ISSN: 2345-2897; Health Education and Health Promotion. 2022;10(2):369-375.

The Effect of Cyber Security Knowledge on Employees' Personal Growth: An Empirical Study in Private Hospitals in Libya and Yemen

ARTICLE INFO

Article Type
Descriptive Study

Authors
Ali Alferjanya M.A.O.*[1] *MSc,*
Musaed Al-mwald M.N.[2] *PhD,*
Alias R.B.[3] *PhD*

How to cite this article
Ali Alferjanya M A O, Musaed Al-mwald M N, Alias R B. The Effect of Cyber Security Knowledge on Employees' Personal Growth: An Empirical Study in Private Hospitals in Libya and Yemen. Health Education and Health Promotion. 2022;10(2):369-375.

ABSTRACT

Aims This study aimed to explore the effect of cyber security knowledge (proactive, reactive, and active) on employees' personal growth (growth mindset, metacognition, and self-authorship) in private hospitals in Libya and Yemen.

Instrument & Methods The descriptive analytical approach was used to determine the relationship between the independent CSK and dependent variable PG, the current study took place in March 2021 and was applied to a stratified random sample of 164 managers from the middle and lower management.

Findings The stability values of the main variables indicated that in general, the study instrument has a high stability coefficient and its ability to achieve the study objectives is high. There was a low dispersion in the responses about proactive, reactive, development of talents, growth mindset, metacognition, and self-authorship in private hospitals in Libya and Yemen. Generally, it turns out that the reality of the study sample's point of view was low. The coefficient of determination R2 showed its value of changes in a growth mindset in private hospitals in Libya & Yemen is due to the change in CSK.

Conclusion Results indicated a lack of understanding of cyber threats and recommended mitigations and uncertainty regarding applicable legislation governing electronic patient information; also, the level of CSK & PG in the studied hospitals was low. The findings also show that CSK positively affects employees' PG beyond the demographic differences in respondents.

Keywords Cybersecurity; Knowledge; Engineering; Patient Generated Health Data

[1]College of Graduated Studies, Universti Tenaga National, Putrajaya, Malaysia
[2]College of Computing and Informatics, Universti Tenaga National, Putrajaya, Malaysia
[3]Graduate Business School, Universiti Tenaga National, Putrajaya, Malaysia

Correspondence
Address: College of Graduated Studies, Universti Tenaga National, Putrajaya, 43000 Malaysia
Phone: +60 (174) 252274
Fax: -
pm20929@student.uniten.edu.my

Article History
Received: April 22, 2022
Accepted: June 5, 2022
ePublished: June 15, 2022

CITATION LINKS

[1] Mind framing: a proposed framework for personal ... [2] Symposium on the healthy ... [3] Erik Erikson's stages of psychosocial ... [4] Disagreement about recommendations for measurement ... [5] Solution-focused self-help for improving university ... [6] Coaching as a social ... [7] Primary ... [8] Hospital bring-your-own-device security challenges ... [9] Healthcare data breaches: insights and ... [10] Security engineering of patient-centered ... [11] Data breach notification: issues and challenges for ... [12] The effect of organizational information security ... [13] Organizational information security policies: a review ... [14] Gender difference and employees' cybersecurity ... [15] Talent management in healthcare: a systematic ... [16] Strengthening personal growth: The effects of a ... [17] Cybersecurity of Hospitals ... [18] The effects of strategy of enhanced metacognition ... [19] Towards understanding cybersecurity capability ... [20] Cybersecurity and privacy issues for socially integrated mobile ... [21] Proposing new blockchain challenges ... [22] Transforming healthcare cybersecurity from reactive to proactive ... [23] Healthcare staffs' information security practices ... [24] The technologisation of the social: a political ... [25] Cybersecurity and cyber defense: national ... [26] The role of cybersecurity and policy awareness ... [27] Strategic resource use for learning: a self-administered intervention ... [28] Research methods for business: a skill building ...

Introduction

Personal growth is seen as a change within an individual that is affective, cognitive, or behavioral, and is typically, believed of as positive, making the employee even complete and truly functional [1].

Personal growth tends to be identified as the life-long cycle of enhancing individual's identity and self-awareness, learning skills, and creating human resources to eventually improve individual's success at work and quality of life [2, 3], indicates to the approaches and strategies that promote human growth at the personal level. Maslow's theory highlighted that an individual has five fundamentals needs, which are Physiological, Security needs, Affiliation needs, Esteem needs and on the top Self-actualization needs which involve recognizing ones` full potential or self-development and personal growth [3].

Personal growth has been mentioned in the six variables of psychological well-being defined by the proposed model of Carol Ryff, besides autonomy, environmental mastery, supportive relationships with colleagues, meaning in life, and self-acceptance. She established three major axes of personal growth: power, awareness, and self-development [4]. Nowadays, personal growth has been achieved widely through workshops, social interactions, work coaching, learning programmes, and techniques for time-management [5, 6]. According to the World Health Organization's (WHO) technical series on primary health care, information, and communication technology (ICT) is becoming more prevalent in the healthcare industry. With the introduction of smartphones, tablets, and laptop computers, digital technologies for health have impacted how health services are delivered and operated [7]. Furthermore, with the ongoing COVID-19 pandemic, the adoption rate of such technologies has been expedited. Therefore, cybersecurity is increasingly becoming a prominent concern among healthcare providers adopting digital technologies to improve patient quality of care.

The recent reports on cyberattacks, such as ransomware, and WannaCry, have brought to life the destructive nature of such attacks upon healthcare. In addition to cyberattacks, which have been targeted against the vulnerabilities of information technology infrastructures, a new form of cyberattack aims to exploit human vulnerabilities; such attacks are categorized as "social engineering attacks." Healthcare is particularly attractive to cybercriminals because of its data-rich nature, critical use-cases, and multiple access points [8]. Additionally, healthcare data is more valuable on the dark web [9]. The sector is believed to have the financial muscle to pay for cyber criminals' attacks such as ransomware. Notable cases include the German hospital hacks [10], which resulted in a patient's death, and the unauthorized access to some medical records in Finland [11], in which the hackers' demanded ransoms from each of the patients involved. While the mode of entry was not specified in these incidents, most of these attacks resulted from human elements. To this end, strengthening the healthcare workforce, colloquially referred to as the human firewall, is necessary to complement technical information security solutions. As a result, numerous comprehensive studies have been conducted to recognize the critical role of human factors in cyber security incidents [12-14].

The main objective of this empirical paper was to outline the positive effect of cyber security knowledge (CSK) on employees' personal growth in private hospitals in Libya and Yemen, highlighting the disparity between current healthcare security practices and the required security practices specified in the information security policy. In addition, the healthcare sector's security gaps and risky practices were examined. In order to improve employees' personal growth, develop them in a scientific and thoughtful manner, and prevent competitors from obtaining their expertise and knowledge, the organization is required to pay attention to the CSK which considered to be one of the riskiest threats in today's business world [15]. Therefore, this study aimed to explore if there is an effect of CSK (proactive, reactive, and active) on employees' personal growth (growth mindset, metacognition, and self-authorship) in private hospitals in Libya and Yemen.

Although the education field is mainly concentrated on planning for individual's career as a guide for personal growth (PG), scholars find out PG within workplace is rather a term of workers' capacity and agency to deal with, shape and appropriate their situation. This is why the structure of strengths intervention has recently been investigated as a means to improve feelings of skill, productivity and superiority in workers to encourage PG [16], with an immediate influence on general self-effectiveness and an indirect impact on PG.

Le Cunff [1], indicated that Personal growth is consists of three basic constructs which are: Growth mindset, Metacognition, and Self-Authorship. Growth mindset which can be identified as the belief that basic abilities mostly can be gained through devotion and hardworking, talent and brain are just the starting point. The theory of growth mindset is supported by cognition research that shows that everybody has the capacity to improve their intellect [17]. Metacognition, usually defined as "knowing about knowing" or "thinking about thinking" which means the capacity to recognize and control individual's cognitive process and gain information about how and when to use relevant techniques for problem-solving [18]. Self-authorship refers to the internal coordination and generation of individual's values, internal loyalties, and the self-belief in

individual's abilities to rely on internal values in case to make choices [18].

PG Constructs consist particularly of three stages, a growth mindset considered crucial to the first two stages of PG, Pact and Act. While metacognition mostly useful for the next stages Act and React. Finally, self-authorship though to be very essential for the stages, React and Impact. Figure 1 shows personal growth constructs and stages.

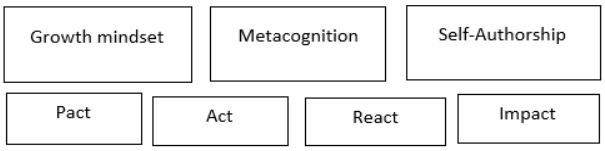

Figure 1) Personal growth constructs and stages [1]

To conclude, PG featured distinguishably in the need's literature since the 40s and 50s of the last century, for example, Maslow's theory hierarchy of needs, Alderfer's theory of existence, relatedness and growth, this stresses that personal growth opportunities are particularly valuable to employers. As a human being, an individual feels a great sense of fullness and wholeness by fulfilling growing needs. The company is expected to take responsibility, provide growth opportunities for employees, and make personal growth a crucial construct to be investigated. The current research enhances that CSK can help the organization to achieve that.

The paradigm shift toward digitalized healthcare necessitates the storage of massive amounts of electronic patient data across multiple operating [19]. Integrating new technologies with out-of-date, legacy, or unsupported operating systems compromises interoperability and exposes organizations to increased cybersecurity risk. Historically, healthcare organizations have prioritized patient care over cybersecurity and have viewed the electronic health record as the holy grail of optimal patient care. Healthcare, however, lags other industries regarding data security and the development of comprehensive cybersecurity training programs for employees [20]. In addition, as the volume and value of patient information increases, health managers must develop cybersecurity capabilities across their organization [21]. Cybersecurity capability development entails updating existing information technology and anticipating and proactively acquiring the need for new technology, cybersecurity talent, and comprehensive organizational training.

Information security practices are proactive measures taken by healthcare staff to adhere to security policies or rules and ensure the information system's confidentiality, integrity, and availability [22]. There are numerous security measures, but the most common are internet use, email use, social media use, password management, incident reporting, information handling, and mobile computing [23]. Within the context of the human aspect of information security practices, these security practices were identified as being more prone to security violations. Compliance with these security measures for healthcare personnel is contingent on various factors, including knowledge, attitude, and behavior, collectively referred to as asked variables. Cybercrime will cost the global economy $10.5 trillion by 2025. While that figure is difficult to comprehend, security threats exist and affect virtually everyone, from large multinational corporations to small businesses and everything in between [24]. In addition, cyber threats have become more sophisticated, because attackers can adapt to new security regulations, businesses must stay one step ahead to protect their operations. They will have an advantage over attackers if they have a comprehensive, well-planned, and unique cybersecurity strategy. The most popular cybersecurity strategies are proactive, active, and reactive.

Proactive strategy-"BEFORE THEY COME, WE WILL BE READY" cyber defence is based on comprehensive cyber security assessments. It uses real-time network monitoring, and cyber threat intelligence feeds to build a detailed picture of the security landscape and how threats manifest and are exploited. The in-depth analysis can help identify and remediate weak spots before exploits are available and identify areas for targeted investment to improve the system's overall security. In addition, encryption and/or dynamic distribution technologies can protect data in transit and at rest [25].

Active strategy-"WHEN THEY COME, WE WILL RESPOND" With enhanced security monitoring of information and assets, an active approach to security builds on the reactive approach. In addition, vulnerability management, advanced firewalls, multi-factor authentication, NAC (network access controls), DLP (data loss prevention), and other technologies are deployed and managed. Also, security information event management (SIEM) systems are deployed to provide real-time monitoring [26].

Reactive strategy-"IF THEY COME, WE WILL RESPOND". The reactive strategy is simple to comprehend. For instance, a data breach could occur. Protective measures are implemented first, followed by restoration efforts. Almost certainly, all businesses that understand the potential for a cyberattack have experimented with various of network security solutions. Businesses almost certainly have antivirus, firewall, and threat monitoring software installed. They have devised a strategy to combat an attack in the unfortunate but possible event. After the threat has passed, the team follows well-documented procedures to determine what went wrong and what preventative measures should be taken to avoid future occurrences [27].

The main objective of this empirical paper was to outline the positive effect of cyber security knowledge on employees' personal growth in private hospitals in Libya and Yemen, highlighting the disparity between current healthcare security practices and the required security practices specified in the information security policy. In addition, the healthcare sector's security gaps and risky practices were examined. In order to improve employees' personal growth, develop them in a scientific and thoughtful manner, and prevent competitors from obtaining their expertise and knowledge, the organization is required to pay attention to cyber security knowledge which is considered to be one of the riskiest threats in today's business world. Therefore, this study aimed to explore the effect of Cyber security knowledge (proactive, reactive, and active) on employees' personal growth (growth mindset, metacognition, and self-authorship) in private hospitals in Libya and Yemen.

Instrument and Methods

The descriptive analytical approach was adopted to study the relationship between all the main and sub-variables, the data of which were derived from the study population. The study population consisted of managers in the middle and lower management in the biggest 5 private hospitals in Libya and the biggest 5 private hospitals in Yemen. This study took place in March 2021. The number of middle managers reached 140, while the number of lower managers reached 357. Thus, the total number of the population in this research is 497 managers. A stratified random sample of 164 managers from the middle and lower management (33% of the population). The researchers calculated it after determining the study population of 497 [28]. Accordingly, the researchers distributed 164 questionnaires to the study sample members through Google form, a total of 147 questionnaires were retrieved, with a percentage of 90%. After examining the retrieved questionnaires, 9 were invalid. Thus, the number of valid questionnaires for analysis became a total of 138, with a percentage of 84% of the distributed questionnaires.

The study tool was adopted from previous studies and modified to suit the current study, PG was measured with the help of the instrument that achieved a high statistical validity (0.962), and high reliability Cronbach's alpha (0.937) [1]. This scale was created originally by Robitschek and developed it in 2014 consisting of three constructs which are (Growth mindset, Metacognition, Self-Authorship) and divided into three items for each construct [1]. CSK was measured using the model [26] which achieved a high level of stability and reliability consisting of three constructs (Proactive, Reactive, Active) and divided into ten items.

Conceptual framework consists of the varied variables used in this study named as, CSK as an independent variable, employees' personal growth as a dependent variable. Based on the literature review, the researcher poses the conceptual framework of this study illustrated in Figure 2.

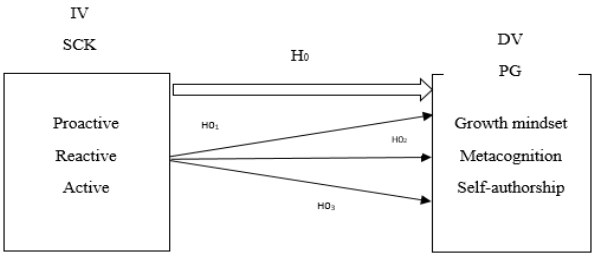

Figure 2) Theoretical framework
Note. Independent Variable: CSK[26]. Dependent Variable: Personal growth[1]

To achieve the objectives of this study, the researchers used frequencies and percentages to describe the study sample's demographic variables; To determine the relative importance of the study variables, mean±SD was used; Finally, to discover the effect of the independent variable on more than one dependent variable, utilized multiple regression analysis.

Findings

Table 1 illustrates the respondents profile in terms of nationality, gender, age, level of education, and work experience.

Table 1) Personal and functional characteristics of the respondents

Variable		Number	Percent
Gender			
Libya	Male	43	31.159
	Female	31	22.463
Yemen	Male	39	28.260
	Female	25	18.115
Age (Year)			
Libya	30 or less	12	8.695
	30-40	24	17.391
	41-50	27	19.565
	More than 50	11	7.971
Yemen	30 or less	14	10.144
	30-40	19	13.768
	41-50	22	15.942
	More than 50	9	6.521
Level of Education			
Libya	High school or Diploma	17	12.318
	Bachelor's	44	31.884
	Master or Doctorate	13	9.420
Yemen	High school or Diploma	12	8.695
	Bachelor's	43	31.159
	Master or Doctorate	9	6.521
Work experience (Year)			
Libya	Less than 5	8	5.797
	5-10	21	15.217
	11-20	31	22.463
	More than 20	14	10.144
Yemen	Less than 5	9	6.521
	5-10	18	13.043
	11-20	23	16.666
	More than 20	14	10.144

To calculate the reliability coefficient, the internal consistency test Cronbach Alpha was used, through the researcher applying his study tool in its final form to the stability sample that Consisted of 11 individuals from outside the study sample. Table 2 presents the stability values of the main variables, which indicated that in general, the study instrument has a high stability coefficient and its ability to achieve the study objectives is high.

There was a low dispersion in the responses about proactive, reactive, development of talents, growth mindset, metacognition, and self-authorship in private hospitals in Libya and Yemen. Generally, it turns out that the reality of the study sample's point of view was low (Table 3).

The statistical analysis results presented a significant effect of CSK on growth mindset, metacognition, and self-authorship in private hospitals in Libya & Yemen. The coefficient of determination R^2 showed its value of changes in a growth mindset in private hospitals in Libya & Yemen is due to the change in CSK.

Table 2) The stability values of the main study variables (Cronbach Alpha)

Variable	Number of Items	α
CSK	10	0.887
Proactive	3	0.764
Reactive	4	0.739
Active	3	0.771
Personal Growth	9	0.853
Growth mindset	3	0.786
Metacognition	3	0.791
Self-authorship	3	0.744

Table 3) Results of mean±SD of questionnaire about private hospitals in Libya & Yemen

Dimensions	Mean±SD	Importance of item
Proactive		
I am familiar with the term Cyber security	2.92±0.770	1
I have attended Information Technology security training	1.28±0.752	3
My current education influences my knowledge of cybersecurity	2.03±0.869	2
Total	2.076±0.524	-
Deviations		
I know which websites are secure by checking the HTTP and HTTPS URLs	1.19±0.834	4
I do not open email links or attachments if I do not know who the sender is	3.34±0.785	1
I have skills and knowledge in using the computer's application software	2.93±0.764	3
I regularly check my operating system update	2.98±0.853	2
Total	2.61±0.497	-
Active		
I am aware of how to behave in the event of a cyber-attack	1.96±0.807	3
I use different passwords across multiple web portals, systems, or applications	2.74±0.915	2
I use my work devices for work-related activities only	3.85±0.835	1
Total	2.85±0.523	-
Growth mindset		
I understand how to make the specific changes that I need in my working life	2.34±0.851	1
I have a strong sense of where I am heading in my working life	1.74±0.918	3
I initiate the transition process once I want to change something in my working life	1.92±0.822	2
Total	2.00±0.546	-
Metacognition		
I can choose what role I want to play in a group	2.14±0.938	2
I realize what I need to get started toward reaching my goals	2.37±0.902	1
I have a clear action plan to support me in reaching my targets	1.45±0.791	3
The overall mean and standard deviation of metacognition	1.99±0.534	-
Self-authorship		
I am taking charge of my working life	3.12±0.715	1
I understand what my unique contribution to the work might be	2.00±0.836	3
I have a method for making my working life more balanced	2.17±0.842	2
The overall mean and standard deviation of Self-Authorship	2.43±0.508	-

Table 9) Multiple regression analysis test results for the effect of CSK on PG in private hospitals in Libya & Yemen

Dependent Variable	Model summary			ANOVA				Coefficients			
	R	R^2	Adjusted R^2	F.	df.		Sig.	β		T.	Sig.
Personal growth	0.761	0.572	0.528	84,385	regression	3	0.0001	Proactive	0.346	4.853	0.0001
					The rest	207		Reactive	0.379	4.631	0.001
					Total	210		Active	0.321	3.414	0.0001
Growth mindset	0.684	0.402	0.322	35.015	regression	3	0.0001	Proactive	0.264	3.771	0.0001
					The rest	207		Reactive	0.223	2.416	0.006
					Total	210		Active	0.190	2.415	0.019
Metacognition	0.767	0. 506	0. 359	47.630	regression	3	0.0001	Proactive	0.224	3.062	0.003
					The rest	207		Reactive	0.197	3.467	0.014
					Total	210		Active	0.354	2.338	0.000
Self-authorship	0.543	0.368	0.331	37.613	regression	3	0.0001	Proactive	0.249	3.463	0.001
					The rest	207		Reactive	0.301	4.644	0.0001
					Total	210		Active	0.033	0.603	0.482

Discussion

Based on the current findings, a set of recommendations can be divided into practical recommendations to the surveyed hospitals management, and a practical ones related to researchers and students in the field of business administration and cyber security, the most important are the following:

1. Establish hands-on study programmes and training workshops that include cyber awareness courses in order to:
   - Increase employees' awareness of cyber security threats.
   - Foster new perspectives on cyber risk and accountability for the preservation of organizational data.
   - Turn knowledge into actions by reducing human elements that result in cyber security flaws.
   - Create new standards to guide optimal cyber practices.
2. Extend existing understanding about cyber security among workers from other regions.
3. Invest in cyber security technologies because a large portion of the population lacks the skills and knowledge required to defend against cyber risks. Nonetheless, it is critical to invest in cyber retraining in order to influence perceptions about cyber threats.
4. The necessity for comparative study arose as a result of cultural differences in cyber security understanding. As a result, training programmes should be designed with an international perspective in mind, focusing on individual behaviour rather than local and regional manifestations.
5. Employees' personal growth should be enhanced by practitioners promoting both cognitive and behavioral components.
6. Cognitive characteristics may be increased by reflecting on personal interests, talents, and values, which may improve employees' goal formulation in an intelligent approach.
7. Employees may be guided in constructing a realistic and time-bound action plan to achieve their personal objectives, which would improve their goal implementation capacities and, as a result, the behavioral aspects of personal growth.
8. Organizations should engage supervisors with training so they likely to encourage employees' personal growth, develop their goal setting, and communicate on employees' daily well-being.
9. A better employee's personal growth make them less reliant on affective swings to participate in everyday professional difficulties, which would positively contribute to beneficial outcomes such as greater person-job fit.

It is vital to note that this research has several limitations that should be considered. The primary restriction of this study is the sort of respondents. Workers in private hospitals in Libya and Yemen comprised the sample size. It is advised that a larger sample size, one that is not deemed a convenient sample and covers many disciplines, be used to increase the study's robustness. Another point of contention is from the variables' measurement. Face validity was employed in the construction of the questionnaire, and we relied on a team of professionals to design our survey instrument. Because this is one of the few research that assesses CSK and personal growth, the questionnaire should be re-evaluated to ensure its reliability and validity.

Future research should focus on developing particular instruments to assess CSK. Although we used a single-item scale to quantify this variable, multi-item scales were proven to be more reliable. Nonetheless, other scholars have proposed that if a single-item inquiry can elicit meaningful information, its simplicity can impart validity and reliability, even at the sacrifice of comprehensive detail. Still, more comprehensive tools for assessing cyber security expertise are required. Furthermore, this sort of study should be carried out in other nations with different values and attitudes, with the findings compared to the current study. Future research should look at how particular training programmes based on our study findings might increase CSK, personal growth, and skill-based behaviour.

Conclusion

Cybercrime poses a severe threat to information security as internet consumption rates continuously increase in organizations. Therefore, CSK has become increasingly urgent for both organizations and employees. Furthermore, the finding of the current study approved that CSK must be a strategic requirement for any organization that seeks to update its employees' skills and knowledge to achieve PG. A higher level of personal growth can lead to self-efficacy and job satisfaction, positively impacting organizational well-being and effectiveness.

Acknowledgments: None declared.
Ethical Permissions: There is no ethical code for this article.
Conflicts of Interests: None declared.
Authors' Contributions: Ali Alferjanya MAO (First Author), Introduction Writer/Methodologist/Main Researcher/Statistical Analyst/Discussion Writer (50%); Musaed Al-mwald MN (Second Author), Introduction Writer/Methodologist/Assistant Researcher (30%); Alias RB (Third Author), Assistant Researcher/Discussion Writer (20%)
Funding/Support: This paper is funded by the authors, under University Tenaga Nasional, Malaysia.

References

1- Le Cunff AL. Mind framing: a proposed framework for personal growth [Internet]. NESS LABS; 2019 [Cited 2022

Mar 3]. Available from: https://nesslabs.com/mindframing
2- Senn MJE, editor. Symposium on the healthy personality. Josiah Macy, Jr. Foundation; 1950.
3- McLeod S. Erik Erikson's stages of psychosocial development. Simply Psychol [Internet]. New York: Simply Psychology; 2018 [Cited 2022 Mar 3]. Available from: https://www.simplypsychology.org/Erik-Erikson.html
4- Ryff CD, Boylan JM, Kirsch JA. Disagreement about recommendations for measurement of well-being. Prev Med. 2020;139:106049.
5- Pakrosnis R, Cepukiene V. Solution-focused self-help for improving university students' wellbeing. Innov Educ Teach Int. 2015;52(4):437-47.
6- Shoukry H, Cox E. Coaching as a social process. Manag Learn. 2018;49(4):413-28.
7- World Health Organization. Primary care. Geneva: World Health Organization; 2022 [Cited 2022 Mar 5]. Available from: https://www.who.int/teams/integrated-health-services/clinical-services-and-systems/primary-care.
8- Wani TA, Mendoza A, Gray K. Hospital bring-your-own-device security challenges and solutions: Systematic review of gray literature. JMIR mHealth uHealth. 2020;8(6):e18175.
9- Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare data breaches: insights and implications. Healthcare. 2020;8(2):133.
10- Yari IA, Dehling T, Kluge F, Geck J, Sunyaev A, Eskofier B. Security engineering of patient-centered health care information systems in peer-to-peer environments: Systematic review. J Med Internet Res. 2021;23(11):e24460.
11- Karyda M, Mitrou L. Data breach notification: Issues and challenges for security management. MCIS. 2016:60.
12- Dong K, Ali RF, Dominic PDD, Ali SEA. The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. Sustainability. 2021;13(5):2800.
13- Cram WA, Proudfoot JG, D'arcy J. Organizational information security policies: A review and research framework. Eur J Inf Syst. 2017;26(6):605-41.
14- Anwar M, He W, Ash I, Yuan X, Li L, Xu LD. Gender difference and employees' cybersecurity behaviors. Comput Hum Behav. 2017;69:437-43.
15- Mitosis KD, Lamnisos D, Talias MA. Talent management in healthcare: A systematic qualitative review. Sustainability. 2021;13(8):4469.
16- van Woerkom M, Meyers MC. Strengthening personal growth: The effects of a strength's intervention on personal growth initiative. J Occup Organiz Psychol. 2019;92(1):98-121.
17- Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, et al. Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. BMC Med Inf Decis Mak. 2020;20(1).
18- Song JY, Park JE. The effects of strategy of enhanced metacognition on the improvement of creative problem solving skills. J Digit Converg. 2017;15(7):1-2.
19- Offner KL, Sitnikova E, Joiner K, MacIntyre CR. Towards understanding cybersecurity capability in Australian healthcare organizations: A systematic review of recent trends, threats and mitigation. Intell Nat Secur. 2020;35(4):556-85.
20- Al-Muhtadi J, Shahzad B, Saleem K, Jameel W, Orgun MA. Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. Health Inform J. 2019;315-29.
21- Alonso SG, Arambarri J, López-Coronado M, de la Torre Díez I. Proposing new blockchain challenges in eHealth. J Med Syst. 2019;43:64.
22- Bhuyan SS, Kabir UY, Escareno JM, Ector K, Palakodeti S, Wyant D, Kumar S, Levy M, Kedia S, Dasgupta D, Dobalian A. Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations. J Med Syst. 2020;44(5):1-9.
23- Yeng PK, Yang B, Snekkenes EA. Healthcare staffs' information security practices towards mitigating data breaches: A literature survey. Stud Health Technol Inform. 2019;261:239-45.
24- O'Connor P. O'Connor P, Benţa MI, editors. The technologisation of the social: A political anthropology of the digital machine. London: Routledge; 2021.
25- Galinec D, Moznik D, Guberina B. Cybersecurity and cyber defense: National level strategic approach. Automatika. 2017;58(3):273-86.
26- Wong LW, Lee VH, Tan GW, Ooi KB, Sohal A. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. Int J Inf Manag. 2022;66:102520.
27- Chen P, Chavez O, Ong DC, Gunderson B. Strategic resource use for learning: A self-administered intervention that guides self-reflection on effective resource use enhances academic performance. Psychol Sci. 2017;28(6):774-85.
28- Sekaran U, Bougie R. Research methods for business: a skill building approach. 7th Edition. Hoboken: Wily; 2016.