Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities

Dari Alhuwail[1,2] Eiman Al-Jafar[3] Yousef Abdulsalam[4] Shaikha AlDuaij[1]

[1] Information Science, College of Life Sciences, Kuwait University, Kuwait City, Kuwait
[2] Health Informatics Unit, Dasman Diabetes Institute, Kuwait City, Kuwait
[3] Health Informatics and Information Management, Faculty of Allied Health Sciences, Kuwait University, Kuwait City, Kuwait
[4] Quantitative Methods and Information Systems, College of Business Administration, Kuwait University, Kuwait City, Kuwait

Address for correspondence Dari Alhuwail, PhD, Department of Information Science, College of Life Sciences, Kuwait University, Kuwait City, Kuwait (e-mail: dari.alhuwail@ku.edu.kw).

Appl Clin Inform 2021;12:924–932.

Abstract

Objectives This study investigated information security behaviors of professionals working in the public health sector to guide policymakers toward focusing their investments in infrastructure and training on the most vulnerable segments. We sought to answer the following questions: (1) Are certain professional demographics more vulnerable to cybersecurity threats? (2) Do professionals in different institution types (i.e., hospitals vs. primary care clinics) exhibit different cybersecurity behaviors? (3) Can Internet usage behaviors by professionals be indicative of their cybersecurity awareness and the risk they introduce?

Methods A cross-sectional, anonymous, paper-based survey was distributed among professionals working in public health care organizations in Kuwait. Data were collected about each professional's role, experience, work environment, cybersecurity practices, and understanding to calculate a cybersecurity score which indicates their level of compliance to good cybersecurity practices. We also asked about respondents' internet usage and used K-means cluster analysis to segment respondents into three groups based on their internet activities at work. Ordinary least squares regression assessed the association between the collected independent variables in question on the overall cybersecurity behavior.

Results A total of 453/700 (64%) were responded to the survey. The results indicated that professionals with more work experience demonstrated higher compliance with good cybersecurity practices. Interestingly, nurses demonstrate higher cybersecurity aptitude relative to physicians. Professionals that were less inclined to use the internet for personal use during their work demonstrated higher cybersecurity aptitude.

Conclusion Our findings provide some guidance regarding how to target health care professional training to mitigate cybersecurity risks. There is a need for ensuring that physicians receive adequate cybersecurity training, despite the opportunity costs and other issues competing for their attention. Additionally, classifying professionals based on their internet browsing patterns may identify individuals vulnerable to cybersecurity incidents better than more discrete indicators such as age or gender.

Keywords

- health information technology
- informatics
- health information
- privacy
- security

received
May 1, 2021
accepted
July 29, 2021

DOI https://doi.org/10.1055/s-0041-1735527.
ISSN 1869-0327.

Background and Significance

When cybersecurity is mentioned, Hollywood has conditioned the layman to imagine laser-protected server rooms, flashy hardware, exposed wires, encryptions, and a hip protagonist furiously bashing their laptop's keyboard to generate a smooth flow of green-on-black programming syntax. The reality is that there are many elements to sound cybersecurity far more vulnerable and susceptible to breaches than the digital and technological elements. For example, the physical security of portable information technology assets (such as a flash drive) is just as critical in Health IT certification guidelines and one of the largest categories of breaches.[1] Another often overlooked element is the cybersecurity risk related to user behavior. Recent studies demonstrate that the majority of information security incidents are the result of a lack of knowledge or understanding among an organization's staff about the relevant policies and appropriate security procedures.[2] Phishing attacks and similar scams target vulnerable users rather than IT systems, and they are rising across all sectors.[3]

The health sector, in particular, has lagged behind all other sectors in terms of cybersecurity.[4] Health information technology (HIT) has become a fundamental infrastructural component in many health care institutions.[5,6] Recent evidence illustrates that health care organizations, especially hospitals, are constantly challenged with cybercrime, which causes breaches of protected health information.[7] While the direct and indirect cost of a breach varies today, the average cost per breached health care record exceeds 400 USD per record.[8] Many breaches are related to health care professionals' behaviors and negligence.[9]

Literature Review and Hypotheses

Cybersecurity is defined as safeguarding networks, devices, and confidential data from unauthorized access/attacks.[3] The United States Food and Drug Administration provided a more specific definition for cybersecurity by including the prevention of any unauthorized modification, misuse, or/and denial of use of confidential information that has been transferred from one device to another external one.[10,11] Cybersecurity threats can be external or internal, and some of the cyberattacks are caused by human mistakes. Often, these human mistakes happen due to failure to adhere to an organization's policies, rules, regulations, and procedures related to information security.[10,12,13] Fernández-Alemán et al specified that human mistakes form 42% of breaches.[9]

A bibliometric analysis of the literature published in 2019 suggested that in this domain, "nontechnological variables (human-based and organizational aspects, strategy, and management) may be understudied."[14] To minimize internal cybersecurity attacks, several studies recommended promoting a security culture by implementing strict cybersecurity measures, setting clear policies and procedures, and create comprehensive employees' awareness cybersecurity programs.[3,13,15,16] Awareness programs promote the education of staff personnel about cybersecurity measures and provide training on how to secure information access, manipulation, and transfer of data across different health care systems. The Health Insurance Probability and Accountability Act requires health care personnel to be regularly educated and provided with the needed training regarding patient information security measures.[17]

Similar Studies

Kessler et al conducted a survey about the organizational information security climate in which attitudes and behaviors of staff personnel were investigated;[13] their results indicate that having a safe climate does affect employees' behavior positively causing a reduction in the number of data breaches. The authors concluded that training employees plays important role in improving the cybersecurity. In the same study, the results revealed that older employees were more careful when dealing with sensitive and confidential information than younger employees.[13]

Argaw et al explored what health care facilities need to implement effective security awareness programs[12]; they concluded that health care facilities need to recognize their employees' actions and assess their security knowledge and behavior. Fernández-Alemán et al conducted study aimed at evaluating the security behavior of health care professionals in a public hospital setting.[9] The study used a survey to explore the staffs' cybersecurity behaviors. The authors emphasized the significance of introducing cybersecurity measures in orientation and training events for new employees to develop their self-awareness in cybersecurity topics such as handling personal health information, using e-mail systems security, and surfing the internet safely. The survey used in Fernández-Alemán et al study was adopted with minor modification after obtaining permission from the corresponding author.

Objectives

In this study, multiple behavioral issues related to cybersecurity that we consider (as included in the survey) seek to answer the following research questions: (1) Are certain professional demographics more vulnerable to cybersecurity threats? (2) Do professionals in different institution types (i.e., hospitals vs. primary care clinics) exhibit different cybersecurity behaviors? (3) Can patterns of internet usage behavior of professionals be indicative of their cybersecurity awareness?

Given the lack of studies investigating cybersecurity practices in Kuwait and prior studies in other contexts, the following hypothesis were generated:

1. The cybersecurity awareness and practices of health staff is positively associated with more years of work experience. We propose that there is a positive association between higher years of experience and safe security measures practices. Employees with more years of experience were less likely to get involved high-risk behaviors.[13] Additionally, several studies investigated the

cybersecurity behaviors of employees in a hospital setting.[9,12,13]

2. The cybersecurity awareness and practices of health staff working at hospitals is higher than staff working at polyclinics. We hypothesize that staff working in hospitals demonstrate a higher rate of cybersecurity awareness than those working in smaller health care facilities (i.e., polyclinics). We propose that this could be attributed to the complexity and number of connected health IT solutions as well as the resources available in the health care facility.
3. Health staff who access a wider variety of websites on the internet exhibit better cybersecurity awareness and better practices. Studies found that computer skills and a person's perceived technical savviness can predict the person's security behavior.[18] In this study, we hypothesize that health care professionals who access a wider range of websites are more technical savvy and hence demonstrate better cybersecurity awareness.

Methods

Study Design

This study employs a cross-sectional design[19] through an anonymous paper-based survey targeting professionals working in public health care organizations in Kuwait. The study was conducted in full accordance with the World Medical Association Declaration of Helsinki and commenced after obtaining the necessary ethical approvals from the Medical Research Committee at the Ministry of Health, Kuwait.

The survey instrument used in this research was adopted from a prior survey instrument with the authors' approval.[9] The use of the prior survey instrument was influenced by the fact that the authors wanted to understand and explore the cybersecurity practices in an arguable different population. Therefore, modifications to the instrument were necessary to fit the research questions, context, and ethical research requirements. For example, we did not ask questions about if a user's password included a personal name or a special date as required by the Medical Research Committee. The instrument is paper based, in the English language, and self-administered voluntarily by the participants. The survey consisted of 7 demographic questions and 19 security behavior questions. Demographic information collected included gender, age, years of work experience, job title, clinical specialty, education, and current place of employment.

The security questions were further broken down into the following subsections:

(i) Knowledge about organizational security policies
(ii) Secure use of internet and intranet
(iii) Protecting patient health information
(iv) Reporting information security incidents

The questions were piloted with 15 health care professionals and necessary changes were made to ensure clarity. Feedback from the pilot survey informed the design and structure of the final survey instrument.

Study Context

The study's sample is gathered in Kuwait, a country with a high per-capita GDP that offers universal health care to its citizens and residents. The public health system serves the population through three levels: primary care (polyclinics), secondary care (general hospitals), and tertiary care (specialized hospitals).[20] With its focus on providing high-quality and efficient patient care, the MoH has been implementing electronic health information systems across all levels of care.[20]

However, the appropriate cybersecurity infrastructure, professionals' awareness of cybersecurity risks, protocols, and policies continue to lag. Thus, we believe this is a fitting context to examine our research questions given the structure of health care and the escalating need for cybersecurity, seeing that Kuwait ranked in the top 10 countries worldwide in email malware and spam.[21]

Data Collection

The survey was distributed to health care professionals working in the public health care system. To ensure that our sample was inclusive, we targeted all major public hospitals in the country as well as over 20 polyclinics who provided permission to survey their staff. We identified contact persons in each of these institutes and tasked them with distributing the surveys. In total, 42 health care institutions were represented.

Variables of Interest and Data Analysis

The data were analyzed by using R software (version 3.5). First, descriptive statistics describe the demographics of the sample. Second, based on a series of questions regarding internet use in the workplace, we applied a K-means cluster analysis to classify individuals based on their internet usage behavior. To test our hypotheses, ordinary least squares regression assessed the association between the independent variables in question on the overall cybersecurity behavior. The construction of a composite cybersecurity behavior score, which serves as the dependent variable, is described in the following paragraph.

The first step in the analysis was to establish a composite cybersecurity score based on the security questions. Our method follows Fernández-Alemán et al[9] with modifications to resolve some limitations in that work and account for our modified version of the survey instrument. The items are presented in ►Table 1. For each of the 16 items related to cybersecurity practices, one point was given if the respondent indicated positive behavior. Questions with a negative connotation (i.e., "Have you ever shared your password with someone?") were reverse coded. Then, the sum of the points was divided by the number of questions that the respondent answered. This normalization was done so as not to penalize respondents for missing or "N/A" responses. Responses with more than four missing responses or "N/A" were dropped. Ten responses were dropped as a result. Finally, the cybersecurity score was rescaled to be between 0 and 10. The distribution and univariate statistics of the cybersecurity score are reported in the following section.

Table 1 Respondent classification based on browsing behavior

	Group 0	Group 1	Group 2
Cluster size (*n*)	142	137	174
Average age (and standard deviation)	39 (9.7)	37.6 (10.2)	33.6 (7.9)
At work, which of the following websites do you visit?(% of respondents who selected the category)			
Social networks (e.g., Twitter, Facebook)	0	53	97
Videos (e.g., YouTube)	0	18	88
Online music	0	20	39
Cloud storage (e.g., Dropbox)	0	20	63
Online newspapers and magazines	0	10	60
Personal e-mail accounts (e.g., Gmail)	0	42	95
Games	0	2	40
Instant messaging services	0	16	62
Work/clinical related websites	29	36	90

The independent variables included one continuous variable, years of clinical experience, and several other binary variables: gender (1 = male, 0 = female), medical education location (1 = received locally, 0 = received internationally), institution type (1 = hospital, 0 = polyclinic or other), and employment category. Three employment categories were considered: physicians, nurses, and support staff (nutritionists, pharmacists, technicians, etc.). The physician's category was the baseline case; therefore, only the dummy variables for nurses and support staff are included in the model. Using physicians as the baseline case is arbitrary and having another group, as the baseline would produce the same results except that the coefficient will be relative to the baseline group. We chose to test these variables because they are common demographic characteristics that are generalizable to any health care context around the world and used in many previous studies.[9] Furthermore, they can be quickly and accurately self-reported.

To test Hypothesis 3, we classified respondents based on their internet browsing behavior. Internet browsing behavior was assessed based on the types of sites the users visited. In the survey, we asked respondents to indicate the types of websites they visit during working hours (►**Table 1**). Because many different combinations of websites were possible, we opted to cluster respondents into a few distinct groups or archetypes. Using a K-means cluster analysis (via the K-means function in R), we then grouped respondents based on usage patterns to arrive at a three-cluster classification scheme for the respondents.

Results

Response Rate and Descriptive Statistics

A total of 700 questionnaires were distributed randomly at public health care institutes. The survey was returned by 453 individuals for a response rate of 64.4%. ►**Table 2** provides descriptive statistics about the respondents' demographics. Most participants were physicians (64.5%) followed by nurses (30.8%) and other support staff (4.6%). The overall sample of exhibited more female respondents. This was largely driven by the nursing demographic A greater portion of the sample were females, largely driven by the nursing demographic and the administrative staff, which have a largely proportion of females of in the country.

In total, 57% of the sample worked at polyclinics, 34% at hospitals, and 9% worked at specialized health care centers (e.g., burns, dental). The respondents per facility ranged from over 50 (at the major hospitals) to one respondent for small clinics. We did not control for facility-specific characteristics for lack of data and the fact that while workplace culture may differ between facilities, all public institutions share a similar organizational structure, infrastructure, and resources.

Security Behavior Responses and Composite Security Score

The results of the security behavior questions are presented in ►**Supplementary Table S1** (available in the online version). Questions in the security behavior section took on a binary ("yes" or "no") format, with a few cases that added a "N/A" option. The majority of respondents (63%) indicated that they had been informed of their organization's security policies, and (65%) know the policy for handling and discarding confidential patient records. This adherence to policy also seems to be reflected in the low number of respondents indicating that they ever shared, received, or copied patient health information without authorization. Furthermore, 74% of respondents ensured that patient health information is protected from unauthorized individuals.

The 16 questions (►**Supplementary Table S1** [available in the online version]) were added together, after reverse coding certain items, to come to a composite security score. The cybersecurity score across 443 respondents appeared normally distributed with a mean of 7.02, median of 7.33, and a standard deviation of 1.68.

Table 2 Respondent demographics ($n = 453$)

Demographic	*n*	%
Gender		
Male	138	30.6
Female	313	69.4
Age		
18–25	12	2.7
26–30	133	29.5
31–35	98	21.7
36–40	81	18.0
41–45	50	11.1
46–50	28	6.2
51+	13	2.9
Role		
Physicians	289	64.5
Nurses	138	30.8
Support staff (nutritionist, pharmacist, admin, etc.)	21	4.6
Place of work		
Polyclinics	254	57
Hospitals	150	34
Specialized centers (e.g., burns, dental)	42	9

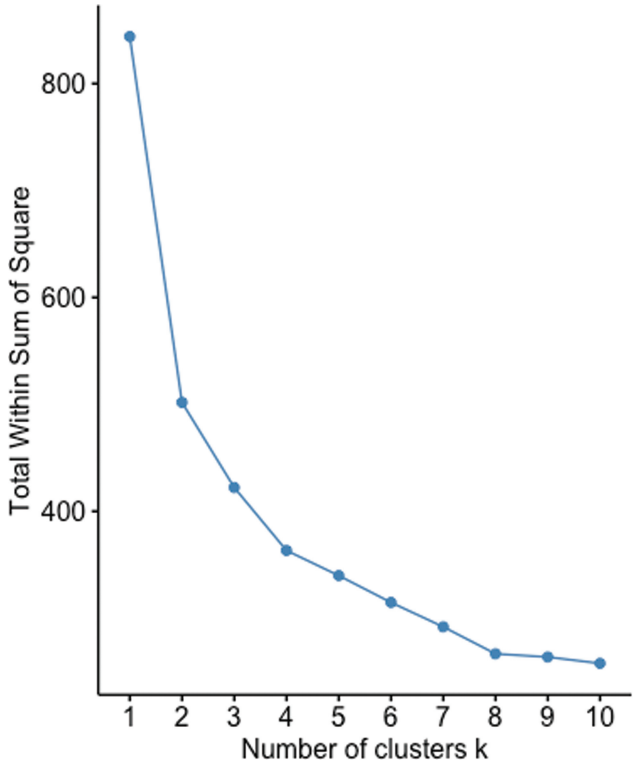

Fig. 1 This scree plot graphs the sum of squares (y-axis) if we were to force the observations into a different number of clusters (x-axis). Sum of squares always decrease with more clusters but at a diminishing rate. Thus, the optimal number of clusters to use is qualitatively determined at the point the incremental reduction in sum of squares from an additional cluster is significantly diminished relative to the previous cluster's benefit. This is referred to as the "elbow method" heuristic.

Results from Classifying Internet Browsing Behavior

We opted to classify respondents' internet browsing behavior by applying a clustering methodology to arrive at logical groupings for the sample. This was achieved by using R's K-means function along with the cluster package (►Table 1).

A distinct group that only browsed work-related websites and portals was first identified (whom we labeled as Group 0 with $n = 142$). The remaining respondents fit a two-cluster model. Two clusters appeared to be the most appropriate number of clusters to apply based on the elbow method heuristic, which considers the reduction within group sum of squares from incrementally increasing the number of clusters and presented in a scree plot (►Fig. 1). This cluster analysis methodology is common among the social sciences such as sociology, management, and psychology.[22]

The cluster analysis implemented via R's cluster package (►Fig. 2). One cluster captured casual internet users who accessed one or two types of websites, mostly for personal messaging and social media during work (Group 1, $n = 137$). The final cluster represented heavy users who not only browsed five to seven different types of websites, including work-related, social media, music or video streaming, shopping, etc. (Group 2, $n = 174$). ►Fig. 1 portrays the between-group distinctions and within-group conformance between clusters 1 and 2 based on the two principal axis factors that explain that account for the highest variance in the data. Two binary dummy variables representing the latter two clusters

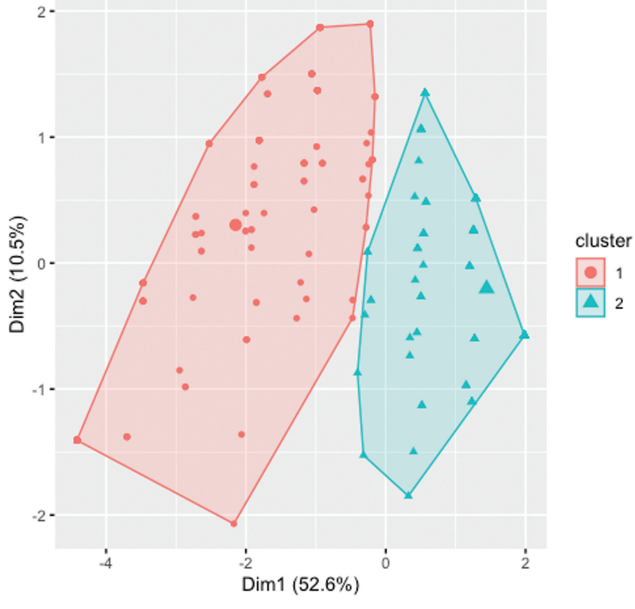

Fig. 2 Visual representation of the two clusters of Internet users. The x and y axes are the principal axis factors that are statistically derived from having the highest explained variance from nine items.

Table 3 Means, standard deviations, and correlations

Variable	M	SD	1	2	3	4	5	6	7
Security score	7.02	1.68							
Experience	11.78	9.00	0.28[b]						
Gender	0.33	0.47	−0.26[b]	−0.11[a]					
Education	0.30	0.46	−0.26[b]	−0.28[b]	−0.15[b]				
Institution type	0.53	0.50	0.02	−0.07	−0.12[a]	−0.06			
Role: physician	0.66	0.47	−0.40[b]	−0.19[b]	0.27[b]	0.25[b]	−0.18[b]		
Role: nurse	0.29	0.45	0.39[b]	0.26[b]	−0.31[b]	−0.32[b]	0.23[b]	−0.88[b]	
Role: support	0.05	0.23	0.04	−0.11[a]	0.05	0.12[a]	−0.07	−0.33[b]	−0.15[b]

Note: M and SD are used to represent mean and standard deviation, respectively. The numbers in the columns correspond to the numbers in the rows.
[a]$p < 0.05$.
[b]$p < 0.01$.

Table 4 Regression results using security score as the criterion

Predictor	Coefficient	Standard error	T-Statistics	*p*-Value
(Intercept)	6.86	0.18	38.23	<0.001[b]
Years of experience	0.02	0.01	2.86	0.004[b]
Gender (male)	−0.38	0.14	−2.743	0.006[b]
Education (local)	−0.38	0.14	−2.628	0.009[b]
Work setting (hospital)	−0.13	0.12	−1.08	0.281
Job role				
Physicians				
Nurse	0.71	0.14	−2.63	<0.001[b]
Support staff	0.61	0.27	2.30	0.022[a]
Internet use at work				
Strictly work-related				
Some social media	−0.21	0.14	−1.40	0.161
Entertainment	−1.36	0.15	−8.87	<0.001[b]

Note: $R^2 = 0.419$[b]. Residual standard error: 1.174 on 428 degrees of freedom.
[a]$p < 0.05$.
[b]$p < 0.01$.

are added to the regression analysis to test Hypothesis 3, with Cluster 0 serving as the reference.

Results from the Regression Analysis

The means, standard deviations, and correlations of the independent variables are presented in ►Table 3. The regression results are presented in ►Table 4. Respondents with more professional experience demonstrated more compliant security behavior ($p < 0.01$), consistent with Hypothesis 1. The data did not show support for Hypothesis 2 ($p > 0.10$). Holding all else constant, females demonstrated a higher security score than males by 0.76 on average.

Concerning the association between internet usage and cybersecurity awareness, the results indicated that Groups 0 and 1 (the groups that did not use the internet at work and the group that only used it for social media and personal messaging, respectively) showed no significant difference in cybersecurity awareness. However, Group 2, which used the internet to browse a variety of websites, scored significantly lower on the cybersecurity score ($p < 0.01$). Therefore, we did not find support for Hypothesis 3.

Discussion

The largest cybersecurity breaches in the health care sector (portable devices, insider access, and physical breaches) do not require more advanced technologies to mitigate their risks, but rather instilling "best practices" onto the stakeholders. This study set out to further explore the stakeholders that pose the biggest risks to cybersecurity in the health sector to provide policymakers and CIOs guidance about where to focus their attention when it comes to training and incentive alignment. Thus, our study assessed the cybersecurity awareness of health

care professionals to identify the areas of vulnerability in professionals' practices and identify factors that correlate with cybersecurity awareness.

Principal Findings

The findings in this research context are consistent with previous studies indicating that the majority of information security incidents are the result of professionals' limited knowledge of their institution's policies and best practices security procedures.[2,23]

We hypothesized that professionals with more years of work experience demonstrated higher cybersecurity awareness, with the intuition that they had more time to absorb cybersecurity training and best practices. Indeed, professionals with more experience demonstrated higher compliance with good security behaviors than those less senior. Hence, we find evidence to support Hypothesis 1. Interestingly, this did not translate to job title seniority. Physicians, who are generally considered to be of higher seniority in terms of job role, demonstrated the lowest cybersecurity scores compared with nurses and administrators. This may be explained by the fact their physicians have a higher "cognitive load," with much of their attention dedicated to clinical development and training. We acknowledge that cybersecurity training and best practices can get crowded out by the many clinical, administrative, other institutional guidelines that health care professionals need to adhere to. However, health care organizations must prepare their workforce through training and awareness programs; implementing the best security protocols alone will not make health care organizations immune to cyberattacks.[23]

Cybersecurity awareness is no better among the staff of hospitals relative to primary care clinics, showing a lack of supporting Hypothesis 2. Perhaps the higher criticality and abundance of sensitive information in hospital systems motivates higher investment to offset this. Recent reports suggest that "larger organizations and hospitals tend to be much more formal. They have deeper IT resources, and they have dedicated and devoted a lot of time and energy and money into developing their cybersecurity threat detection, remediation, and policies and procedures."[24]

One study suggested that the cybersecurity vulnerabilities varied by the size and type of the health care facility.[25] The complexity brought by connecting several health IT solutions in a healthcare facility (e.g., EHRs, mHealth tools, networked medical devices, etc.)[26] brings more risks of internal and external threats and exploitations of sensitive data.[15,27] Future studies should further investigate the characteristics (e.g., size, type, services provided, etc.) of the health care facility and their relationships with cybersecurity vulnerabilities.

In Hypothesis 3, we considered how cybersecurity behavior correlates, not only with some demographic indicators but rather by other technology use behaviors. Indeed, three distinct clusters of respondents emerged from the analysis. The results of the regression analysis indicated that the heaviest internet users were also the ones least aware of cybersecurity policies and practices. We had expected more affluent internet users to have more cybersecurity awareness, but in the words of Murray Davis (1979) we find that "what seems to be a good phenomenon is, in reality, a bad phenomenon."[28] This group that seeks social media and entertainment through internet outlets is not so diligent about stewardship of hospital information and technology assets. Perhaps this could be attributed to the fact that "people who feel well informed about online safety feel less vulnerable to cybercrime and are less inclined to take security measures."[29] Certainly, many cases can be made about the value that instant messaging, social media, and other internet media can bring to the clinical environment.[30–33] We consider this an interesting area for future research: balancing the benefits of instant messaging, social media, and internet use with the costs to productivity and cybersecurity risks.

Recommendations

Stronger cybersecurity programs at health care facilities can raise awareness and make information security training available to professionals, both clinical and nonclinical.[34–36] To improve end-user adoption and buy-in of cybersecurity programs and technologies, it is important utilize a targeted bottom-up approach via personalized outreach, in-person contacts, and frequent announcements throughout the workflow (i.e., rounds).[37] As more patients go online, cybersecurity programs become especially important as clinicians consider discussing and potentially showcasing relevant and useful online resources (e.g., videos, social media channels, websites, etc.).[38,39] Cybersecurity training competes against clinical training, which is naturally perceived as having more immediate benefits and directly related to the clinician's job roles. As such, programs must be concise and effective while highlighting the relevance and the urgency of the matter.[40]

Health care leaders and managers should also recognize the importance of information security and foster an environment that is conducive to achieving protecting the data of the organization, including patient information.[41] Future work should investigate the alignment of the information security programs at healthcare facilities and the existing national strategies, policies, regulations, and frameworks.[42] This alignment should also include the training of relevant stakeholders at every level, both inside and outside the healthcare system (e.g., insurance companies, law enforcement agencies, etc.).[43]

Limitations and Future Research

This research draws on a cross-sectional sample from a diverse pool of participants working at public health care organizations. The findings only provide information about professionals' self-reported attitudes and behavior regarding information security. Since our entire sample was from Kuwait, we were unable to tease out any cultural or context-specific deviance in attitudes and awareness of cybersecurity, though this may an avenue for future research.

While trying to gather as large a random sample as possible, we are certainly susceptible to sample selection bias, whether due to the facilities that we were able to approach or due to the voluntary nature of responses. We would expect that more remote institutions and less-aware professionals are less likely to participate in the survey. In any case, we had to accept these risks to achieve a decent

sample size, and the descriptive statistics showed representative distributions with regards to gender, age, and health institution represented.

The cluster analysis regarding internet browsing behavior produced some interesting insights. Nonetheless, we recognize that it misses some important aspects related to internet usage, particularly the duration of time spent on each type of website and purpose (i.e., visiting YouTube to educate patients versus for personal entertainment). Another dimension worth exploring is to consider whether breaches happen due to personal devices or work computers since people's behaviors can be vastly different when using personal vs work devices.

Conclusion

The security behaviors of health care professionals are critical to the protection of the organization against these threats. Therefore, it is imperative for professionals working in healthcare facilities to play an active role in protecting patients confidentially, ensuring data privacy, and understand relevant information security policies. The findings of this study can provide some guidance about how to target health care professional training to mitigate cybersecurity risks. There is a need for ensuring that physicians receive adequate cybersecurity training, despite the opportunity costs and other issues competing for their attention. Future studies should examine the available national regulations, standards, and guidelines on health information security and suggest opportunities for improvement. It is also worthwhile to investigate similar healthcare systems around the region. While there may be security threats of using the internet at work, clinicians can benefit from access to readily available evidence-based resources that can aid their care practices.

Clinical Relevance Statement

Health information technology (IT) has become a fundamental infrastructural component in many health care facilities. However, this critical infrastructure is constantly threatened daily by cyber-attacks, affecting millions of patients and their private information. Health care institutions are no longer immune to the growing threats of cyberattacks. The security behaviors of health care professionals are critical to the protection of the organization against these threats. Therefore, active efforts must be made to ensure the preparedness and awareness of professionals.

Multiple Choice Questions

1. Which of the following is true with regards to cybersecurity in a health care setting?
   a. Training and raising awareness of health care professionals is critical.
   b. Health information technology has become an integral infrastructural component in many health care institutions.
   c. Health care data breaches have critical consequences that can be costly.
   d. All of the above.

   Correct Answer: Option d is the correct answer. As health care institutions and hospitals increasingly rely on health information technology solutions (e.g., electronics health record), training, and raising awareness of health care professionals and staff at any health care institution is of utmost importance. The consequences of cybersecurity incidents (e.g., data breaches) can have negative and costly impact on the organization, the patients, and professionals.

2. When developing a cybersecurity program at a hospital, it is important to:
   a. Ensure adequate training and awareness of organization's security policies and procedures.
   b. Encourage the use of personal devices and emails.
   c. Allow unrestricted access to the internet using the organization's network.
   d. The Information Technology Department/Division is solely responsible for the cybersecurity program.

   Correct Answer: Option a is the correct answer. Concise and effective cybersecurity training and awareness of organization's security policies and procedures is an essential as part of any cybersecurity program and should be mandated for all staff. All professionals working in health care facilities, and in every department/division must play an active role in protecting patient confidentially, ensuring data privacy, and understand relevant information security policies.

Protection of Human and Animal Subjects

The study was conducted in full accordance with the World Medical Association Declaration of Helsinki and commenced after obtaining the necessary ethical approvals from the Medical Research Committee at the Ministry of Health, Kuwait.

Funding

None.

Conflict of Interest

None declared.

Acknowledgments

The authors wish to acknowledge José Luis Fernández-Alemán for providing the survey instrument which inspired the survey for this study. The authors also wish to thank Technician Syed Faisal Habib for help with data entry.

References

1 Blanke SJ, McGrady E. When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: a cybersecurity risk assessment checklist. J Healthc Risk Manag 2016;36(01):14–24

2 McIlwraith A. Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness. 1st ed. Routledge; 2016
3 Jalali MS, Bruckes M, Westmattelmann D, Schewe G. Why employees (still) click on phishing links: investigation in hospitals. J Med Internet Res 2020;22(01):e16775
4 Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care 2017;25(01):1–10
5 Buntin MB, Burke MF, Hoaglin MC, Blumenthal D. The benefits of health information technology: a review of the recent literature shows predominantly positive results. Health Aff (Millwood) 2011;30(03):464–471
6 Feldman SS, Buchalter S, Hayes LW. Health information technology in healthcare quality and patient safety: literature review. JMIR Med Inform 2018;6(02):e10264
7 Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res 2018;20(05):e10059
8 Choi SJ, Johnson ME. Understanding the relationship between data breaches and hospital advertising expenditures. Am J Manag Care 2019;25(01):e14–e20
9 Fernández-Alemán JL, Sánchez-Henarejos A, Toval A, Sánchez-García AB, Hernández-Hernández I, Fernandez-Luque L. Analysis of health professional security behaviors in a real clinical setting: an empirical study. Int J Med Inform 2015;84(06):454–467
10 Ondiege B, Clarke M, Mapp G. Exploring a new security framework for remote patient monitoring devices. Computers 2017;6 (01):11
11 Food and Drug Administration (FDA) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Food and Drug Administration (FDA); 2018
12 Argaw ST, Troncoso-Pastoriza JR, Lacey D, et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak 2020;20(01):146
13 Kessler SR, Pindek S, Kleinman G, Andel SA, Spector PE. Information security climate and the assessment of information security risk among healthcare employees. Health Informatics J 2020;26 (01):461–473
14 Jalali MS, Razak S, Gordon W, Perakslis E, Madnick S. Health care and cybersecurity: bibliometric analysis of the literature. J Med Internet Res 2019;21(02):e12644
15 Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 2018; 113:48–52
16 Gordon WJ, Wright A, Glynn RJ, et al. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. J Am Med Inform Assoc 2019;26(06):547–552
17 The Office of the National Coordinator for Health Information Technology. Guide to Privacy and Security of Electronic Health Information. Department of Health and Human Services; 2015
18 Anwar M, He W, Ash I, Yuan X, Li L, Xu L. Gender difference and employees' cybersecurity behaviors. Comput Human Behav 2017; 69:437–443
19 Levin KA. Study design III: cross-sectional studies. Evid Based Dent 2006;7(01):24–25
20 Regional Health Systems Observatory - EMRO. Health Systems Profile: Kuwait. Cairo, Egypt; 2006. Report No.: Report no. 17297e
21 Abu-Taieh E, Alfaries A, Al-Otaibi S, Aldehim G. Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. Int J Cyber Warf Terror IJCWT 2018;8(03):46–59
22 Ketchen DJ, Shook CL. The application of cluster analysis in strategic management research: an analysis and critique. Strateg Manage J 1996;17(06):441–458
23 Bhuyan SS, Kabir UY, Escareno JM, et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. J Med Syst 2020;44(05):98
24 Fred Donovan. For ASCs, size matters when it comes to healthcare cybersecurity. HealthITSecurity. Published August 30, 2018. Accessed July 3, 2021 at: https://healthitsecurity.com/news/for-ascs-size-matters-when-it-comes-to-healthcare-cybersecurity
25 Gabriel MH, Noblin A, Rutherford A, Walden A, Cortelyou-Ward K. Data breach locations, types, and associated characteristics among US hospitals. Am J Manag Care 2018;24(02):78–84
26 Nock O, Starkey J, Angelopoulos CM. Addressing the security gap in IoT: towards an IoT cyber range. Sensors (Basel) 2020;20(18): E5439
27 Willing M, Dresen C, Haverkamp U, Schinzel S. Analyzing medical device connectivity and its effect on cyber security in german hospitals. BMC Med Inform Decis Mak 2020;20(01):246
28 Davis MS. That's interesting: towards a phenomenology of sociology and a sociology of phenomenology. Philos Soc Sci 1971;1 (02):309–344
29 Kimpe LD, Walrave M, Verdegem P, Ponnet K. What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behav Inf Technol 2021;0 (00):1–13
30 Caudle KE, Gammal RS, Whirl-Carrillo M, Hoffman JM, Relling MV, Klein TE. Evidence and resources to implement pharmacogenetic knowledge for precision medicine. Am J Health Syst Pharm 2016; 73(23):1977–1985
31 Ko A, Turner J. Online resources to support clinical practice. Home Healthc Now 2018;36(02):114–122
32 Hagedorn PA, Kirkendall ES, Spooner SA, Mohan V. Inpatient communication networks: leveraging secure text-messaging platforms to gain insight into inpatient communication systems. Appl Clin Inform 2019;10(03):471–478
33 Liu X, Sutton PR, McKenna R, et al. Evaluation of secure messaging applications for a health care system: a case study. Appl Clin Inform 2019;10(01):140–150
34 Arain MA, Tarraf R, Ahmad A. Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. J Multidiscip Healthc 2019; 12:73–81
35 Ayatollahi H, Shagerdi G. Information security risk assessment in hospitals. Open Med Inform J 2017;11:37–43
36 Zarei J, Sadoughi F. Information security risk management for computerized health information systems in hospitals: a case study of Iran. Risk Manag Healthc Policy 2016;9:75–85
37 Tsega S, Kalra A, Sevilla CT, Cho HJ. A bottom-up approach to encouraging sustained user adoption of a secure text messaging application. Appl Clin Inform 2019;10(02):326–330
38 Rozenblum R, Bates DW. Patient-centred healthcare, social media and the internet: the perfect storm? BMJ Qual Saf 2013;22(03): 183–186
39 Tan SS-L, Goonawardene N. Internet health information seeking and the patient-physician relationship: a systematic review. J Med Internet Res 2017;19(01):e9
40 Sher M-L, Talley PC, Cheng T-J, Kuo K-M. How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments. Health Inf Manag 2017;46(02):87–95
41 Humaidi N, Balakrishnan V. Indirect effect of management support on users' compliance behaviour towards information security policies. Health Inf Manag 2018;47(01):17–27
42 Hakmeh J. Cybercrime and the digital economy in the GCC countries. The Royal Institute of International Affairs, Chatham House. Accessed 2017 at: https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf
43 Kshetri N. Cybersecurity in Gulf Cooperation Council Economies. In: The Quest to Cyber Superiority. 1st ed. Springer International Publishing; 2016:183–194

