching, Community non-teaching, Walk-in clinic, Other)
3. I am a: (MD, RN/RPN, Other)