ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 12 (2022) No. 5, pp. 282-296
DOI:10.33168/JSMS.2022.0517

A Review on the Challenges and Connections between Cybersecurity and Accounting in Saudi Arabia

Badi Alrawashdeh [1+], Anas Ghazalat [2]

[1] Arab Open University, Saudi Arabia
[2] Arab Open University, Jordan

b.rawashdeh@arabou.edu.sa (corresponding author)

Abstract. The current study seeks to highlight the existing relationship between the two fields of accounting and cybersecurity by conducting a thorough review of the literature on the subjects and discussing a few of the most important terms about the two subjects. In addition to a discussion of the obstacles to the implementation of cybersecurity systems in businesses, this paper sheds light on the relationship between the two fields. A viewpoint on the current state of affairs in KSA regarding advancements in the field of cybersecurity is discussed, as well as a study prepared by Kasasbeh, F. I. O., & Thuneibat, N. S. M. (2018), to showcase the ability of Saudi firms and universities in facing cyber threats. All lead to a conclusion and findings of the research in hand, as well as the mentioned study.

Keywords: accounting, information technology, cybersecurity, finance.

1. Introduction

Cybersecurity is progressively being perceived as a serious various levelled issue that is best tended to by consolidating it as a part of the managerial control structure (Haapamäki, E., and Sihvonen, J. (2019). This progress is halfway because of interest and the board by regulatory subject matter experts, and for the most part because of extended direction from the Big 4 accounting firms and audit industry affiliations (AICPA. 2018).

Market discipline has an impact also (Pendley, J. A. 2018). As a feature of a managerial control structure, cybersecurity has likewise turned into huge regulatory bookkeeping and examining the issue, likely to cost-cutting benefit examination, interior control assessment, and openness methodology contemplations. The reason for this paper is to propel the examination concerning network security in the bookkeeping field by exploring how well continuous composing watches out for the bookkeeping implications of those objectives, as well as to endeavour to add more substance to the current writing survey, to propel this field of study.

This writing blend fills a few significant needs. To start, an exhaustive diagram of the momentum insightful data on network protection in bookkeeping and reviewing research is given, as well as an assortment of classes into which these assessments fit. The following objective is to distinguish key subjects and issues that have arisen in past compositions. At long last, the objective is to recognize holes in the composition and suggest useful future examinations and valuable open doors. This composing examination has broad ramifications for exploration and practice, for instance, by posting the advantages and disadvantages of information sharing.

This examination likewise incorporates Gordon and Loeb's model's importance for network protection adventures (2002). Their model, known as the Gordon-Loeb Model, got a great deal of thought in its composition. It adds to consistent investigation and practice by giving a financial model that decides the best aggregate to place assets into getting a given game plan of information. This examination additionally incorporates the occupation of inspecting and controls to additionally foster online protection. It underlines the significance of clear and smooth interest in evaluating IT limits.

The rising utilization of advanced innovations among associations has underlined the importance and job of network safety as another gamble that chiefs should consider, not least because computerized risks and dangers stand out from the overall population (Zadorozhnyi, Z. M., Muravskyi, V., and Muravskyi, V. 2021). Besides, firms that are designated by digital assaults are bound to experience reliable monetary and reputational misfortunes (Halbach, H. 2021). As per progressing research, network safety has developed into one of the main gamble difficulties facing each sort of association and society in only a couple of years.

2. Literature Review

A useful review fills in as an establishment for dispersing data (Demirkan, S., Demirkan, I., and McKee, A. 2020). Besides, for what reason truly does coordinate zero in on network safety in the bookkeeping and evaluating field? The number and seriousness of digital dangers have as of late been remarkable, and powerful digital assaults have been reliably represented (Wilamowski, G. C. 2017). Moreover, the expenses of digital assaults are tremendous; hence, network protection risk for the executives is contended to be basic for associations (Wilamowski, G. C. 2017).

Also, Zadorozhnyi, Z., Muravskyi, V., and Shevchuk, O. (2020) recommended that the web unrest has altogether adjusted the way individuals, organizations, and government offices convey and lead business. For instance, the danger of digital mental fighting has pushed network protection to the very front of the public course of action system.

Besides, Clark, D., Berson, T., and Lin, H. S. (2014) expressed that the developing dependence of both public and confidential areas on Web-based innovations and associations for their monetary organization systems includes some major disadvantages, and this cost is an expanded shortcoming. In any case, Rue, R., Pfleeger, S. L., and Ortiz, D. (2007). successfully guaranteed that for certain associations, information and the innovation that upholds it address their most significant assets.

Mourn, R., Pfleeger, S. L., and Ortiz, D. (2007) contended that in this worldwide information society, where information goes through the internet, it is fundamental to propel an organization. In this way, the fruitful organization is related to an emphasis on growing shortcomings, for example, digital assaults and information battling. The rules affect the inspiration for relationships to put resources into security innovation.

For instance, the Sarbanes-Oxley Act of 2002 (SOX) forced tough prerequisites on organizations (Kim, N. Y., Robles, R. J., Cho, S. E., Lee, Y. S., and Kim, T. H. 2008). The SOX features the meaning of information system controls by requiring organizations and assessors to research the feasibility of inside controls over the monetary detailing piece of the association's organization information structures (Karanja, E., and Zaveri, J. 2014). Gordon, I. M., and Nazari, J. A. (2018), for instance, inspected the impact of SOX on the conscious revelation of information security practices by associations.

The specific confirmation given showed that SOX altogether affects deliberate openness. Gordon, I. M., and Nazari, J. A. (2018) gave strong incidental proof that corporate information security practices stand out since the SOX's execution than previously. They surely upheld the generally held conviction that network protection is a notable necessity of the interior control structure. They contended that the

information content of information security practices is higher in certain endeavours than in others.

Banks, business organizations, security, media correspondences, monetary administrations, transportation, and clinical consideration, for instance, have every one of the reserves of being more proactive in giving purposeful openness of wellbeing, related works out (Gordon, I. M., and Nazari, J. A. (2018) Furthermore, Willemson, J. (2006) proposed rules for skilled online protection organization. Their money-saving advantage examination contrasts the expenses of activity with its advantages, and the makers fought that as long as the advantages of an extra information security development offset the expenses, taking part in that action is significant.

Moreover, that's what they expressed, while expanded online protection doesn't by and large help an association, digital assaults are one of the essential dangers that associations should make due (Willemson, J. 2006). Considering the prior contentions, it is basic to consolidate past network protection composing and recognize the assessment surges of the articles under the survey (Gordon, L. A., Loeb, M. P., and Zhou, L. 2016).

The previous literature explores the threat between cybersecurity and accounting but does not define a clear role for firms to address cyber threats to computerized accounting information systems. Our research aimed to address this deficiency by evaluating the Capability of Computerized Accounting Information Systems in Saudi Public Universities to Face Cyber Threats. To address this escalating issue, we sought to identify current cyber threats to the computerized account information system (CAIS) in Saudi universities in order to mitigate security concerns.

2.1. Cybersecurity limitations

There are various techniques that organizations can use to fortify their network protection against the most serious dangers. To start, there is a significant ofteachg workers about network protection dangers and GivGivethentic preparation to representatives on what to pay special attention to and normal practices utilized by digital assailants. Readiness is basic on because as per an IBM study, "95% of network safety breaks are brought about by human blunder" (Halbach, H. 2021). The following methodology is to have an IT control that anticipates that workers should areas of strhave engthutilisationilize.

An illustration of this would be a mystery key with around 8 characters and the utilization of a picture, number, and letter all through the mystery key. An organization can likewise set up a multi-layered confirmation process. To draw near enough to the data, a delegate should give something like two factors. Another compelling practice is to erase old or superfluous information.

This is successful by lessening how much data the firm is expected to give and is at risk of being gone after. Subsequently, it disposes of the lawful outcomes that an organization could confront assuming there is a data break. This empowers organizations to distinguish flimsy parts and carry out the essential changes to resolve those issues. This methodology requires keeping awake to date on the latest hacking procedures to figure out which piece of the association's organization's security is as now exposed.

Firms can likewise recruit an outsider cybersecurity firm to assist with counselling them on their weak places and give them proposals on the best way to cure the circumstance. As well as, introducing antivirus and cybersecurity programming to caution firms of possible dangers or information breaks. These are the most well-known procedures to assist with fortifying cybersecurity utilized throughout the accounting business.

Some of the Common Weaknesses and Threats for Cybersecurity:

1. Cybersecurity can be Expensive for Businesses: Organizations that require more funds to secure their information and frameworks may suffer as a result of this burden. It is not unusual for a company to need to invest more in cybersecurity than it receives. This is the fundamental reason why many organizations are hesitant to invest in cybersecurity (Mohammed, D., Mariani, R., & Mohammed, S. 2015).
2. Network Protection can be Confusing for Firms: Online security measures necessitate a significant amount of time and effort. Indeed, for some organizations, it can be too difficult to even consider understanding. This can cause a slew of problems in a business. It can also result in data loss or a security breach if the organization does not have the appropriate security instruments in place (Mohammed, D., Mariani, R., & Mohammed, S. 2015).
3. Cybersecurity Requires Consistent Monitoring: A company must keep an eye on the security of all of its frameworks. Especially since programmers and cybercriminals are constantly devising new ways to infiltrate a company's organization (Mohammed, D., Mariani, R., & Mohammed, S. 2015).
4. Cybersecurity is not Temporary: Cybersecurity isn't something you can simply implement, set, and forget. It takes a long time to form and institute. It also necessitates continuous monitoring and updating of the security systems installed. To reap the benefits of network protection, you must keep it under your control (Mohammed, D., Mariani, R., & Mohammed, S. 2015).
5. Cybersecurity can be Extremely Dangerous for Businesses: Organizations are frequently concerned about implementing appropriate cybersecurity measures because it can make information less secure and can also prompt security breaches that can cost them a lot of money, notoriety, and, surprisingly, clients (Mohammed, D., Mariani, R., & Mohammed, S. 2015).

2.2. The relationship between accounting and cybersecurity

Network protection has turned into a vital practice for organizations across ventures, particularly the accounting business. As the pace of cyberattacks develops, Hackers realize that a weak framework that contains significant financial data can turn out to be an obvious objective.

Accounting cybersecurity rehearses guarantee that a firm ensures delicate information, for the consistency of a firm as well as for the wellbeing of customers who've endowed firms with their financial, individual, and expert data (Wang, T., K. N. Kannan, and J. R. Ulmer. 2013).

Methods and Precautionary Measures for a Successful Cybersecurity (Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. 2013):

1. *Encryption:* Encryption guarantees that information is shielded from external powers. Commonly, accounting firms centre around encryption for information that is on the way, like utilizing scrambled email frameworks. Nonetheless, information ought to likewise be scrambled while very still, put away in frameworks or on gadgets.
2. *Backups:* A firm wants to have the arrangement to back up information, working frameworks, and applications. This methodology is judicious in case of a cyberattack as well as assuming a catastrophic event were to remove admittance to actual areas or harmed servers. An excess reinforcement plan guarantees that information and data are put away in the cloud and backed up routinely. Virtualization takes into account reinforcements to be open in minutes on account of a cyber occurrence or another issue. Particularly during charge season, an accounting firm necessities a demonstrated backup plan if the information is compromised. Routinely planned Backups additionally guarantee that little data is lost on account of an event.
3. *Email Security:* Progressively, business is done over email. In any case, email is additionally the essential wellspring of phishing assaults, during which programmers send a false emails, frequently with a critical source of inspiration. At the point when an accidental user taps on a connection or appended record, they can release a cyberattack that inserts documents in gadgets and organizations that can be enacted sometime in the future to take scrapes or shut down frameworks.
4. *Access Controls:* A firm must be certain that they have a thorough and all-around arranged admittance of the executive's procedure. Just give admittance to frameworks and data to the individuals who totally should approach that data, in light of job, gathering, or occupation title. Also, to be certain that entrance rules incorporate what to do when somebody leaves the association, as well.

5. *Passwords and Authentication:* Accounting firms ought to have rigid password strategies set up. Expect representatives to change passwords consistently and require solid passwords that incorporate numbers, exceptional characters, and both upper and lowercase letters. Rules on length and intricacy are foremost. multifaceted authentication is additionally significant, requiring more than one method of authentication from a client before getting to frameworks, applications, sites, and messages.

2.3. Terminology

- Cybersecurity: Cybersecurity is frequently utilized as an undifferentiated term for information security. Notwithstanding, cybersecurity isn't just the security of cyberspace itself yet in addition to the insurance of the individuals who work in cyberspace and any of their resources that can be reached through cyberspace (von Solms and van Niekerk, 2013). Online protection includes technologies, cycles, and controls that are intended to secure frameworks, organizations and information from cyberattacks. Viable cybersecurity lessens the danger of cyberattacks and secures social orders, associations, and people from the unapproved abuse of frameworks, organizations, and advances. Cybersecurity is an umbrella idea that incorporates data security and data affirmation (Craigen, D., Diakun-Thibault, N., & Purse, R. 2014). In this manner, Cybersecurity includes the assurance of data that is surveyed and communicated through any PC organization (Carley, K. M., Cervone, G., Agarwal, N., & Liu, H. (2018).

- Sarbanes-Oxley Act (SOX): A federal law that set up clearing auditing and financial guidelines for public organizations. Administrators made the enactment to assist with securing investors, workers, and general society from accounting mistakes and false financial practices (Zhang, I. X. 2007).

- American Institute of Certified Public Accountants (AICPA): The national professional organization of Certified Public Accountants (CPAs) in the United States, later on, the AICPA went into a joint venture with their comparable in the UK, the Chartered Institute of Management Accountants (CIMA), an organization that delivered the Chartered Global Management Accountant (CGMA) assignment. Then, at that point, the AICPA and the CIMA co-made the Global Management Accounting Principles (GMAPs). The Association of International Certified Professional Accountants was dispatched in 2017 as a different joint endeavour between the AICPA and CIMA to consolidate both public and executive accounting. The AICPA and CIMA participation bodies remain and give all current advantages to members (Nagle, B. M., Menk, K. B., & Rau, S. E. 2018).

- Computerized Accounting Information System (CAIS): CAIS manages direct and indirect financial exercises that incorporate exchanges, information on the board, information handling, and a choice decision supportive network. The framework is embraced for its simple to-utilize easy to understand design, quick and exact

computing capacity, simple information stockpiling and recovering choices, and synopsis perspective on the framework. The system offers a choice decision-supportive network to mechanize business cycles and help direction. CAIS Implementation can start as a straightforward accounting framework and be ventured into a total endeavour asset arranging with office mechanization, merchant upheld frameworks, and surprisingly specific reason capacities. However, much CAIS offers various advantages, it isn't dependably totally protected from cyber threats. Since technology is open to everybody, individuals/bunches with the right abilities and wrong expectations can look for ways of infiltrating into the framework and take ordered data or even harm the framework. Bansah, E. A. (2018) showed that this sort of interruption can prompt an extreme loss of usefulness and financial resources. Al-Hashimy, H. N. H., & Yusof, N. A. (2021) in his exploration on saw cyber threats concerning CAIS referenced associations in Saudi Arabia and showed that the failure of CAIS to manage these dangers may even influence the security of the framework and its partners (Al-Hashimy, H. N. H., & Yusof, N. A. 2021).

2.4. Cybersecurity in Saudi Arabia

Saudi government perceives that they need to use the advantages presented by the internet and in this manner, they stress the take-up of web innovation to facilitate the improvement in the field of training, economy, medication, design, and business overall. It is apparent that the internet is indispensable for more productive government tasks and conveying quick and further developed administrations to mass individuals. Saudi Arabia made the internet accessible to over 70% of its populace. During the Jubail Cybersecurity conference, it was reported that KSA received over 60 million cyber assaults in 2015 alone. Additionally, Saudi Arabia faces 164,000 Cyber-Attacks/each day. The hackers who are related to these assaults, come from 120 distinct countries. Specialists are continually attempting to overhaul security, be that as it may, programmers are additionally adjusting, and they are changing their methodology consistently (GLANCE, C. R. A. A. 2017). It was referenced that worldwide the pace of accomplishment in cyberattacks is 18% and the cyber-attack percentage is generally 26%. The rest are managed by the security framework (Kasasbeh, F. I. O., & Thuneibat, N. S. M. 2018). To stay away from harm, KSA should act proactively and put resources into proactive measures rather than in responsive measures. The Ministry of Interior's National Cyber Security Center (NCSC) in Riyadh, Kaspersky Lab referenced that 60% of organizations in KSA have encountered cyber-attack over the time of most recent year (Alhashim, S. S., & Rahman, M. H. 2021).

3. Methodology

The used study in this paper is a study that’s prepared by Kasasbeh, F. I. O., & Thuneibat, N. S. M. (2018), in a paper titled International Review of Management

and Marketing The Ability of Computerized Accounting Information Systems in Saudi Public Universities to Face Cyber Threats. The study analyzes is to measure the ability of CAIS to confront cyber-attacks considering the recurrence and strength of the assault interceded by access control. The creator expects that some impact of those assaults on the framework's capacity is represented by the entrance control to the framework. The review targets gathering information relating to individuals' perspectives concerning the capacity of the colleges in Saudi Arabia to confront cyberattacks. The information was gathered from three colleges in KSA. The author decided not to unveil the names of the colleges or members to keep up with anonymity. The study applied an arbitrary inspecting procedure. The study was controlled through printed versions. 486 duplicates were gotten in kind with every one of the vital fields filled likewise. Out of 486 respondents, 463 were male and 23 were female. We had 52 first-year understudies, 107 fifth-year understudies, 171 teachers, 108 educators, and 48 staff addressing the review questions. The quantity of members from the three Universities is 178, 138, and 170. The survey remembered 5-point Likert scale inquiries for the likeliness of assaults from different vindictive projects, an accessible enemy of malware programs shielding the framework, access control to the record data framework, and the capacity of the framework to battle off those attacks.

Table 1: Comparison of measurement models.

Model	χ^2	df	$\Delta\chi^2$	Δdf	CFI	GFI	NFI	RMSEA	SRMR

Full measurement model (4 factors) 3767.855 3423			0.912	0.854	0.496	0.014	**0.045**
Model 1 3772.073 3425	−4.218	−2	0.911	0.854	0.495	0.014	**0.045**
(2 factors, combines "Attack" and "Access" into one factor) Model 2 3777.676 3425	−9.821	−2	0.910	0.854	0.494	0.015	**0.045**
(2 factors, combines "Attack" and "Ability" into one factor) Model 3 3776.693 3425	−8.838	−2	0.910	0.854	0.495	0.015	**0.045**
(2 factors, combines "Access" and "Ability" into one factor) Model 4 3773.356 3424	−5.501	−1	0.910	0.854	0.495	0.015	**0.045**
(2 factors, combines "Attack" and "Protection" into one factor) Model 5 3774.644 3425	−6.789	−2	0.910	0.854	0.495	0.015	**0.045**
(2 factors, combines "Access" and "Protection" into one factor) Model 6 3774.651 3425	−6.796	−2	0.910	0.854	0.495	0.015	**0.045**
(2 factors, combines "Ability" and "Protection" into one factor)							
Model 7 3777.286 3426	**−9.431**	**−3**	**0.910**	**0.854**	**0.495**	**0.015**	**0.045**

(one-factor model)

*n=486, *P<0.005, **P<0.001, $\chi^{2=}$Chi-square discrepancy, df=Degree of freedom, CFI: Comparative fit index, NFI: Normed fit index, RMSEA: Root mean square error of approximation. In all measurement models, error terms were free to covary one pair of items to improve fit and help reduce bias in the estimated parameter values (Reddy, 1992)*

Table 2 shows the mean score and standard deviations associated with each variable. The table shows that respondents tendto agree (mean score = 3.5) that attacks from malicious programsare a concern for the security of the computerized account informationsystem (CAIS) in Saudi universities. Respondents shared their concerns regarding the access control system (mean =1.3) and tend to disagree that the access control system is adequate. Respondents neither agree nor disagree on the (mean = 2.6) fact that computerized account information systems (CAIS) working in Saudi Arabian universities have adequate ability to face the cyber threat. Respondents also showed concerns regarding the performance of current anti-malware programs in defeating and containing the threats. Table 2 also illustrates the correlations between the factors extracted. It shows that access control is negatively correlated with an attack from a malicious program (−0.283**). Therefore, better access control is likely to reduce attacks (negative correlation). Better access control shows a better ability to face cyber threats (.238**). Greater ability is likely to reduce attacks (−0.143**). Anti-malware is likely to provide better access control and safeguard against intruders (0.162**).

Table 2: Means, SDs and correlations.

Variable	Mean± SD	1	2	3	4
Attack from Malicious programsAccess control	3.4630±0.59046 1.2984±0.14117	1 −0.283**	1		
The ability of CAIS to face cyber threats	2.6235±0.29825	−0.143**	0.238**	1	
Anti-Malware program	**2.7196±0.56482**	**−0.030**	**0.162****	**−0.055**	**1**

Four factors have been imputed for path analysis. The four factors have been entered into the structural model and regression lines have been added as per the hypothesized relationships. The interaction factor has been calculated using SPSS and added for moderation effect. After model building, the SEM model was run and the achieved model fitness values were compared to the suggested baseline values. As stated by Liang and Xue, (2009) and Abu- Musa (2006). Table 3 shows that all the model fit indices were met and therefore, the model has been considered a good fit.

Table 3: SEM model fit indices.

Df	2	-	-
χ^2/df	3.68	<5 “good fit,” >5 “poor fit”	**Good fit**
NFI	0.997	≥0.9	**Good fit**
RFI	0.983	≥0.9	**Good fit**
IF	0.998	≥0.9	**Good fit**
TITLE	0.988	≥0.9	**Good fit**
CFI	0.998	≥0.9	**Good fit**
GFI	0.994	≥0.9	**Good fit**
RMS	0.074	≤0.05 “close approximate fit,” >0.05 but<0.08 “marginal fit,” ≥0.10 “poor fit”	**Marginal fit**
***Model is a good fit [9-14]**			

Table 4 shows ifthere is any significant difference in participants’ perceptions across different demographic statuses regarding the ability of CAIS to facecyber-threat. One-way ANOVA analysis has been performed and the results have been summarized in the following Table 4. Table 4 illustrates that for all three of the demographic factors the P values (Sig.) are >0.05. This indicates that participants’ perception regarding the ability of CAIS to face cyber threats is not biased by their demographic status.

Table 4: Perception of the ability of CAIS to face cyber threats across different demographic conditions.

The ability of CAIS to face cyber threats Demographic	n	Mean±SD	F	Significance
Gender Male	463	2.6246±0.29769	0.143	**0.706**

Female **Role** **1st year**	23 52	2.6005±0.31531 2.6582±0.25685	0.927	**0.448**
students 5th year	107	2.5871±0.29547		
students **Lecturer**	171	2.6177±0.30620		
Professor	108	2.6301±0.29993		
Staff **University**	48	2.6725±0.31382		
1	178	2.6280±0.25960	1.920	**0.148**
2	138	2.5843±0.27451		
3	**170**	**2.6505±0.34870**		

4. Analysis

The used approach is Statistical Package for the Social Sciences (SPSS) version 20 along with AMOS 20 plugin for data analysis and model building. The data gathered has been coded numerically and entered into SPSS. The questionnaire consists of 85 questions on four factors and 3 questions on the demographic status of the respondents. The dependent variable "Ability of CAIS to face cyber threat" was extracted from 13 items, the independent variable "Attack from Malicious Programs" was extracted from 18 items, the mediator "Access Control" consists of 12 questionnaire items and the moderator "Anti-Malware Program" was extracted from 42 questionnaire items. As the researcher of the paper in hand agrees with the resulting analysis, with an emphasis on the necessity for economies on the individuals level, organizations level, and nations level, to invest heavily and quickly in technologies, to protect important data, as well as minimize the damage of cyber-attacks, or even to reach the extent of blocking such attacks completely.

5. Conclusion and Findings

The developing reliance of both public and private firms on IT and organizations for their financial administration frameworks expands their weakness to cyber threats. Furthermore, the economy has become more information based; in this manner, ensuring data resources has turned into a top plan thing for accountants and managers. Cybersecurity has in this manner expanded, becoming one of the main dangers the executive's challenges confronting each kind of association inside the space of only a couple of years. To stay away from cyber threats, each association should execute a cybersecurity program or a cybersecurity technique. This likewise applies to nations and wards, and thus, it was contended that it is fundamental for nations to distribute public cybersecurity methodologies. Besides, numerous countries as well as Saudi Arabia recognize the state offices responsible for setting the best expectations and reacting to cyber threats, to get the development in the kingdom, without placing any viewpoint in jeopardy.

Acknowledgment

The Author would like to thank the Arab Open University in the Kingdom of Saudi Arabia for supporting this study.

References

AICPA. (2018). Association of International Certified Professional Accountants. The CPA Advocate - Archived Articles 2018.

Alhashim, S. S. & Rahman, M. H. (2021). Cybersecurity threats in line with awareness in Saudi Arabia. In *2021 International Conference on Information Technology (ICIT)*, 314-319. IEEE.

Al-Hashimy, H. N. H. & Yusof, N. A. (2021). The relationship between the computerized accounting information system and the performance of contracting companies. *Materials Today: Proceedings.*

American Institute of Certified Public Accountants, AICPA. (2017). SOC for Cybersecurity: A Backgrounder. New York, NY: AICPA.

Bansah, E. A. (2018). The threats of using computerized accounting information systems in the banking industry. *Journal of Accounting and Management Information Systems.*

Carley, K. M., Cervone, G., Agarwal, N., & Liu, H. (2018). Social cyber-security. In International conference on social computing, behavioural-cultural modelling and prediction and behaviour representation in modelling and simulation, 389-394. Springer, Cham.

Clark, D., Berson, T., & Lin, H. S. (2014). At the nexus of cybersecurity and public policy: Some basic concepts and issues.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, 7(2), 189-208.

Drew, J. (2012). Managing cybersecurity risks. *Journal of Accountancy*, 214(2), 44.

GLANCE, C. R. A. A. (2017). Kingdom of Saudi Arabia.

Gordon, I. M., & Nazari, J. A. (2018). Review of SOX in the business ethics literature. *Managerial Auditing Journal*.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, 34(5).

Gordon, L. A. & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (Security)*, 5(4).

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*.

Halbach, H. (2021). How the growth of technology has forced accounting firms to put an emphasis on cybersecurity.

Halbach, H. (2021). How the growth of technology has forced accounting firms to put an emphasis on cybersecurity.

Karanja, E., & Zaveri, J. (2014). Ramifications of the Sarbanes Oxley (SOX) Act on IT governance. *International Journal of Accounting and Information Management*.

Kasasbeh, F. I. O., & Thuneibat, N. S. M. (2018). The ability of computerized accounting information systems in saudi public universities to face cyber threats. *International Review of Management and Marketing.*

Kim, N. Y., Robles, R. J., Cho, S. E., Lee, Y. S., & Kim, T. H. (2008, October). SOX act and IT security governance. In *2008 International Symposium on Ubiquitous Multimedia Computing*, 218-221. IEEE.

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity challenges and compliance issues within the US healthcare sector. *International Journal of Business and Social Research.*

Nagle, B. M., Menk, K. B., & Rau, S. E. (2018). Which accounting program characteristics contribute to CPA exam success? A study of institutional factors and graduate education. *Journal of Accounting Education*.

Pendley, J. A. (2018). Finance and accounting professionals and cybersecurity awareness. *Journal of Corporate Accounting & Finance*, 29(1).

Rue, R., Pfleeger, S. L., & Ortiz, D. (2007). A framework for classifying and comparing models of cyber security investment to support policy and decision-making. In WEIS.

Sarbanes, P. SOX (2002, July). Sarbanes-Oxley act of 2002. In The Public Company Accounting Reform and Investor Protection Act. Washington DC: US Congress, 55.

Seda, M., & Kramer, B. P. (2009). State of forensic accounting tracks at the university undergraduate/graduate levels and the related need to change the educational model used in the accounting curriculum. *Journal of Forensic Studies in Accounting & Business*, 1(1).

Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. *IOSR Journal of Computer Engineering*.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security.

Wang, T., K. N. Kannan, and J. R. Ulmer. (2013). The association between the disclosure and the realization of information security risk factors. Information Systems Research, 24(2), 201–218. DOI: https://doi.org/10.1287/isre. 1120.0437.

Wilamowski, G. C. (2017). Using analytical network processes to create authorization, authentication, and accounting cyber security metrics (Doctoral dissertation, The George Washington University).

Willemson, J. (2006). On the Gordon & Loeb model for information security investment. In WEIS.

Zadorozhnyi, Z. M., Muravskyi, V., & Muravskyi, V. (2021). Combined outsourcing of accounting and cybersecurity authorities. In *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*.

Zadorozhnyi, Z., Muravskyi, V., & Shevchuk, O. (2020). The accounting system is the basis for organising enterprise cybersecurity. *Financial and credit activity: problems of theory and practice.*

Zhang, I. X. (2007). Economic consequences of the Sarbanes–Oxley Act of 2002. *Journal of accounting and economics.*