Journal of Computer and Communications, 2021, 9, 77-90
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Cybersecurity Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment

Ahmad Reda Alzighaibi

Department of Information Systems, College of Computer Science and Engineering, Taibah University, Yanbu, KSA
Email: azighaibi@taibahu.edu.sa

How to cite this paper: Alzighaibi, A.R. (2021) Cybersecurity Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment. *Journal of Computer and Communications*, **9**, 77-90.
https://doi.org/10.4236/jcc.2021.911006

Received: September 29, 2021
Accepted: November 14, 2021
Published: November 17, 2021

Abstract

The cyberspace has simultaneously presented opportunities and challenges alike for personal data security and privacy, as well as the process of research and learning. Moreover, information such as academic data, research data, personal data, proprietary knowledge, complex equipment designs and blueprints for yet to be patented products has all become extremely susceptible to Cybersecurity attacks. This research will investigate factors that affect that may have an influence on perceived ease of use of Cybersecurity, the influence of perceived ease of use on the attitude towards using Cybersecurity, the influence of attitude towards using Cybersecurity on the actual use of Cybersecurity and the influences of job positions on perceived ease of use of Cybersecurity and on the attitude towards using Cybersecurity and on the actual use of Cybersecurity. A model was constructed to investigate eight hypotheses that are related to the investigation. An online questionnaire was constructed to collect data and results showed that hypotheses 1 to 7 influence were significant. However, hypothesis 8 turned out to be insignificant and no influence was found between job positions and the actual use of Cybersecurity.

Keywords

Cybersecurity Attack, Technology Acceptance Model (TAM) Model, Academic Data, Saudi Arabia

1. Introduction

Cybersecurity has become an integral component of internet-connected systems in as far as the protection of such systems is concerned. Cybersecurity provides a proactive approach towards the mitigation of cyber attacks on academic data and personal information, which result in data breaches and identity theft [1]. In

June 2019, the Australian National University was a victim of cyber-attack, targeted for its payroll and personal information dating back to nineteen years. As such, Cybersecurity is a risk management function in any given organization. Its main objective is to design, develop, and maintain the confidentiality of data, integrity, as well as the availability of data to the right users [2] [3]. More specifically, Cybersecurity includes elements of network security and a reliable incident response plan. Common cyber related threats to academic data and personal information data centers include ransomware, phishing, social engineering, and malware. Consequently, a comprehensive Cybersecurity policy covering information security, operational security, network security, disaster recovery planning and application security is crucial for the two categories of data centers.

Additionally, the policies and coverage areas of Cybersecurity must be cognizant of the fact that the data security risks are continually evolving. Therefore, Cybersecurity policies are most suitable if they are adaptive and proactive. Some of the remarkable products available off shelf providing essential Internet security include MacAfee, Cisco, Kaspersky's, and Trend Micro. Educational institutions have also engaged qualified professionals in the field to advise and monitor the safety and security of their data and networks. Among the notable employees include titles such as chief information security officer, security engineers, security analysts, and security architects [4].

Cybersecurity awareness on the other hand is an essential Cybersecurity measure that involves spreading public awareness and empowering the people using the systems. Awareness in this field involves being mindful of threat reaction plans, defensive procedures, as well as attack red flags that non-technical employees can use to safeguard themselves and the institution's resources from cyber-attacks. Most institutions harboring academic and personal data have a have fully-fledged digital platform, as well as Cybersecurity toolkits for managing the security of student records and payroll. The most common of the Cybersecurity toolkit include secure wireless networks, encryption tools, digital certificates, safe browsing tools, data disposal protocols, 2-step verifications for personal login details, as well as checklists for lost devices.

Web-based training against cyber attacks, both in-house and custom-made, should be prioritized and made available to employees and students within educational institutions [5]. This paper comprehensively evaluates the Cybersecurity risks facing academic and personal data in the context of educational institutions. It also emphasizes the importance of the TAM model, which includes increasing the awareness of Cybersecurity, its attainability as well as its implementation [5]. Eight hypotheses were developed to investigate the different influences on the proposed model. This makes this study a very important study especially in the emerging technologies of the cyber space.

2. Literature Review

2.1. Cybersecurity Background

Technology has resulted in the proliferation of information through different arrays, including academia, smart cities and manufacturing automation. This spread has resulted in opportunistic changes such as an increased quality of life, effective service delivery and an increase in the number of clients that can be effectively served [6]. For instance, through the automation of most of the academic document management systems and learner material delivery, one instructor can comprehensively manage and assess large numbers of learners per class, in contrast to the smaller numbers generated by a manual system. On the other hand, the deployment and proliferation of Information and Communications Technology (ICT) has resulted in significant challenges to data security. The demanding matter of privacy when choosing a technology platform to adopt as an institution remains paramount, in addition to the consent of the platform owners to the option chosen [7] [8] [9]. Social media platforms including Facebook, Twitter, Instagram and Google among others have had challenges in the compliance of privacy and data security laws of other countries in the European Union as well as Australia [10] [11] [12]. While there are remarkable benefits to the adoption of robust technological solutions in academic fronts as well as personal life, privacy threats initiated by pirates and hackers fraudulently accessing otherwise private data as a result of the Internet connectivity of ICT remain a significant drawback [13].

Modern society significantly depends on technology in most of its facets. More often than not, ICT based devices are interdependent, which suggest that despite one party being robust and proactive in securing data, failure of other devices to abide by privacy laws holds a negative effect on the rest [14]. Consequently, there are concerns about the process of authorizing the government a role in the protection of data through legislation and eventually institutions, which imply that governments may unlawfully access the private data of its citizens for surveillance means and political gain [15].

Traditionally, Cybersecurity has been largely associated with the software elements of ICT devices, however, recent findings have demonstrated otherwise. Huawei Technologies have demonstrated that at the point of manufacturing, hardware may be made to illegitimately and clandestinely transmit data to the manufacturer [16]. The transmission of such data results in surveillance and data breach, and governments as well as private institutions should strive to ensure the safety and integrity of their data [17].

As stated by experts and policy makers, the frequency and severity of cyber attacks is anticipated to continue rising and venturing into areas that were not prime targets in the past, such as academic data. Personal data has always been targeted by hackers because of the value attached to it by marketing institutions and the field of social engineering [18].

2.2. Cybersecurity Attacks on Academic Data

Academic data has become a prime target for cyber-attacks owing to the invaluable user information, computing resources, instrument designs, proprietary compounds, personal communications, and patient data for schools offering referral hospital services [19] [20]. Most of the information is accessible to devices that are connected to the World Wide Web via the Internet. As such, it is imperative that the developers of such websites must have sufficient experience to mitigate the chances of having a "poorly written code, open ports or digital entry points" [21]. This would compromise the operating system and computer hardware of the institutions. According to Perkel [22] and Kent [23], cyber-attacks are varied and may come from unlikely sources such as the "installation of programs intended to co-opt system resources to keystroke loggers and scanning software designed to purloin user information and passwords" (p. 1261).

Research data has become the new front for cyber-attacks alongside a range conflicting interests between researchers and the information security experts. On the one hand, information security experts advocate for a system that is centralized in an attempt to enhance monitoring and system administration aspects such as limiting access and monitoring the traffic to such storage systems [24]. On the contrary, the ethos of researchers is that such data should be readily available to students, fellow researchers, and collaborators [25]. Fortunately, advances in security solutions have, to an extent, enabled academic data to be managed in an unconstrained manner [26] [27]. Similarly, hackers have developed their skills in proliferating such systems. As a result, the Cybersecurity advances to academic data can be viewed as a continuously evolving phenomenon that will continue in perpetuity [23].

Drive-by hackers rank the highest amongst the reported number of attempted cyber-attacks on educational networks. In most instances, the drive-by hackers are professionals in the organized crime industry or in some instances State actors whose intentions largely remain unknown. Universities continue to report a rising number of attacks and data breaches according to EDUCAUSE [23] [28] [29]. EDUCAUSE is a non-profit organization established by higher education IT professionals and as such provides some of the most credible data on Cybersecurity incidences in relation to the academic sector [30] [31]. Besides, the organization has transformed to providing invaluable insights relating to policy and best practices when securing research data. Despite the remarkable contribution of such organizations, some challenges remain prominent such as underfunding and researcher independence [32].

Researcher independence presents the largest challenge to the implementation of security policies on academic data, more specifically research related data. Cybersecurity and information systems management largely fall under the administrative field. Researcher needs may not conform to the procedural nature of Cybersecurity protocols already in place for universities and other academic institutions. For instance, the nature of the researcher's work demands installing of certain software programs; collaborating with colleagues from different parts of the world in addition to developing and deploying tools that are designed for both private and public consumption [33]. The degree of such instances varies between the works of different researchers, and thus may result in the exposure of an institution's networks to unauthorized access and manipulation [22] (p. 1261).

Despite improvements in technology such as the invention of virtual machines that allow all users to practically log on to a central computer that can be managed by the information security experts, breaches are still occurring. The benefits remain that that despite any attack, a properly managed central computer can be rolled back in a matter of seconds. Therefore, Cybersecurity shifted its focus beyond mitigating cyber-attacks; to acknowledging that they are inevitable and consequently new policies are being created to ensure that data is always available [34] [35]. Cloud computing solutions have immensely contributed to immediate data recovery as well as backup integrity since they are mostly managed by highly specialized professionals using state of the art equipment and in most cases anonymous locations [25]. Virtual machines and cloud computing solutions including isolated architectures helps in reducing the chances of a cyber-attack more effectively in addition to the professional security provided, continuous monitoring, auto backup and restoration protocols [36].

2.3. Cybersecurity Attacks on Personal Information

At present, society is, more than ever, facing a myriad of sophisticated security risks in cyberspace as a result of the evolution of malicious cyber-attacks [37] [38] [39] [40]. According to Li, *et al.*, [41] employees should be knowledgeable of the information security policies and procedures within the corporations they work in, as a means to competently manage Cybersecurity tasks. Moreover, given an individual's extensive use of technological devices, from smart homes, smartphones, and personal computers to using credit cards to purchase from e-commerce websites, awareness should be prioritized in order to mitigate cyber-attacks on personal information [41] [42] [43].

Social engineering has increasingly become the most frequent threat to individual users in the cyberspace. Human hacking largely involves using immoral means to gain access to individuals' credentials such as passwords, credit card details and bank accounts and using them to gain access to secure networks. Among the well documented approaches that hackers employ to access confidential user information through the "manipulation of people's tendency to trust, or baiting them as they try to follow their curiosities and desires" [44] [45]. Despite the high levels of awareness among consumers regarding the dangers of the cyberspace to personal information, some individuals still fall prey to the hacker's tricks. For instance, a 2013 TNS Global for Hannon study on email user's vigilance revealed that more than thirty percent of users tend to open an email with the full knowledge that the contents could be harmful and malicious [44] (p. 32).

The struggle that hackers go through to access personal data leads to the question of the motivation behind such attacks. According to a 2012 study by Chitery, *et al.* [46], "to evaluate the variables of cause and identifying the susceptible members of an organization, financial gain, access to proprietary information, competitive advantage, revenge, fun, and other unspecified reasons ranked the highest" [47]. On the other hand, the most likely entities to fall prey for cyber-attacks targeting personal information include new employees, IT professionals, clients, partners and contractors, and top-level management. The techniques used in this case include "emails with internal URLs, emails with external URLs, beacon documents, and forms to obtain credentials" [22].

Given the extent of the damage caused by attacks on personal information, preventive measures against the attacks are the best course of action to be taken to mitigate such attacks. In contrast to industrial or institutional scales, it is unlikely that individuals would have backups for their data or recovery measures. Moreover, the data targeted is unlikely to be salvaged once the breach has taken place [48] [49]. Audits and compliance can also minimize the chances of cyber-attacks on personal information by having technical teams review network logs, revalidating employee credentials, and reviewing desktop security configuration regularly. In addition to audits, technical procedures can also be implemented to protect personal data within an enterprise. For instance, all external facing services should have firewalls, virtual private networks, intrusion prevention systems, and intrusion detection systems installed in a bid to provide layers of defense and data protection against fraudsters on the internet [50] [51] [52] [53]. Other measures include the provision of a well-documented security policy as well as physical guidance to protect physical assets associated with personal data [54].

3. Hypotheses and Research Framework

Based on the previously deliberated literature and our research objectives of filling the gaps, the following hypotheses were constructed:

H1. Awareness of Cybersecurity has a significant influence on perceived ease of use of Cybersecurity.

H2. Attitudes towards Cybersecurity have a significant influence on perceived ease of use of Cybersecurity.

H3. Knowledge about Cybersecurity has a significant influence on perceived ease of use of Cybersecurity.

H4. Perceived ease of use of Cybersecurity has a significant influence on attitude towards using Cybersecurity.

H5. Attitude towards using Cybersecurity have a significant influence on actual use of Cybersecurity.

H6. Job positions have a moderator role influence on perceived ease of use of Cybersecurity.

H7. Job positions have a moderator role significant influence on attitude towards using Cybersecurity.

H8. Job positions have a moderator role influence on actual use of Cybersecurity.

The proposed research model (see **Figure 1**) is constructed to determine the moderator's role of education and Job position between TAM constructs. Therefore,

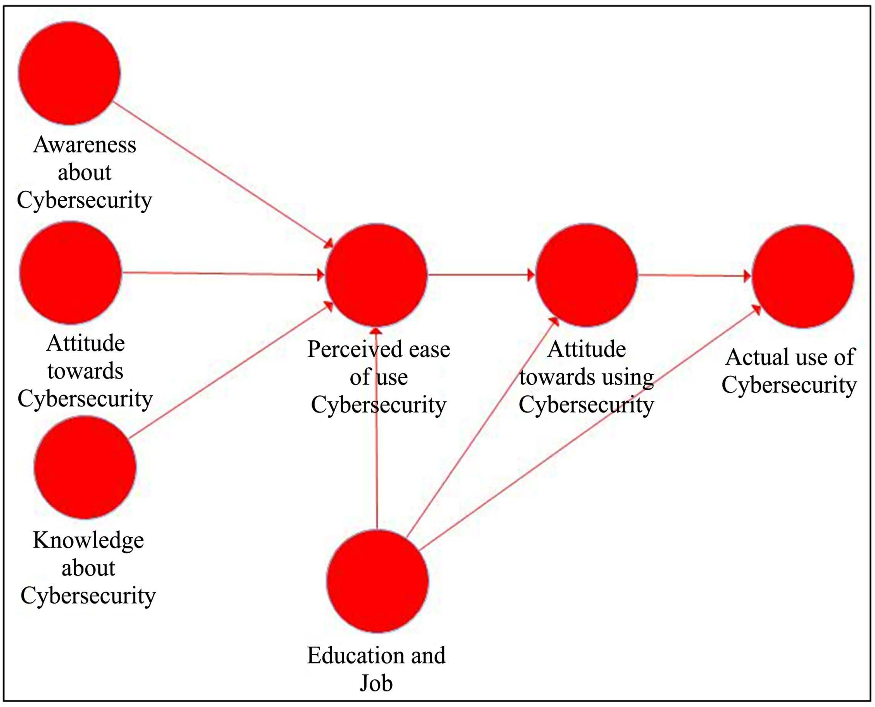
Awareness about Cybersecurity
Attitude towards Cybersecurity
Knowledge about Cybersecurity
Perceived ease of use Cybersecurity
Attitude towards using Cybersecurity
Actual use of Cybersecurity
Education and Job

Figure 1. Research model.

eight hypotheses were established, and research models were expressed as shown in Figure 1.

4. Result Analysis

4.1. Demographic Profile and Data Collection

An online questionnaire was distributed to Academic staff in Yanbu branch at Taibah University asking them to answer the questionnaire. An overall of 112 respondents, of which 90 accomplished questionnaires ensuing in a response rate of about (80%) were investigated after two weeks of distributing the questionnaires data. The respondent's Jobs profile were as follows: faculty of computer science (88%), faculty of business (5%), faculty of science (4%), and (3%) employed in the faculty of engineering.

Amongst the respondents, 8% had a master's degree, 92% had a PhD degree, 22% had less than five years of academic experience, whereas (70%) had academic experience ranging between 5 - 10 years, and 8% of respondents had more than 10 years of academic experience.

The questionnaire encompassed three sections: The first section measured the demographic analysis of the respondents' employees: gender, age, position, and educational level. The second section measured TAM model determined by awareness of Cybersecurity; attitude towards Cybersecurity; knowledge about Cybersecurity; perceived ease of use Cybersecurity; attitude towards using Cybersecurity; and actual use of Cybersecurity. Last, the third section measured the Job position as a mediator. All questionnaire items measured using the five-point Likert scale ranging from "strongly disagree" to "strongly agree".

4.2. PLS Path Modeling

This article deployed Smart PLS 3 software for analysis. The software uses the Partial Least Structural Equation Modeling (PLS-SEM) technique [54]. The author used 5000 subsamples to get significant values of path coefficients and factors loading according to Hair Jr. *et al.*, [50]. Smart PLS have some of the advantages over other tools. For instance, Smart PLS better realizes the regression estimation. It is essential to estimate measurement model (outer model) and structural model (inner model) in PLS-SEM. Fornell and Larcker [43] summarized the measurement model must have an adequate level of validity and reliability before testing the model structure. Construct reliability appraised by calculating the internal consistency, whereas the average value extracted (AVE) and the composite reliability were assessed using Cronbach's alpha. The results illustrated an acceptable level of consistency, as validity results were above the recommended cut-off value of (0.70) as demonstrated in Cronbach's alpha values of each construct (see **Table 1**).

The analysis in **Table 1** illustrated the actual use construct R2 = 0.398 which indicated that the size of the explanatory power of this form was low but enough; whereas the regression of attitude towards using Cybersecurity = 0.864 which indicated that the size of the explanatory power of this form was high; also as illustrated in **Table 1**. The R2 of Cybersecurity ease of use was 0.674. Hence, the above constructs were statistically significant. **Table 2** reveals that all constructs fulfills latent constructs correlations ranging from 0.448 to 0.887, which are below the threshold of 0.90 [47]. Above results satisfy the discriminant validity.

As shown in **Table 3** and **Figure 2** the path coefficient (beta) value for all hypotheses 1; 2; 3; 4; 5; 6; 7 ranges from 0.207 to 0.85 and T test ranges from 2.042 to 4.324 significant and thus support hypotheses 1; 2; 3; 4; 5; 6; 7. Unexpectedly, H8 is negative and not significant; path coefficient (beta) −252; T test −1.287; P value 0.234, and thus does not support hypothesis H8.

Table 1. Reliability and validity results.

	AVE	Composite Reliability	R Square	Cronbachs Alpha
Job	0.710964	0.879733		0.791708
Actual use	0.839816	0.912932	0.398045	0.809451
Attitude	0.475189	0.782652		0.633675
Attitude using	0.504196	0.798668	0.864086	0.664109
Awareness	0.582231	0.844607		0.746319
Ease of Use	0.401083	0.817893	0.674458	0.746466
Knowledge	0.607841	0.821674		0.670050

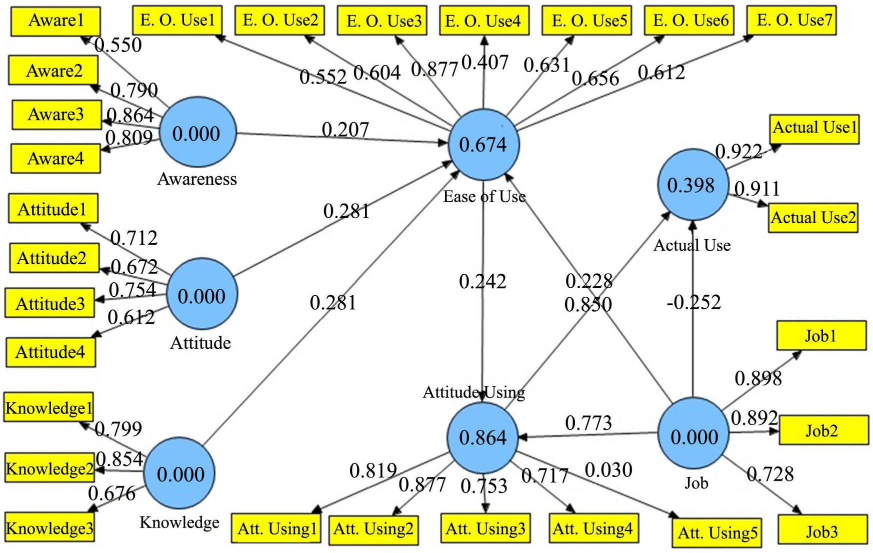

Figure 2. PLS results.

Table 2. Latent constructs correlations.

	Job	Actual use	Attitude	Attitude using
Job	1.000000			
Actual use	0.520076	1.000000		
Attitude	0.476786	0.626368	1.000000	
Attitude using	0.887505	0.621995	0.580996	1.000000
Awareness	0.448984	0.645107	0.694776	0.463624
Ease of Use	0.554895	0.834780	0.722727	0.671034
Knowledge	0.358299	0.538601	0.675882	0.503419

Table 3. Direct effects.

Items	Path coefficient	T statistics	P values	Result
H1	**0.207**	**2.042**	**0.015**	**accept**
H2	**0.281**	**2.514**	**0.014**	**accept**
H3	**0.281**	**2.496**	**0.042**	**accept**
H4	**0.242**	**2.100**	**0.092**	**accept**
H5	**0.850**	**4.324**	**0.000**	**accept**
H6	**0.228**	**2.132**	**0.034**	**accept**
H7	0.773	3.991	0.000	accept
H8	−0.252	−1.287	0.234	rejected

5. Conclusion

This research investigated factors that affect that may have an influence on perceived ease of use of Cybersecurity, the influence of perceived ease of use on the attitude towards using Cybersecurity, the influence of attitude towards using Cybersecurity on the actual use of Cybersecurity and the influences of job positions on perceived ease of use of Cybersecurity and on the attitude towards using Cybersecurity and on the actual use of Cybersecurity. It was found that awareness of cybersecurity, attitude of cybersecurity and knowledge of cybersecurity have a significant impact on perceived ease of use of cybersecurity. Moreover, it was shown that perceived ease of use has a significant impact on attitude towards using Cybersecurity. Furthermore, attitude towards using Cybersecurity has a significant impact on actual use of Cybersecurity. Job Satisfaction was found to have a moderator role influence on perceived ease of use of Cybersecurity and on the attitude towards using Cybersecurity. However, it was found that job positions have no influence on actual use of Cybersecurity.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Abele, E., Chryssolouris, G., Sihn, W., Metternich, J., Elmaraghy, H., Seliger, G., Sivard, G., ElMaraghy, W., Hummel, W., Tisch, M. and Seifermann, S. (2017) Learning Factories for Future Oriented Research and Education in Manufacturing. *CIRP Annals*, **66**, 803-826. https://doi.org/10.1016/j.cirp.2017.05.005

[2] Adams, N. and Heard, N. (2016) Security Science and Technology, Vol. 1: Dynamic Networks and Cyber-Security. World Scientific Publishing, Singapore. https://doi.org/10.1142/q0022

[3] Addae, J.H., Brown, M., Sun, X., Towey, D. and Radenkovic, M. (2017) Measuring Attitude towards Personal Data for Adaptive Cybersecurity. *Information and Computer Security*, **25**, 560-579. https://doi.org/10.1108/ICS-11-2016-0085

[4] August, T. and Tunca, T.I. (2011) Who Should Be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments. *Management Science*, **57**, 934-959. https://doi.org/10.1287/mnsc.1100.1304

[5] Bhatia, J., Breaux, T.D., Friedberg, L., Hibshi, H. and Smullen, D. (2016) Privacy Risk in Cybersecurity Data Sharing. *Proceedings of the* 2016 *ACM on Workshop on Information Sharing and Collaborative Security* (*WISCS* 16), Vienna, 24 October 2016, 57-64. https://doi.org/10.1145/2994539.2994541

[6] Blythe, J. and Johnson, S. (2018) The Consumer Security Index for IoT: A Protocol for Developing an Index to Improve Consumer Decision Making and to Incentivize Greater Security Provision in IoT Devices. *Living in the Internet of Things*: *Cybersecurity of the IoT*-2018, London, 28-29 March 2018, 1-7. https://doi.org/10.1049/cp.2018.0004

[7] Bologa, R., Lupu, A.R., Boja, C. and Georgescu, T. (2016) Sustaining Employability: A Process for Introducing Cloud Computing, Big Data, Social Networks, Mobile Programming and Cybersecurity into Academic Curricula. *Sustainability*, **9**, Article No. 2235. https://doi.org/10.3390/su9122235

[8] Brown, A.E. and Grant, G.G. (2005) Framing the Frameworks: A Review of IT Governance Research. *Communications of the Association for Information Systems*, **15**, 696-712. https://doi.org/10.17705/1CAIS.01538

[9] Carin, L., Cybenko, G. and Hughes, J. (2018) Cybersecurity Strategies: The QuERIES Methodology. *Computer*, **41**, 20-26. https://doi.org/10.1109/MC.2008.295

[10] Cherdantseva, Y. and Hilton, J. (2013) A Reference Model of Information Assurance & Security. 2013 *International Conference on Availability*, *Reliability and Security*, Regensburg, 2-6 September 2013, 546-555. https://doi.org/10.1109/ARES.2013.72

[11] Chiravuri, A. and Nazareth, D. (2001) Consumer Trust in Electronic Commerce: An Alternative Framework Using Technology Acceptance. *Proceedings of* 2001 7*th Americas Conference on Information Systems*, Boston, USA, January 2001, Article No. 152.

[12] CNIL (2019, January 21) The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC. https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[13] Cohen, E.B. (2011) Navigating Information Challenges: Issues in Informing Science and Information Technology. Informing Science Press, Santa Rosa.

[14] Conteh, N.Y. and Schmick, P.J. (2016) Cybersecurity: Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks. *International Journal of Advanced Computer Research*, **6**, 31-38. https://doi.org/10.19101/IJACR.2016.623006

[15] Daniel, B. (2014) Big Data and Analytics in Higher Education: Opportunities and Challenges. *British Journal of Educational Technology*, **46**, 904-920. https://doi.org/10.1111/bjet.12230

[16] Dasgupta, S., Granger, M. and McGarry, N. (2002) User Acceptance of E-Collaboration Technology: An Extension of the Technology Acceptance Model. *Group Decision and Negotiation*, **11**, 87-100. https://doi.org/10.1023/A:1015221710638

[17] Dua, S. and Du, X. (2011) Data Mining and Machine Learning in Cybersecurity. Auerbach Publications, Boca Raton.

[18] Evans, M., Maglaras, L.A., He, Y. and Janicke, H. (2016). Human Behaviour as an Aspect of Cybersecurity Assurance. *Security and Communication Networks*, **9**, 4667-4679. https://doi.org/10.1002/sec.1657

[19] Evers, V. and Day, D. (1997) The Role of Culture in Interface Acceptance. *Human-Computer Interaction INTERACT*'97, Springer, Boston, 260-267. https://doi.org/10.1007/978-0-387-35175-9_44

[20] Farooq, A., Isoaho, J., Virtanen, S. and Isoaho, J. (2015) Information Security Awareness in Educational Institution: An Analysis of Students Individual Factors. 2015 *IEEE Trustcom*/*BigDataSE*/*ISPA*, Helsinki, 20-22 August 2015, 352-359. https://doi.org/10.1109/Trustcom.2015.394

[21] Fornell, C. and Larcker, D.F. (1981) Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research*, **18**, 382-388. https://doi.org/10.2307/3150980

[22] Furman, S., Theofanos, M.F., Choong, Y.Y. and Stanton, B. (2012). Basing Cybersecurity Training on User Perceptions. *IEEE Security & Privacy Magazine*, **10**, 40-49. https://doi.org/10.1109/MSP.2011.180

[23] Hai Jr., J.F., Hult, G.T., Ringle, C. and Sarstedt, M. (2016) A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Sage Publications, Los Angeles.

[24] Henseler, J., Hubona, G. and Ray, P.A. (2016) Using PLS Path Modeling in New Technology Research: Updated Guidelines. *Industrial Management & Data Systems*,

116, 2-20. https://doi.org/10.1108/IMDS-09-2015-0382

[25] Hibshi, H., Breaux, T.D. and Broomell, S.B. (2015) Assessment of Risk Perception in Security Requirements Composition. 2015 *IEEE* 23*rd International Requirements Engineering Conference* (*RE*), Ottawa, 24-28 August 2015, 146-155. https://doi.org/10.1109/RE.2015.7320417

[26] Hina, S. and Dominic, D.D. (2017) Need for Information Security Policies Compliance: A Perspective in Higher Education Institutions. 2017 *International Conference on Research and Innovation in Information Systems* (*ICRIIS*), Langkawi, 16-17 July 2017, 1-6. https://doi.org/10.1109/ICRIIS.2017.8002439

[27] Hoofnagle, C.J., Sloot, B.V.D. and Borgesius, F.Z. (2019) The European Union General Data Protection Regulation: What It Is and What It Means. *Information & Communications Technology Law*, **28**, 65-98. https://doi.org/10.1080/13600834.2019.1573501

[28] Isaak, J. and Hanna, M.J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, **51**, 56-59. https://doi.org/10.1109/MC.2018.3191268

[29] Jabbour, C., Rey-Valette, H., Maurel, P. and Salles, J.M. (2019) Spatial Data Infrastructure Management: A Two-Sided Market Approach for Strategic Reflections. *International Journal of Information Management*, **45**, 69-82. https://doi.org/10.1016/j.ijinfomgt.2018.10.022

[30] Karre, H., Hammer, M., Kleindienst, M. and Ramsauer, C. (2017) Transition towards an Industry 4.0 State of the LeanLab at Graz University of Technology. *Procedia Manufacturing*, **9**, 206-213. https://doi.org/10.1016/j.promfg.2017.04.006

[31] Kent, A.D. (2016) Cyber Security Data Sources for Dynamic Network Research. In: Adams, N. and Heard, N., Eds., *Security Science and Technology*: *Dynamic Networks and Cyber-Security*, Vol. 1, World Scientific Publishing, Singapore, 37-65. https://doi.org/10.1142/9781786340757_0002

[32] Khan, M.A. (2017) A Survey of Security Issues for Cloud Computing. *Journal of Network and Computer Applications*, **71**, 11-29. https://doi.org/10.1016/j.jnca.2016.05.010

[33] Kuner, C., Svantesson, D.J.B., Cate, F.H., Lynskey, O. and Millard, C. (2017) The Rise of Cybersecurity and Its Impact on Data Protection. *International Data Privacy Law*, **7**, 73-75. https://doi.org/10.1093/idpl/ipx009

[34] Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019) Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior. *International Journal of Information Management*, **45**, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

[35] Liu, C.W., Huang, P. and Lucas, H.C. (2016) Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*. https://doi.org/10.2139/ssrn.2850178

[36] McIlwraith, A. (2006) Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness. Gower Publishing, Ltd., Aldershot.

[37] Lv, I., Mehmood, Z., Zhang, Y.D., Ota, K., Sajjad, M. and Singh, A.K (2019) Mobile Cloud-Assisted Paradigms for Management of Multimedia Big Data in Healthcare Systems: Research challenges and opportunities. *International Journal of Information Management*, **45**, 246-249. https://doi.org/10.1016/j.ijinfomgt.2018.10.020

[38] Mori, S. (2019) US Technological Competition with China: The Military, Industrial and Digital Network Dimensions. *Asia-Pacific Review*, **26**, 77-120.

https://doi.org/10.1080/13439006.2019.1622871

[39] Perkel, J. (2010) Cybersecurity: How Safe Are Your Data? *Nature*, **464**, 1260-1261. https://doi.org/10.1038/4641260a

[40] Qian, X. (2019) Cyberspace Security and U.S.-China Relations. *Proceedings of the* 2019 *International Conference on Artificial Intelligence and Computer Science—AICS* 2019, Wuhan, July 2019, 709-712. https://doi.org/10.1145/3349341.3349495

[41] Rebollo, O., Mellado, D., Fernández-Medina, F. and Mouratidis, H. (2015) Empirical Evaluation of a Cloud Computing Information Security Governance Framework. *Information and Software Technology*, **58**, 44-57. https://doi.org/10.1016/j.infsof.2014.10.003

[42] Rouibah, K. and Abbas, H. (2010) Effect of Personal Innovativeness, Attachment Motivation and Social Norms on the Acceptance of Camera Mobile Phones: An Empirical Study in an Arab Country. *International Journal of Handheld Computing Research*, **1**, Article No. 3. https://doi.org/10.4018/jhcr.2010100103

[43] Safa, N.S., Solms, R.V. and Furnell, S. (2016) Information Security Policy Compliance Model in Organizations. *Computers & Security*, **56**, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

[44] Schechner, S. (2019) EU Nears Decisions in Facebook Privacy Cases. https://www.wsj.com/articles/eu-nears-decisions-in-facebook-privacy-cases-11565602202

[45] Sherman, A., Dark, M., Chan, A., Chong, R., Morris, T., Oliva, L., Springer, J., Thuraisingham, B., Vatcher, C., Verma, R. and Wetzel, S. (2017) INSuRE: Collaborating Centers of Academic Excellence Engage Students in Cybersecurity Research. *IEEE Security & Privacy*, **15**, 72-78. https://doi.org/10.1109/MSP.2017.3151327

[46] Smeureanu, I. and Isaila, N. (2011) Information Technology, Support for Innovation in Education Sciences. *Procedia—Social and Behavioral Sciences*, **15**, 751-755. https://doi.org/10.1016/j.sbspro.2011.03.177

[47] Solms, B.V. and Solms, R.V. (2018) Cybersecurity and Information Security—What Goes Where? *Information and Computer Security*, **26**, 2-9. https://doi.org/10.1108/ICS-04-2017-0025

[48] Taneja, A. and Arora, A. (2019) Modeling User Preferences Using Neural Networks and Tensor Factorization Model. *International Journal of Information Management*, **45**, 132-148. https://doi.org/10.1016/j.ijinfomgt.2018.10.010

[49] Thames, L. (2017) Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing. Springer, Cham. https://doi.org/10.1007/978-3-319-50660-9

[50] Trim, P.R.J. and Upton, D. (2013) Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training. Routledge, London. https://doi.org/10.4324/9781315575681

[51] Vakilinia, I. and Sengupta, S. (2019) A Coalitional Cyber-Insurance Framework for a Common Platform. *IEEE Transactions on Information Forensics and Security*, **14**, 1526-1538. https://doi.org/10.1109/TIFS.2018.2881694

[52] Wangen, G., Shalaginov, A. and Hallstensen, C. (2018) Cyber Security Risk Assessment of a DDoS Attack. *International Conference on Information Security*, Honolulu, 3-6 September 2016, 183-202. https://doi.org/10.1007/978-3-319-45871-7_12

[53] Wilson, C. (2020) Running Head: Electronic Data Breaches and Legislation in The U.S.: An Analysis of the Relationship between Recent Electronic Data Breaches and Enacted Data Security and Privacy Legislation in The United States. Honors Bachelor Thesis, Appalachian State University, North Carolina.

https://libres.uncg.edu/ir/asu/f/Wilson_Christian_Spring%202020_Thesis.pdf

[54] Wong, K.K.K. (2013) Partial Least Squares Structural Equation Modeling. In: Homburg, C., Klarmann, M. and Vomberg, A.E., Eds., *Handbook of Market Research*, Springer, Cham, 1-47. https://doi.org/10.1007/978-3-319-05542-8_15-2