Importance of Adding Cybersecurity to Accounting Curricula: An Applied Study on Saudi Universities

Norah Almutairi[1*] Husain Elnafabi[2]

1. Department of Accounting, College of Business and Economics, Qassim University, Buraydah, Saudi Arabia.
2. Department of Accounting, College of Business and Economics, Qassim University, Buraydah, Saudi Arabia.

* E-mail of the corresponding author: norahmusaad@gmail.com

Abstract

In the current technological era, it is necessary to complete the accounting curricula to keep pace with the developments of the profession. This study aimed to assess the extent to which the importance of adding cybersecurity to accounting curricula. A survey was provided to collect primary data from 122 participants who represented faculty members of the accounting departments at Saudi Arabia universities, and multiple statistical methods were used to analyse the data and find out the relationship between the variables in the study model. The findings show that it is important to add cybersecurity to accounting curricula. These results suggest that it is not clear to what extent accounting students are currently qualified to work with the basics of cybersecurity. The results also indicate that knowledge of cybersecurity increases the competitiveness of accounting graduates. The results presented the most difficulties facing the accounting departments to add the cybersecurity curriculum, such as the lack of references available for teaching cybersecurity in accounting curricula, some faculty members do not know the importance of cybersecurity in accounting, and it is difficult to provide qualified faculty to teach cybersecurity in accounting departments. As a result of these investigations, suggestions for future research were identified.

Keywords: Cybersecurity, Accounting Curricula, Accounting Students, Accounting Graduates.

DOI: 10.7176/RJFA/15-9-02

Publication date: October 30th 2024

1. Introduction

The world today is in the age of technology. The expansion in the use of technology increases cyber threats, which requires improving cybersecurity. Cybersecurity comprises technologies, processes, and controls that are designed to protect systems, networks, and data from cyber-attacks. Effective cybersecurity reduces the risk of cyber-attacks and protects societies, organizations, and individuals from the unauthorized exploitation of systems, networks, and technologies. Cybersecurity is an umbrella concept that encompasses information security and information assurance (No & Vasarhelyi, 2017). Cybersecurity is no longer a technical issue only, but has become an indispensable prerequisite for protecting financial institutions from cyber risks, and its absence represents a huge threat to the financial sector. As the number of cybersecurity incidents continues to increase and stakeholders are becoming increasingly concerned, companies are devoting considerable resources to their cybersecurity risk management efforts and related cybersecurity disclosures (Eaton et al., 2019). However, accountants should move beyond that level of factual knowledge and engage in proactive thinking about security issues in their organisations and, ultimately, translate this thinking into actions that can help thwart cybercriminals (Pendley, 2018).

The accounting profession realizes the importance of cybersecurity in many areas of the profession. From a regulatory perspective, the American Institute of CPAs (AICPA) has developed a cybersecurity risk management reporting framework. Using it, organisations can communicate pertinent information about their cybersecurity and risk management efforts and educate stakeholders about the systems, processes, and controls they have in place to detect, prevent, and respond to breaches (AICPA, 2018a). The framework is a key component of a new System and Organisation Controls (SOC) for Cybersecurity engagement, through which a CPA reports on an organisation's enterprise-wide cybersecurity risk management programme. This information can help senior management boards of directors, analysts, investors, and business partners gain a better understanding of organisations' efforts (AICPA, 2018b).

Cybersecurity has been characterized as “multidisciplinary” as it involves not just technical issues, but also important business concerns faced by all enterprises today (Yang & Wen, 2017). Indeed, practitioners in the field acknowledge that there is a need for cybersecurity degree programmes in different disciplines, including business (McGettrick et al., 2014). Business schools, with their departments in management, accounting, marketing, information systems, etc., are well suited to address the multidisciplinary nature of cybersecurity (Yang & Wen, 2017). Cybersecurity has become a managerial accounting and auditing matter, subject to cost-benefit analysis, internal control assessment, and disclosure policy considerations (Haapamäki & Sihvonen, 2019). With recent increases in cybersecurity interest, it is imperative to supplement the current accounting curriculum, equip accounting graduates with sufficient knowledge and skills to assess cybersecurity risk, and learn about controls to mitigate such risks (Roohani & Zheng, 2019).

The Association to Advance Collegiate Schools of Business (AACSB) focuses on continuous quality improvement in management and accounting education. The AACSB emphasized the importance of integrating privacy and security concerns into the accounting curriculum. In particular, the AACSB's revised accounting accreditation standard A5 released in 2018 indicates that AACSB accredited accounting degree programmes should include learning objectives to develop skills and knowledge related to the integration of information technology into accounting and business. This includes the ability of both faculty and students to adapt to emerging technologies as well as the mastery of current technology. Graduates should understand the capabilities of technology tools, along with their impact and the concomitant risks and opportunities (AACSB International, 2018).

The development of the Certified Public Accountant (CPA) exam is a substantial change in the accounting profession. One new discipline is Information Systems and Control (ISC), which is focused on technology and business controls. This discipline may have content focused on information technology and data governance, internal control testing, and information system security, including network security, software access, and endpoint security. The performance of SOC engagements is also likely to be covered in this section. (Coffey & Conrad, 2021). As the CPA Exam evolves, so too must the accounting curriculum. Many schools have already begun making the necessary transition to student future readiness. The AICPA and the National Association of State Boards of Accountancy (NASBA) released the CPA Evolution Model Curriculum. The goal was to aid faculty as they seek to transition their programmes to reflect the new core and disciplines. The CPA licensure model is promoted through the CPA Evolution initiative (AICPA & NASBA, 2021). The purpose of this study is to clarify several aspects of the importance of cybersecurity for accounting curricula.

2. Literature Review

2.1 Cybersecurity and Accounting

Recent years have witnessed academic interest in cybersecurity in accounting. In a comprehensive review of the literature on cybersecurity related to accounting and auditing over the period 2000-2018, Haapamäki and Sihvonen (2019) found that there is a phenomenal growth of cybersecurity-related studies in accounting and auditing since 2018. Cybersecurity has become increasingly important for accounting and public policy (Haapamäki & Sihvonen, 2019). These studies provide a broad definition of the areas to be considered. However, accounting faculty members need additional details to understand the skills required to be included in the accounting curriculum. There is a relationship between cybersecurity and several areas of accounting. Cybersecurity is not just related to risk management. It encompasses several areas in accounting such as management accounting, disclosure, audit, accounting information systems (AIS), and accounting behaviour (Janvrin & Wang, 2019). Cybersecurity incidents continue to increase, and accountants are uniquely positioned to help companies with these efforts in advisory and assurance capacities by presenting a model of effective cybersecurity risk management. The accountants' core competencies can add significant value in each of the model stages (Eaton et al., 2019). Through looks into the current and potential uses of blockchain technology in business, specifically in accounting. The blockchain should be effectively implemented in different aspects of cybersecurity and accounting, such as auditing and general accounting procedures (Demirkan et al., 2020).

2.2 Development of Accounting Education

There are expected changes in technology that will affect the accounting profession and consequently education will be affected and adjusted to these new technologies. It is important to highlight where enhancements can be made to curricula. Academic and professional educators generally expect that the predicted developments will occur in the future and that the progress in digitalization of accounting practice will have a profound impact on the accounting profession. Developing curricula are necessary to keep education and the profession aligned for future purposes and to incorporate the skills and knowledge needs of graduates as identified by the market (Al-Htaybat et al., 2018). Students' learning needs are to prepare them for workplaces characterized by rapidly changing requirements in information and communication technology (ICT) (Daff, 2021). The new technologies in accounting impact the skills required for graduate and early career accounting professionals. There is an important, complementary, and yet slightly different role played by stakeholders (universities/employed organisations/professional associations) in building technology-related skills to help collectively nurture early career accountant talent (Jackson et al., 2022). Information technology and software are an important need in the accounting job market, along with technical accounting knowledge and personal and interpersonal skills. Accounting curricula should adapt to evolving job market needs. Komarev and Preobragenskaya (2022) propose a comprehensive framework of competencies demanded by employers in the Gulf Cooperation Council (GCC) region to be integrated into the local accounting curricula. The proposed framework highlights a different priority of competencies to be developed by undergraduate and graduate-level accounting programmes. Universities can use the methodology described and the proposed competence framework to help evolve their accounting curricula according to market needs.

2.3 Cybersecurity in Accounting Curricula

Henderson et al. (2016) makes a pedagogical case for demonstrating how a prevalent cybersecurity threat, SQL Injection (SQLi), operates. The accounting students first answer background questions on SQLi and then simulate SQLi in both a Microsoft Access and web-based environment. Accounting students need to understand how these threats operate; especially accounting students interested in career opportunities in Information Technology (IT) Auditing. This knowledge can help these students develop a deeper understanding of the risks associated with cybersecurity threats, as well as the countermeasures to mitigate these threats. Yang and Wen (2017) suggest a descriptive cybersecurity curriculum model, which can also serve as a baseline for future studies on business-school cybersecurity programmes. The methodology used and the resulting descriptive model can help integrate a cybersecurity curriculum with other traditional business disciplines. Yang (2019) suggests a new graduate-level cybersecurity curriculum model for business. Al-Maharfi (2019) suggests a curriculum for Accounting Information systems (AIS) course contents for undergraduate accounting programmes through a comparison of the academic environment and the needs of the professional market. One of the categories on which academics and professionals agreed was the security and auditing of accounting information systems. Yang (2021) proposes a meta-model of cybersecurity curriculum: Assessing cybersecurity curricular frameworks for business schools, which can help curriculum designers customize their cybersecurity programmes based on their priorities and resources, faces the challenge of deciding which curriculum frameworks to utilize and which topics and areas to emphasize when developing cybersecurity curriculums in higher education institutions. Boss et al. (2022) provided six short, open-ended cases that highlight the growing need to incorporate cybersecurity into the accounting curriculum. One or more of the cases can be used in introductory, core, and/or advanced accounting classes to emphasize the importance of cybersecurity for accounting students. The cases can be worked as individual assignments or in student groups. These cases address cybersecurity disclosure issues in financial reporting, the impact of a cybersecurity breach in financial audits, the risks to tax preparers of storing personally identifiable information, calculating and evaluating the costs of cybersecurity breaches, and examining cybersecurity disclosures in 10-Ks. Cybersecurity concepts should be introduced at all levels of accounting curricula, and not only in accounting information systems courses (Boss et al., 2022).

Overall, these studies agree with the current study about the importance of adding cybersecurity in business colleges, especially in the accounting curricula. To date, there is a general lack of studies describing how to add cybersecurity to accounting curricula. The study sought to answer the following specific research questions:

(1) How important is adding cybersecurity to accounting curricula in Saudi universities? (2) To what extent are accounting students qualified in the basics of cybersecurity for the current business environment? (3) Does a knowledge of the basics of cybersecurity increase the competitiveness of accounting graduates? (4) Is there an effect of students' qualifications and graduates' competitiveness on adding cybersecurity to accounting curricula? (5) What are the difficulties of adding cybersecurity to accounting curricula?

3. Research Design

3.1 Data Collection

The questionnaire was adopted for collecting primary data related to the problem of the study. A questionnaire was designed consisting of five parts: The first part included demographic data designed to find out the academic data and find out whether the participant had cybersecurity knowledge. The other parts contain four axes that measure the main variables of the study. The first axis is the importance of adding cybersecurity to the accounting curricula. The second axis is the extent to which accounting students are qualified to work within the basics of cybersecurity. The third axis is the competitiveness of accounting graduates in the market. The fourth axis is the difficulties of adding cybersecurity to accounting curricula. The questionnaire was sent by email to all members of the accounting faculty whose email addresses are published on the official websites of universities and colleges in the period from the beginning of December 2021 until the end of January 2022; 125 responses were obtained; three responses were excluded because they were not valid for analysis.

3,2 Population and Sample

The list of public universities and the list of private universities and colleges published on the Ministry of Education website until 2021 were taken. thus, searched in all universities and colleges to determine which universities and colleges provide the accounting programme at the undergraduate level, to cover all accounting departments in Saudi universities and colleges. Table 1 shows the number of universities and colleges that provide accounting programmes in Saudi Arabia. There are 44 Saudi public and private universities and colleges that provide accounting programmes for the undergraduate level. The study sample is a random sample from the faculty members in accounting departments in Saudi universities and colleges.

Table 1. The Number of Universities and Colleges That Provide Accounting Programmes at The Undergraduate Level in Saudi Arabia.

Type	**Number of universities and colleges**
Public universities and colleges	28
private universities and colleges	16
Total	44

4. **Results and Discussion**

4,1 Validity and reliability of the questionnaire

To calculate the validity of internal consistency, Pearson's correlation coefficient was used between each item in the questionnaire and the total degree of the domain to which they belong.

Table 2. Pearson Correlation Coefficients Between Each Statement and The Total Degree of Measure.

Domain	Items	Pearson correlation coefficient	P-value (Sig.)	Pearson correlation coefficient	P-value (Sig.)
Importance of Adding Cybersecurity to Accounting Curricula	1	0.782**	0.000	0.654**	0.000
	2	0.784**	0.000		
	3	0.761**	0.000		
	4	0.774**	0.000		
	5	0.629**	0.000		
Qualification of Students	1	0.742**	0.000	0.811**	0.000
	2	0.857**	0.000		
	3	0.941**	0.000		
	4	0.888**	0.000		
	5	0.926**	0.000		
Competitiveness of Graduates	1	0.712**	0.000	0.753**	0.000
	2	0.852**	0.000		
	3	0.886**	0.000		
	4	0.869**	0.000		
Difficulties	1	0.787**	0.000	0.753**	0.000
	2	0.701**	0.000		
	3	0.647**	0.000		
	4	0.778**	0.000		
	5	0.794**	0.000		
	6	0.562**	0.000		
	7	0.804**	0.000		
	8	0.797**	0.000		

Note: (**) means the statistically significant correlation at (0.01)or less.

The results, as shown in Table 2, indicate that all p values equal to (0.000) are

less than the level of significance (0.05), so there is a statistically significant relationship between each element and the total degree of the domain, and there is a statistically significant relationship between each domain and the total degree of measure.

Table 3. Reliability Coefficients Cronbach's Alpha.

Domain	Items	Coefficients Cronbach's alpha
Importance of Adding Cybersecurity to Accounting Curricula	5	0.770
Qualification of Students	5	0.921
Competitiveness of Graduates	4	0.835
Difficulties	8	0.879
Overall Reliability Coefficients	22	0.875

To calculate the reliability, Cronbach's alpha coefficients were used. From Table 3, the overall reliability coefficients are (0.875), suggesting very good internal consistency reliability for the scale with this sample. Values above 0.7 are considered acceptable; however, values above 0.8 are preferable (Pallant, 2020). This indicates that the tool is characterized by great stability, which achieves the purpose of the study.

4.2 Descriptive statistics

4,2,1 Demographic Characteristics

The demographic data was divided into two parts; the first part is about the academic data of the respondents (type of university, university name, academic degree, and years of experience), and the second part is about the knowledge of cybersecurity of the respondents (how familiar with cybersecurity topics and practical experience in cybersecurity).

Table 4. Demographic Information (Academic Data).

Academic data			
Variable	Answer	Frequency	Percentage
Type of University	Public University	110	90.2%
	Private University	12	9.8%
	Total	122	100.0%
Academic degree	Professor	14	11.5%
	Associate Professor	8	6.6%
	Assistant Professor	44	36.1%
	Lecturer	36	29.5%
	Teaching Assistant	20	16.4%
	Total	122	100.0%
Number of years of academic experience	5 years or less	40	32.8%
	6 to 10 years	34	27.9%
	11 to 15 years	25	20.5%
	16 to 20 years	4	3.3%
	More than 20 years	19	15.6%
	Total	122	100.0%

As shown in Table 4. The public universities had the highest percentage of respondents with 90.2% of the sample size, while the respondents from private universities were 9.8% of the sample size.

The Assistant Professor category had the highest percentage of respondents with 36.1% of the sample size. The second-largest category was the Lecturer with a percentage of 29.5% of the sample size, and the Professor category represented 11.5% of the sample size.

Table 4 shows that 32.8% of the respondents had 5 years or less of experience, 27.9% had 6 to less than 10 years of experience. 20.5% of the respondents had 11 to 15 years of experience, and 3.3% had 16 to 20 years of experience, while 15.6% of the respondents had more than 20 years of experience. That means that 61% of the respondents had 10 years or less of experience, and 39% of the respondents had 10 years or more of experience.

Table 5. The Universities Name

Answer	Frequency	Percentage
University of Prince Mugrin	2	1.6%
Prince Sultan University	3	2.5%
Umm Al-Qura University	11	9.0%
Imam Muhammad bin Saud Islamic University	13	10.7%
Jouf University	11	9.0%
Prince Sattam bin Abdulaziz University	3	2.5%
Qassim University	10	8.2%
Jazan University	4	3.3%
Najran University	1	0.8%
Saudi Electronic University	1	0.8%
Shaqra University	1	0.8%
University of Bisha	3	2.5%
Imam Abdulrahman bin Faisal University	8	6.6%
King Saud University	8	6.6%
Taibah University	5	4.1%
King Faisal University	2	1.6%
Yanbu University College	1	0.8%
Dar Al Uloom University	1	0.8%
King Abdulaziz University	5	4.1%
Gulf Colleges	2	1.6%
King Fahd University of Petroleum and Minerals	1	0.8%
Taif University	3	2.5%
Princess Nourah Bint Abdul Rahman University	4	3.3%
Majmaah University	2	1.6%
University of Hafr Al Batin	1	0.8%
King Khalid University	3	2.5%
Prince Sultan College of Business	1	0.8%
Northern Border University	2	1.6%
University of Ha'il	3	2.5%
University of Business and Technology	1	0.8%
University of Tabuk	3	2.5%
Onaizah Colleges	2	1.6%
University of Jeddah	1	0.8%
Total	122	100.0%

As can be seen from the data in Table 5, the highest percentage of respondents was from Imam Muhammad bin Saud Islamic University with 10.7%, and the second highest percentage of respondents was from Umm Al-Qura University and Jouf University with 9.0% each, then 8.2% of the respondents from Qassim University. The fourth highest percentage of respondents was for Imam Abdulrahman bin Faisal University and King Saud University, with 6.6% for each.

Table 6. Demographic Information (knowledge of Cybersecurity).

Knowledge of Cybersecurity			
Variable	Answer	Frequency	Percentage
How familiar are you with cybersecurity topics? (More than one choice can be selected)	Attending educational lectures on cybersecurity topics	53	43.4%
	Attending conferences and seminars on cybersecurity topics	17	13.9%
	Attending specialized courses for cybersecurity training	9	7.4%
	Other	16	13.1%
	I don't have any of the above to learn about cybersecurity	45	36.9%
Do you have practical experience in cybersecurity?	Yes	15	12.3%
	No	107	87.7%
	Total	122	100.0%

The upper half of Table 6 shows that 43.4% of the respondents attended educational lectures on cybersecurity topics, 13.9% attended conferences and seminars, and 13.1% have a piece of knowledge from other sources. What is interesting about the data in this table is that there 7.4% of the respondents attended specialized courses for cybersecurity training, while 36.9% do not have any knowledge about cybersecurity topics.

The bottom half of Table 6 shows that 87.7% of the respondents didn't have a practical experience in cybersecurity, and what stands out in the table, there is that 12.3% of the respondents had a practical experience in cybersecurity.

4.2.2 Data Analysis and Test Study Hypotheses

Results and Discussion Related to First Hypothesis

H1: It is important to add cybersecurity to accounting curricula.

The first axis of the questionnaire was designed to assess the extent to which the importance of adding cybersecurity to accounting curricula. Five items on the questionnaire measured the extent to which the importance of adding cybersecurity to accounting curricula. Table 7 shows the means and standard deviations of the responses of the study sample.

Table 7. Descriptive Statistics for Each Item in Domain (Importance of Adding Cybersecurity in Accounting Curricula).

No.	Item	Mean	Standard deviation	Ranking	Interpretation
1	Cybersecurity is considered one of the core competencies of this time.	4.48	0.61	1	Strongly agree
3	Cybersecurity is importantly linked to several areas of accounting, such as accounting information systems, management accounting, internal auditing, risk management, and disclosure.	4.40	0.71	2	Strongly agree
2	Cybersecurity is multidisciplinary, which makes it of great importance for every technology-affected discipline in business, and it is necessary to follow developments in it.	4.39	0.66	3	Strongly agree
4	Cybersecurity topics must be included in accounting curricula in Saudi universities.	4.23	0.85	4	Strongly agree
5	The university where I work understands how much change in curricula is required to respond to the growing interest in cybersecurity in Saudi Arabia.	3.83	1.03	5	Agree
	Overall mean	4.27	0.77		Strongly Agree

As can be seen from the table above, the overall mean of the domain Importance of Adding Cybersecurity to the Accounting Curricula was (4.27), the standard deviation was (0.77), and the study sample responded strongly agree in this domain. The most important statement of the first hypothesis statements is (Cybersecurity is considered one of the core competencies of this time) with a mean of 4.48 and a standard deviation of 0.61, while the statement (The university where I work understands how much change in curricula is required to respond to the growing interest in cybersecurity in Saudi Arabia) ranked last with a mean (3.83) and a standard deviation (1.03). Concerning the first study question, it was found that the faculty members of the accounting departments in the universities of Saudi Arabia agree that it is important to add the cybersecurity curriculum to the accounting departments.

It is apparent from Table 8 that very few accounting departments teach cybersecurity topics in their current accounting curricula. From the above data, it can be seen that the curricula in which cybersecurity topics have been added (Accounting Information Systems, Internal Audit, Business Intelligent Course, Forensic Accounting and Cybersecurity, Computerized Accounting App.) are as follows: about 95.1% of accounting departments didn’t teach any cybersecurity topics, 36.1% of respondents expect it to be taught in Accounting Information Systems curriculum, and 25.4% of respondents expect it to be taught as a new independent curriculum. Although 10.7% of the respondents expect their accounting department to not teach cybersecurity topics. 29.5% of the respondents expect cybersecurity topics to be taught in accounting departments by 2025 or later.

Table 8. Where and When the Cybersecurity Topics Should Be added to Accounting Departments.

Variable	Answer	Frequency	Percentage
Are cybersecurity topics taught in current accounting curricula at your university?	Yes	6	4.9%
	No	116	95.1%
	Total	122	100.0%
If yes, what curriculum have cybersecurity topics been added to?	Business Intelligent Course	1	16.7%
	Forensic Accounting and Cybersecurity	1	16.7%
	Accounting Information Systems and the Course of Internal Auditing	1	16.7%
	ACC381 Accounting Information Systems	1	16.7%
	Computerized Accounting App.	1	16.7%
	Internal Auditing and oversight of Information Security	1	16.7%
	Total	6	100.0%
If your university does not teach any of the cybersecurity topics in the accounting curriculum, in which accounting curriculum do you expect the cybersecurity topics to be taught?	New independent curriculum	31	25.4%
	Internal audit curriculum	7	5.7%
	Management accounting curriculum	1	.8%
	Accounting information systems curriculum	44	36.1%
	The curriculum of computer applications in accounting	14	11.5%
	Elective curriculum offered by other disciplines	12	9.8%
	I don't think my university will teach cybersecurity topics in the accounting curricula	13	10.7%
	Total	122	100.0%
If accounting curricula at your university do not currently include coverage of cybersecurity topics, in which academic year do you think most Saudi universities include it in accounting curricula?	2022-2023	18	14.8%
	2023-2024	35	28.7%
	2024-2025	29	23.8%
	2025 or later	36	29.5%
	I don’t think most Saudi universities will teach cybersecurity topics in accounting curricula	4	3.3%
	Total	122	100.0%

Results and Discussion Related to the Second Hypothesis

H2: There is a relationship between the qualification of current accounting students and the importance of adding cybersecurity in accounting curricula.

The second axis of the questionnaire aimed to know what extent are accounting students qualified in the basics of cybersecurity for the current business environment. Five items on the questionnaire measured the extent to which accounting students are qualified to work within the basics of cybersecurity. Table 9 shows the means and standard deviations of the answers of the study sample.

Table 9. Descriptive Statistics for Each Item in Domain (Qualification of Students).

No	Item	Mean	Standard deviation	Ranking	Interpretation
1	Current curricula allow the accounting student to work on technology-based accounting activities in a business environment.	3.52	1.15	1	Agree
2	The current curricula provide sufficient knowledge for the accounting student to maintain the confidentiality, integrity, and availability of electronic accounting data and information.	3.46	1.04	2	Agree
4	The current curricula provide sufficient knowledge for the accounting student in identifying cyber risks and threats and setting appropriate controls for them.	2.93	1.26	3	Neutral
3	The current curricula provide sufficient knowledge for the accounting student to prevent or reduce cyberattacks on accounting programmes and data and deal with them if they occur.	2.92	1.30	4	Neutral
5	The current curricula provide sufficient knowledge for the accounting student in cryptography and its uses and keep abreast of renewed cryptography in the information technology environment and accounting information systems.	2.75	1.30	5	Neutral
	Overall mean	3.12	1.06		Neutral

As can be seen from the table above, the overall mean of the domain qualification of students was (3.12) and the standard deviation was (1.06), this means that the study sample responded to neutral in this domain. The most important statement of the second hypothesis statement is (The current curricula qualify the accounting student to work on technology-based accounting activities in a business environment) with a mean (3.52) and standard deviation (1.15), and the statement (The current curricula provide sufficient knowledge for the accounting student in cryptography and its uses and keep abreast of renewed cryptography in the information technology environment and accounting information systems) ranked last with a mean (2.75) and standard deviation (1.30). Regarding the second study question, it was found that faculty members of accounting departments at universities in Saudi Arabia do not have specific opinions about the degree to which students are qualified to work within the basics of cybersecurity. Faculty members expect that students are sufficiently qualified to deal with technology in accounting and that they have been qualified to maintain the confidentiality, integrity, and availability of electronic accounting data, but without dealing with cyber risks. This is an important issue for future research.

Results and Discussion Related to the Third Hypothesis

H3: There is a relationship between the competitiveness of accounting graduates and the importance of adding cybersecurity to accounting curricula.

The third axis of the questionnaire aimed to know, to what extent the knowledge of the basics of cybersecurity increases the competitiveness of accounting graduates. Four items of the questionnaire measured whether cybersecurity knowledge increases the competitiveness of accounting graduates. Table 10 shows the means and standard deviations of the responses of the study sample.

Table 10. Descriptive Statistics for Each Item in The Domain (Competitiveness of Graduates).

No	Item	Mean	Standard deviation	Ranking	Interpretation
3	Reliance on those who have basic cybersecurity skills saves information and financial resources from loss in the event of cyber-attacks or any potential security threat.	4.07	0.83	1	Agree
4	Reliance on those who have basic cyber security leads to greater efficiency and quality of performance when identifying and evaluating risks and setting appropriate controls or for any other control purpose.	4.07	0.79	2	Agree
2	An accounting graduate has the advantage of obtaining or retaining a position in the labour market if he or she has a basic knowledge of cybersecurity.	3.81	0.99	3	Agree
1	Accounting graduates currently have the competencies and skills to deal with technology that increase their competitiveness in the labour market.	3.43	1.04	4	Agree
	Overall mean	3.85	0.91		Agree

As can be seen from the table above, the overall mean in the domain Competitiveness of graduates was (3.85) and the standard deviation was (0.91), which means the study sample responded Agree in this domain. The most important statement of the third hypothesis statements is (Reliance on those who have basic cybersecurity skills saves information and financial resources from loss in the event of cyber-attacks or any potential security threat) with a mean (4.07) and standard deviation (0.83), and the statement (Accounting graduates currently have competencies and skills to deal with technology that increase their competitiveness in the labour market) ranked last with a mean (3.43) and standard deviation (1.04). Concerning the third study question, it was found that the faculty members in accounting departments at universities in Saudi Arabia see that knowledge of the basics of cybersecurity increases the competitiveness of accounting graduates.

Tests of Normality

Table 11. Tests of Normality Using Kolmogorov-Smirnova.

Domain	Statistics	df	sig.
Importance of Adding Cybersecurity to Accounting Curricula	0.065	122	0.200
Qualification of Students	0.074	122	0.124
Competitiveness of Graduates	0.083	122	0.080
Difficulties	0.081	122	0.075

As can be seen in Table (11) above, all variables are greater than the significance level (0.05). That means all variables follow a normal distribution.

Table 12. Correlation Matrix Using Pearson Correlation Coefficients for The Relationship Between Every Two Domains.

		Importance of Adding Cybersecurity to Accounting Curricula	Qualification of Students	Competitiveness of Graduates
Importance of Adding Cybersecurity to Accounting Curricula	Correlation	1.000		
	P-value			
Qualification of Students	Correlation	0.371**	1.000	
	P-value	0.001		
Competitiveness of Graduates	Correlation	0.456**	0.461**	1.000
	P-value	0.000	0.000	

(**) There is a statistically positive relationship at the level of significance (0.05) or less.

The results of the correlational analysis are presented in Table 12. There is a positive relationship at the level of significance (0.05) or less between (Importance of Adding Cybersecurity to Accounting Curricula) and (Qualification of students, Competitiveness of graduates). Furthermore, there is a positive relationship at the level of significance (0.05) or less between the qualification of the students and the competitiveness of the graduates.

Results and Discussion Related to the Fourth Hypothesis

H4: There is an effect from the qualification of accounting students and the competitiveness of graduates on the importance of adding cybersecurity to accounting curricula.

Table 13. Multiple Regression Model to Measure the Influence of Independent Variables on The Dependent Variable.

Dependent Variable	Importance of Adding Cybersecurity to Accounting Curricula							
	Unstandardized Coefficients		Standardized Coefficients	T-value	P-value	Collinearity Statistics		Note
Independent Variable	B	Std. Error	Beta			Tolerance	VIF	
(Constant)	3.09	0.29		10.65**	0.00			-
Qualification of Students	0.05	0.02	0.10	2.50*	0.02	0.75	1.33	Positive influence
Competitiveness of Graduates	0.32	0.07	0.43	4.66**	0.00	0.78	1.28	Positive influence
	R			0.570				
	R Square			0.325				
	Adjusted R Square			0.324				
	F-Value			11.156**				
	P-value			0.000				
	Durbin-Watson			1.839				

(**) There is a statistically significant influence at the level of significance (0.01) or less.

(*) There is a statistically significant influence at the level of significance (0.05) or less.

Range of critical values of Durban Watson (1.774 – 2.226).

If it is a value of VIF less than 10, it will be acceptable.

Regarding the fourth study question, it is apparent from Table 13 that there is a positive influence at the level of significance (0.05) or less from the qualification of accounting students and their competitiveness on the importance of adding cybersecurity to accounting curricula.

The Study Model

The study model examines the factors affecting the importance of adding cybersecurity to accounting curricula. This model tests the second, third, and fourth hypotheses.

〖y=β〗_0+β_X1+β_(X2)+ ∝

where Y is the dependent variable, which represents the importance of adding cybersecurity in accounting curricula, x1 which represents the current qualification of accounting students, and x2 which represents the competitiveness of accounting graduates are the two independent variables, a is the intercept, and b1 and b2 are the regression coefficients for the two independent variables. The regression coefficient gives you the change in the dependent variable for each unit change in that independent variable, with the effect of any of the independent variables controlled (referred to as partially out).

Importance of Adding Cybersecurity to Accounting Curricula =

β_0+β_(Qualification of students)+β_(Competitiveness of graduates)+ ∝ =

3.09+0.05*Qualification of students+0.32*Competitiveness of graduates

Results and Discussion Related to the Fifth Hypothesis

H5: There are difficulties that accounting departments face when adding cybersecurity to accounting curricula.

The fourth axis of the questionnaire aimed to determine the greatest difficulties in adding cybersecurity to accounting curricula. Eight items on the questionnaire measured the most difficulties facing the accounting department in adding cybersecurity to accounting curricula. Table 14 shows the means and standard deviations of the responses of the study sample.

Table 14. Descriptive Statistics for Each Item in The Domain (Difficulties).

No	Item	Mean	Standard deviation	Ranking	Interpretation
3	There are few references available for teaching cybersecurity in accounting curricula.	4.00	0.91	1	Agree
6	Some faculty members do not know the importance of cybersecurity in accounting curricula.	3.70	0.99	2	Agree
4	It is difficult to provide qualified faculty to teach cybersecurity in accounting departments.	3.51	1.12	3	Agree
1	There is difficulty in identifying curricula related to teaching cybersecurity topics.	3.39	1.03	4	Neutral
7	The difficulty of determining the appropriate start time for students to teach cybersecurity topics.	3.35	1.11	5	Neutral
8	It is difficult for accounting departments to provide adequate resources and support to teach cyber security within their curricula.	3.34	1.08	6	Neutral
2	It is difficult to develop the content of the current accounting courses syllabuses to introduce cybersecurity topics.	3.18	1.14	7	Neutral
5	It is difficult to train current faculty members assigned to teach cybersecurity in accounting curricula.	3.01	1.18	8	Neutral
	Overall mean	3.44	1.07		Agree

As can be seen from the table above, the overall mean in the domain difficulties was (3.44), and the standard deviation (1.07), which means the study sample responded agree in this domain. The most important statement of the fourth hypothesis statement is (There are few references available for teaching cybersecurity in accounting curricula) with a mean (4.00) and standard deviation (0.91), and the statement (It is difficult to train current faculty members assigned to teach cybersecurity in accounting curricula) ranked last with a mean (3.01) and standard deviation (1.18). Concerning the fifth study question, it was found that the most difficulties are the lack of references available to teach cybersecurity in accounting curricula, some faculty members do not know the importance of cybersecurity, and it is difficult to provide qualified faculty to teach cybersecurity in accounting departments.

T-test

The independent T test was carried out to compare the mean scores of the responses of the study sample according to (type of university and practical experience in cybersecurity).

Table 15. Results of Independent Sample T-Test to Significant Differences Between the Mean of The Responses of The Study Sample According to (Type of University, Do You Have Practical Experience in Cybersecurity?).

Variable	**Domain**	**Category**	**N**	**Mean**	**Std. Deviation**	**T-Test**	**DF**	**P-value**
Type of University	Importance of Adding Cybersecurity to Accounting Curricula	Public University	110	4.25	0.58	-1.28	120	0.20
		Private University	12	4.47	0.38			
	Qualification of Students	Public University	110	3.11	1.06	-0.24	120	0.81
		Private University	12	3.18	1.05			
	Competitiveness of Graduates	Public University	110	3.82	0.76	-1.17	120	0.24
		Private University	12	4.08	0.62			
	Difficulties	Public University	110	3.43	0.80	-0.39	120	0.69
		Private University	12	3.52	0.71			
Do you have practical experience in cybersecurity?	Importance of Adding Cybersecurity to Accounting Curricula	Yes	15	4.57	0.45	2.26*	120	0.03
		No	107	4.22	0.57			
	Qualification of Students	Yes	15	4.01	0.87	3.69**	120	0.00
		No	107	2.99	1.02			
	Competitiveness of Graduates	Yes	15	4.18	0.92	2.03*	120	0.04
		No	107	3.79	0.72			
	Difficulties	Yes	15	3.58	0.86	0.77	120	0.44
		No	107	3.41	0.78			

As can be seen from Table 15, There are no statistically significant differences at the level of significance (0.05) or less between the responses of the study sample in all domains according to (Type of University). There are statistically significant differences at the level of significance (0.05) or less between (Importance of Adding Cybersecurity in Accounting Curricula, Qualification of students, Competitiveness of graduates) according to (Do you have practical experience in cybersecurity?), and these differences are in favor of study sample having practical experience in cybersecurity. There are no statistically significant differences at the level of significance

(0.05) or less between (difficulties) according to (Do you have practical experience in cybersecurity?).

ANOVA test

The ANOVA test was used to determine the significant differences between the mean responses of the study sample according to (academic degree and number of years of academic experience).

Table 16. Results of One Way ANOVA with Significant Differences Between the Mean of The Responses of The Study Sample According To (Academic Degree, Number of Years of Academic Experience).

Variable	**Domain**	**Sources of variation**	**Sum of Squares**	**Df**	**Mean Square**	**F**	**P-value**
Academic Degree	Importance of Adding Cybersecurity to Accounting Curricula	Between Groups	1.30	4	0.33	1.00	0.41
		Within Groups	37.87	117	0.32		
		Total	39.17	121			
	Qualification of Students	Between Groups	13.94	4	3.49	3.36**	0.01
		Within Groups	121.33	117	1.04		
		Total	135.27	121			
	Competitiveness of Graduates	Between Groups	2.75	4	0.69	1.22	0.30
		Within Groups	65.77	117	0.56		
		Total	68.53	121			
	Difficulties	Between Groups	8.04	4	2.01	3.50**	0.01
		Within Groups	67.19	117	0.57		
		Total	75.23	121			
Number of years of academic experience	Importance of Adding Cybersecurity to Accounting Curricula	Between Groups	2.54	4	0.63	2.03	0.10
		Within Groups	36.63	117	0.31		
		Total	39.17	121			
	Qualification of Students	Between Groups	5.38	4	1.35	1.21	0.31
		Within Groups	129.89	117	1.11		
		Total	135.27	121			
	Competitiveness of Graduates	Between Groups	0.88	4	0.22	0.38	0.82
		Within Groups	67.65	117	0.58		
		Total	68.53	121			
	Difficulties	Between Groups	3.44	4	0.86	1.40	0.24
		Within Groups	71.78	117	0.61		
		Total	75.23	121			

It can be seen from the data in Table 16 that there are no statistically significant differences at the level of significance (0.05) or less between (Importance of Adding Cybersecurity in Accounting Curricula, Competitiveness of graduates) according to Academic degree. There are statistically significant differences at the level of significance (0.05) or less between (Qualification of students, Difficulties) according to academic degree. There are no statistically significant differences at the level of significance (0.05) or less between the responses of the study sample in all domains according to (Number of years of academic experience).

Table 17. Results of Scheffe test for significant differences in (Academic Degree).

Domain	Academic Degree	Mean	Professor	Associate Professor	Assistant Professor	Lecturer	Teaching Assistant
Qualification of Students	Professor	3.59	-				
	Associate Professor	3.65		-			
	Assistant Professor	3.22			-		
	Lecturer	2.64	**	**	*	-	
	Teaching Assistant	3.19					-
Difficulties	Professor	3.56	-				
	Associate Professor	3.95		-			
	Assistant Professor	3.26		**	-		
	Lecturer	3.26		**		-	
	Teaching Assistant	3.84					-

As can be seen from Table 17 there are statistically significant differences at the level of significance (0.05) or less in the Qualification of students between Lecturer and other academic degrees, and these differences are in favor of the other academic degree. There are statistically significant differences at the level of significance (0.05) or less in difficulties between the Associate Professor and (Assistant Professor, Lecturer), and these differences are in favor of the Associate Professor.

5. Conclusion

This study set out to assess the extent to which importance of adding cybersecurity to accounting curricula. The purpose of the study was to determine whether accounting students are qualified to work within the basics of cybersecurity in the current business environment and to determine whether cybersecurity knowledge increases the competitiveness of accounting graduates. This study has examined the relationship between the variables. Then assess the effects of qualification of accounting students and the effect of competitiveness of accounting graduates on the importance of cybersecurity in accounting curricula. The study currently identified the most difficulties facing the accounting departments in adding cybersecurity to accounting curricula. The most obvious finding that emerges from this study is that it is important to add cybersecurity to accounting curricula. An interesting finding is that there are a few accounting departments that have already started teaching cybersecurity topics in current accounting curricula. This study found that it is more appropriate to add cybersecurity topics to the Accounting Information Systems curriculum. This study has shown that there are no specific results about the extent to which students are qualified to work within the basics of cybersecurity in the current business environment. Accounting faculty members expect that students are sufficiently qualified to deal with technology in accounting without dealing with cyber risks. This is an important issue for future research. The results of this study indicate that knowledge of the basics of cybersecurity increases the competitiveness of accounting graduates. Multiple regression analysis revealed that There is a positive influence from the qualification of accounting students and their competitive ability on the importance of adding cybersecurity in accounting curricula. This study has identified the most difficulties facing the accounting departments in adding cybersecurity to accounting curricula as the lack of references available for teaching cybersecurity in accounting curricula, some faculty members do not know the importance of cybersecurity, and it is difficult to provide qualified faculty to teach cybersecurity in accounting departments. These results add to the rapidly expanding field of cybersecurity and its impact on accounting in all its fields. The findings of this investigation complement those of earlier studies. The findings of this study make several contributions to the current literature. It can assist in clarifying the concept of cybersecurity in accounting, these findings contribute to participate in filling a gap between accounting education and the accounting profession.

In light of the findings obtained, the study recommends including cybersecurity in accounting curricula in Saudi Arabian universities and establishing specific and clear plans for how to include cybersecurity in accounting curricula. Therefore, there is a definite need to educate and raise awareness of cybersecurity for accounting students; accounting graduates are not required to be cybersecurity specialists but rather to have a knowledge of how it works and its basics. Furthermore, increase the qualification and training of faculty members in the accounting departments of Saudi Arabian universities in the field of cybersecurity. Greater efforts are needed to ensure raising awareness of the importance of cybersecurity in accounting (e.g., research, conferences, training courses, workshops) by accounting departments in universities in Saudi Arabia and the bodies organizing the accounting profession.

The issue of cybersecurity is an intriguing one that could be usefully explored in further research. Several questions remain to be answered. The study findings provide the following insights for future research:

- The results of this study can be relied upon to conduct studies that examine the importance of adding cybersecurity to a specific accounting curriculum.
- A further study could assess the level of awareness of accounting students about cybersecurity.
- A case study of a group of accounting students when they were given a training course on cybersecurity.
- A survey to determine the basics of cybersecurity that companies seek to obtain from accounting graduates.
- A greater focus on challenges and difficulties could produce interesting findings.
- Study to assess the level of awareness of professional accountants for cybersecurity.
- It would be interesting to assess the effects of teaching cybersecurity courses on the competitiveness of accounting departments.

References

AACSB International. (2018). 2018 standards for accounting accreditation. Retrieved from https://www.aacsb.edu/educators/accreditation/accounting-accreditation/aacsb-accounting-accreditation-standards

AICPA. (2018a). Cybersecurity risk management reporting fact sheet. Retrieved from https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative

AICPA. (2018b). SOC for cybersecurity a backgrounder. Retrieved from https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative

AICPA, & NASBA.CPA evolution model curriculum. Retrieved from https://thiswaytocpa.com/programme/modelCPAcurriculum/

Al-Htaybat, K., Alberti-Alhtaybat, L., & Alhatabat, Z. (2018). Educating digital natives for the future: Accounting educators' evaluation of the accounting curriculum. Accounting Education, 27(4), 333-357. https://doi.org/10.1080/09639284.2018.1437758

Al-Maharfi, A. R. A. (2019). Proposed content of accounting information systems course: An empirical comparative study between the academic trends and the Saudi market needs. The Scientific Journal of King Faisal University - Humanities and Administrative Sciences, 20(2), 299-316.

Boss, S., Gray, J., & Janvrin, D. J. (2022). Accountants, cybersecurity isn't just for 'Techies': Incorporating cybersecurity into the accounting curriculum. Issues in Accounting Education, https://doi.org/10.2308/ISSUES-2021-001

Coffey, S. S., & Conrad, C. K. (2021). CPA evolution: What is the early thinking on three CPA exam disciplines. Retrieved from https://www.aicpa.org/news/article/cpa-evolution-what-is-the-early-thinking-on-three-cpa-exam-disciplines#search

Daff, L. (2021). Employers' perspectives of accounting graduates and their world of work: Software use and ICT competencies. Accounting Education, 30(5), 495-524. https://doi.org/10.1080/09639284.2021.1935282

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. https://doi.org/10.1080/23270012.2020.1731721

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. Current Issues in Auditing, 13(2), 1-15. https://doi.org/10.2308/ciia-52419

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. Managerial Auditing Journal, 34(7), 808-834. https://doi.org/10.1108/MAJ-09-2018-2004

Henderson, D., Lapke, M., & Garcia, C. (2016). SQL injection: A demonstration and implications for accounting students. AIS Educator Journal, 11(1), 1-8. https://doi.org/10.3194/1935-8156-11.1.1

Jackson, D., Michelson, G., & Munir, R. (2022). Developing accountants for the future: new technology, skills, and the role of stakeholders. Accounting Education, ahead-of-print(ahead-of-print), 1-28. https://doi.org/10.1080/09639284.2022.2057195

Janvrin, D. J., & Wang, T. (2019). Implications of cybersecurity on accounting information. Journal of Information Systems, 33(3), A1-A2. https://doi.org/10.2308/isys-10715

Komarev, I., & Preobragenskaya, G. (2022). A framework of market-relevant accounting competencies for the gulf cooperation countries (GCC). Journal of Accounting Education, 59, 100782. https://doi.org/10.1016/j.jaccedu.2022.100782

McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K., & Impagliazzo, J. (2014). Toward curricular guidelines for cybersecurity. Paper presented at the Proceedings of the 45th ACM Technical Symposium on Computer Science Education, 81-82. https://doi.org/10.1145/2538862.2538990

No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. Journal of Emerging Technologies in Accounting, 14(1), 1-12. https://doi.org/10.2308/jeta-10539

Pallant, J. (2020). SPSS survival manual: A step by step guide to data analysis using IBM SPSS (7th ed.). London: Routledge. https://doi.org/10.4324/9781003117452

Pendley, J. A. (2018). Finance and accounting professionals and cybersecurity awareness. Journal of Corporate Accounting & Finance, 29(1), 53-58. https://doi.org/10.1002/jcaf.22291

Roohani, S. J., & Zheng, X. (2019). Using ten teaching modules and recently publicized data-breach cases to integrate cybersecurity into upper-level accounting courses. Advances in accounting education: Teaching and curriculum innovations (pp. 113-125). Bingley: Emerald Publishing Limited. https://doi.org/10.1108/S1085-462220190000023007

Yang, S. C. (2019). A curriculum model for cybersecurity master's programme: A survey of AACSB-accredited business schools in the United States. Journal of Education for Business, 94(8), 520-530. https://doi.org/10.1080/08832323.2019.1590296

Yang, S. C. (2021). A meta-model of cybersecurity curriculums: Assessing cybersecurity curricular frameworks for business schools. Education for Business, 96(2), 99-110. https://doi.org/10.1080/08832323.2020.1757594

Yang, S. C., & Wen, B. (2017). Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States. Journal of Education for Business, 92(1), 1-8. https://doi.org/10.1080/08832323.2016.1261790