

## Adopting the cybersecurity concepts into curriculum: the potential effects on students' cybersecurity knowledge

Mohammad Azzeh<sup>1</sup>, Ahmad Mousa Altamimi<sup>2</sup>, Mahmood Albashayreh<sup>3</sup>, Mohammad A. Al-Oudat<sup>3</sup>

<sup>1</sup>Department of Data Science, King Hussein School of Computing Sciences, Princess Sumaya University for Technology, Amman, Jordan

<sup>2</sup>Department of Cybersecurity, Faculty of Information Technology, Applied Science Private University, Amman, Jordan

<sup>3</sup>Department of Computer Science, Faculty of Information Technology, Applied Science Private University, Amman, Jordan

### Article Info

#### Article history:

Received Aug 12, 2021

Revised Dec 15, 2021

Accepted Jan 11, 2022

#### Keywords:

Curricular guidelines

Cybersecurity

Cybersecurity awareness

Knowledge improvement

Theories of learning

### ABSTRACT

This study examines the effect of adopting cybersecurity concepts on the information and technology (IT) curriculum and determines the potential effect on students' knowledge of cybersecurity practices and level of awareness. To this end, a pilot study was first conducted to measure the current level of cybersecurity awareness. The results revealed that students do not have much knowledge of cybersecurity. Thus, a four-step approach was proposed to infuse the relevant cybersecurity topics in five matched courses based on the latest cybersecurity curricular guidelines (CSEC2017). A sample of 42 students was selected purposively without prior knowledge of cybersecurity and divided identically into experimental and control groups. Students in the experimental group were asked to take five consecutive courses over five semesters. In each course, groups went through a pre-test for the infused topics. Then, the experimental group taught the corresponding infused topics. A post-test was administered to both groups at the end of each course, and the t-test was conducted. The results found significant differences between marks of prior and post-tests for 11 out of 14 infused topics. These satisfactory results would encourage universities to infuse cybersecurity concepts into their curriculum.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Ahmad Mousa Altamimi

Department of Cybersecurity, Faculty of Information Technology, Applied Science Private University  
Amman, Jordan

Email: a\_altamimi@asu.edu.jo

## 1. INTRODUCTION

The Internet has developed immensely, facilitating doing business and providing individuals and organizations with digital communication. Over the numerous advantages the internet offers, it is constantly threatened by many risks that often have serious adverse [1]. New digital threats and cyberattacks are coming from new and unexpected sources. Online phishing, social engineering, and malware are just a few examples of cyberattacks [2]. These attacks negatively affect both individuals and the countries' economies. According to [3], it is estimated that cyberattacks' economic impact will increase by around five trillion dollars per year in the next five years. Cyberattacks are getting more sophisticated in the way they misuse and exploit technological advancement [4]. This is in part because many users are unaware of the concept of cybersecurity and how to protect their information. Users often behave in an insecure manner which makes them easy targets for exploitation [5]. According to William Stallings in his book [6], security education provides users with the necessary skills to perform their duties. Education allows users to know actions that could compromise security, identify possible attack vectors, and report to appropriate personnel. The idea of

this approach was identified in the early 2000 s [7], [8]. However, instead of proposing new security courses, efforts have been devoted to proposing guidelines for adopting cybersecurity concepts in the non-security courses to enhance the appropriateness of practice and get better outcomes [9]–[11]. The most notable guideline CSEC2017 results from several computing organizations' joint force (e.g., Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), and International Federation for Information Processing (IFIP)) and was proposed by the cybersecurity community in 2017. The guideline defined the cybersecurity discipline and outlined the concepts that include knowledge areas and crosscutting concepts to provide the basis for knowledge areas in cybersecurity. Students will be empowered with the necessary knowledge to act reasonably in various circumstances and deal with their social reality issues [12].

In this regard, the work of [8] integrated security concepts into existing computer courses. They emphasized this concept's necessity and provided vital suggestions such as security issues that should be discussed throughout the primary and non-major courses in the computer science curriculum to raise awareness of vulnerabilities, threats, and risks. Other researchers have further analyzed this integration and proposed models to provide students with the basic computer security principles without the need for professional instructors insecurity [13]. Researchers recently focused on proposing systematic frameworks for proper integration [14], [15]. In the paper, Ezenwoye [15], proposed a framework with three phases structure based on typical curriculum development cycles (e.g., guideline development, planning, and implementation).

Recently, authors of [16] proposed a conceptual cybersecurity awareness framework to improve the cybersecurity awareness of graduates in any academic institution. The awareness level in developing countries and for new threats have also been investigated in [17]–[19]. Other researchers have considered security in other domains like commercial [20]. Experiments have also been conducted to determine the students' acquired knowledge [21], [22]. In the paper, Siraj *et al.* [21], experimented with the integration across low-level courses using security laboratory modules. Results show a positive impact that is reflected in the security knowledge gained by students. In the paper, Whitney *et al.* [23], the researchers introduced security teaching with Python and got positive results regarding knowledge and awareness. Unfortunately, the widespread attention to this security integration approach is insufficient, and its adoption is minimal [24], [25]. On the other hand, many works have been conducted in the area of educational data mining. Most of them are designed to forecast students' performance to predict their future outcomes based on students' historical data [26]–[28]. The grade point average (GPA) was recognized as the most crucial attribute used to predict performance in many works. As the first step of our study, a pilot study is conducted on 40 students attending the information security course to assess the current level of cybersecurity awareness. The pilot study's main objective was to see how much the students are aware of cyber-attacks and what they do to protect themselves. The survey results indicated that students do not have much knowledge of Cybersecurity; this lack of knowledge reflects when using the Internet while not protecting their data, even on university systems. These findings encourage us to carry out our study. Thus, a four-step methodology is proposed to leverage the cybersecurity concepts into non-security computer science courses and assess the potential effects on students' cybersecurity knowledge. Firstly, five principles have been selected from the cybersecurity Community guideline (CSEC2017) that worked best for the program. The other principles are purposefully not included as they are less important and can be integrated with other concepts. Secondly, the existing curriculum content is mapped to the selected principles. Thirdly, the gaps in the curriculum are identified, where they are filled by infusing new cybersecurity topics. Finally, the gained cybersecurity knowledge is measured to determine the effect of this infusion. The selected security principles are listed in Table 1 along with the related courses, while the complete list of the integrated topics is mentioned in Table 2. Accordingly, the following hypothesis proposed:

$H_a$ : Infusing cybersecurity principles into non-security courses will improve students' awareness and knowledge of Cybersecurity.

Table 1. The selected concepts and corresponding courses

Principles	Course				
	SE	WP	DCN	DB	MP
Fault tolerance	X				
Cryptography algorithms		X			
Secure networking protocols			X		
Authentication techniques				X	X
Hash functions				X	

*SE=Software Engineering, WP=Web-based Programming,*

*DCN=Data Communication and Networks,*

*DS=Database Systems, MP=Mobile Programming, X=selected*

Table 2. The selected courses and their topics

Order	Course name	Level	Topics
1	Software Engineering (SE)	Year 2/Semester 1	SE1: Security breaches SE2: Software vulnerabilities SE3: Fault tolerance techniques
2	Web-Based Programming (WP)	Year 2/Semester 2	WP1: Cryptography WP2: Email and Web Security Protocols WP3: Secure Sockets Layer (SSL) Protocol
3	Data Communication and Networks (DCN)	Year 3/Semester 1	DCN1: Protecting Computing Devices DCN2: Firewall Types DCN3: Two Factor and Mutual Authentication Techniques
4	Database Systems (DB)	Year 3/Semester 2	DB1: Creating and Managing Passwords DB2: SQL injection Attack DB3: Hash Functions
5	Mobile Programming (MP)	Year 4/Semester 1	MP1: Mobile Breaches MP2: Implementing Security Defenses

To conduct the experiment, a sample of 42 IT students have been selected with no prior knowledge in cybersecurity. The sample is then divided into two identical groups, 21 students in the experimental group (E) and 21 students in the control group (C). The students in the experimental group agreed to take the five selected courses. In each course, all students in both groups were asked to undergo pre-evaluation evaluation tests before enrolling on the selected course. In contrast, the experimental group is also administrated to another post-evaluation after the end of that course. Expert instructors have set the questions of both tests in the field of Cybersecurity, and both tests have a different sample of questions.

To statistically test the hypotheses  $H_a$ , two comparisons are performed: within the experimental group and across different groups. Concerning the experimental group, the first comparison was conducted to examine the significant difference between the pre-test and post-test scores of the experimental group alone and the control group alone using paired t-test. The second comparison was conducted to examine the significant difference between pre-test and post-test of both experimental and control groups, using the two-sample t-test. The purpose of both tests is to ensure that the experimental group students are acquired the required cybersecurity knowledge. Results revealed significant differences between marks of pre-evaluation and post-evaluation tests for most infused topics. Moreover, results show that the postmarks are in general higher than pre marks for the experimental group. The results also demonstrate that infusing important cybersecurity topics within other computer science courses can increase students' awareness and knowledge regarding cybersecurity concepts. The remainder of this paper is organized as follows. Section 2 presents the research methodology and the experimental work, along with the evaluation measures. The results are discussed then in section 3. Finally, section 4 presents the conclusion and directions for future research.

## 2. RESEARCH METHOD

The research methodology of our study is divided into three phases. In the first phase, a pilot study is designed based on data collected from 40 students to examine their awareness of cybersecurity concepts. The survey's feedback enables us to determine security awareness levels that university students already have. Applicable principles were set and integrated into five non-security courses in the second phase, following a four-step methodology. Firstly, five appropriate principles have been selected based on the CSEC2017 guideline: fault tolerance, cryptography algorithms, secure networking protocols, authentication techniques, and hash functions. Secondly, a set of courses from the existing curriculum is mapped to the selected principles. Thirdly, the curriculum gaps are identified and filled. Finally, a set of topics is proposed to these gaps.

In the third phase, 42 students have been carefully selected, such that they have no prior knowledge of Cybersecurity, nor they have taken any one of the five courses. The students were divided into two identical groups (experimental and control groups). The students in the experimental group agreed to take the five selected courses in consecutive order. In contrast, the other students in the control group were selected from the registered students in that course. All students were asked to undergo two tests: i) a pre-evaluation test (pre enrolling on the selected course) and ii) a post-test (after the end of that course) on the cybersecurity topics that they have learned within the selected courses. In both tests, the questions were selected carefully by expert instructors in cybersecurity, and both tests have a different sample of questions. A paired t-test statistical test is then performed to examine the significant difference between students' marks in the experimental group for the pre-evaluation and post-evaluation. In addition to using the two-sample t-test to examine the difference between experimental and control groups concerning pre and post-tests.

### 3. RESULTS AND DISCUSSION

#### 3.1. Results of pilot study

The general knowledge about cybersecurity and cyber-attacks, password, authentication, email security, firewalls, and mobile security are investigated. The results of the study are summarized in Table 3. Regarding the first question about the general knowledge of cybersecurity and security attacks, it was found that only 10% are strongly knowledgeable. The other questions' results have confirmed the responses to this self-evaluation. Considering this result for IT specialists' respondents, this lack of knowledge is likely higher in the general population. The second question asked about creating strong passwords. Surprisingly, more than 40% of the respondents used the same password for other services, and another 20% preferred to create an easy password. This might be a bad indicator of password creating knowledge. Similarly, the authentication techniques knowledge is not much better, as seen in question 3. Most of the participants do not know what two-factor authentication is. regarding the website trust in question 4, the same issue is revealed for respondents who consider the email server responsible for scanning the email links, which is not the case in practice. This awareness level is also reflected in question 5, where around 65% of the participants will download and install a program suggested by another site.

Table 3. Results of pilot study

Question	Response	#	%
1. On a scale of one to five (five being the most confident), rank your knowledge about cybersecurity and attacks?	No idea	3	7.50%
	Hear about	10	25.00%
	Some knowledge	16	40.00%
	Good knowledge	7	17.50%
	Strong knowledge	4	10.00%
	<b>Total</b>	<b>40</b>	<b>100.00%</b>
2. Do you use a strong password to access your social or financial accounts?	Re-use the same password used in other services	16	40.00%
	Create a password that is as easy as possible to remember	8	20.00%
	Create a very complex password and store it in a manager service	10	25.00%
	Create a new password that is similar to another service	4	10.00%
	Create an entirely new strong password	2	5.00%
	<b>Total</b>	<b>40</b>	<b>100.00%</b>
3. Do you know what Two-Factor Authentication (2FA) is, and do you use it?	Yes	7	17.50%
	No	33	82.50%
	<b>Total</b>	<b>40</b>	<b>100.00%</b>
4. What would you do if you received an email with links to other sites?	Do not click the link	14	35.00%
	Click the links because the email server has already scanned the email	21	52.50%
	Hover the mouse on links to verify the destination URL before clicking	5	12.50%
	<b>Total</b>	<b>40</b>	<b>100.00%</b>
5. What would you do when a pop-up window is displayed states that you should download and install a diagnostics program to protect your computer?	Download, and install the program	26	65.00%
	Inspect the pop-up windows to verify their validity	8	20.00%
	Ignore the message and close the website	6	15.00%
	<b>Total</b>	<b>40</b>	<b>100.00%</b>
6. What action do you take if you need to connect to the Internet via an open Wi-Fi hotspot, but it asks you to switch off the firewall?	Connect and switch off the firewall	28	70.00%
	Do not connect to it and keep your firewall	8	20.00%
	Connect to it and establish a VPN to a trusted server	4	10.00%
	<b>Total</b>	<b>40</b>	<b>100.00%</b>
7. Have you ever rejected a mobile app request for accessing your contacts, camera, or location?	Yes	24	60.00%
	No	16	40.00%
	<b>Total</b>	<b>40</b>	<b>100.00%</b>

Another parameter that still illustrates low awareness of cybersecurity is shown when 70% of respondents are willing to switch off their firewalls for a free Wi-Fi hotspot given in question 6. It is also important to underline that the awareness about denying a mobile app request personal data positively impacts participants' responses. 60% of the participants will reject a mobile app request accessing their contacts, camera, or locations for the last question.

The survey results indicated that students do not have much knowledge of Cybersecurity; they need to be motivated to security precautions and be exceptionally the risks of online services. Also, it appears that educational institutions do not have an active approach to improving awareness among students. It is worth mentioning here that our pilot results are compatible with recent studies. One can consider the study in [29], which analyzed cybersecurity awareness among education sector members in the Middle East region. The results reveal that the participants do not have the requisite knowledge and understanding of the importance of security principles and their practical application in day-to-day work.

**3.2. Results of pre-evaluation and post-evaluation tests**

**3.2.1. Statistical tests between pre and post exams for experimental group**

In these tests, one noticed that the students' overall average marks in the post-evaluation test are higher than the pre-evaluation test with significant t-test results for two topics (SE1 and SE2), as shown in Table 4. It can also notice that pre-evaluation marks' standard deviation is close to that of post-evaluation marks in most courses. The Cohen's d measure indicates that the effect size for topics (SE1 and SE2) is greater than 0.5, which means a significant difference between pre and postmarks, less than 0.5 for SE1.

Table 1. Results of software engineering course, using paired t-test

ID	Cybersecurity Topic	Before	After	t-test	Effect size (Cohen's d)	Win	tie	lose
SE1	SB	46.7±11.4	66.4±12.8	t=-9.0, p-value<0.001*	1.63	19	0	2
SE2	SV	48.3±18.1	72.7±13.7	t=-8.5, p-value<0.001*	1.53	17	0	4
SE3	MTS	61.0±15.6	65.7±13.4	t=-1.8, p-value=0.08	0.32	12	1	8

\*Significant at 95%. SB=security breaches, SV=software vulnerabilities, MTS=malware types and symptoms

The same findings can be seen for the web programming course, as shown in Table 5. Surprisingly, the web programming course's average marks are less than that of the software engineering course. The paired t-test between the two evaluations shows significant differences between the two marks for all topics. The Cohen's d effect size confirms the obtained statistical differences with an effect size greater than 0.5. Also, the number of wins is significantly greater than the number of losses, which revealed that the number of students who improved their marks is larger than those who failed to improve.

Table 5. Results of web programming course, using paired t-test

ID	Cybersecurity Topic	Before	After	t-test	Effect size (Cohen's d)	win	tie	lose
WP1	CRP	41.1±14.5	52.5±9.4	t=-5.2394, p-value<0.001*	0.95	14	0	7
WP2	EWS	44.8±11.9	57.6±15.9	t=-5.0848, p-value<0.001*	0.92	15	0	6
WP3	SSL	30.4±15.3	46.5±13.7	t=-6.1875, p-value<0.001*	1.11	15	1	5

\*Significant at 95%. CRP=cryptography, EWS=email and web security, SSL=secure sockets layer (SSL)

The results in Table 6 demonstrate that adopting three cybersecurity topics would partially enhance student awareness regarding the Data communication and networking course. However, only two topics (DCN2 and DCN3) show significant improvements, as confirmed by the t-test. Surprisingly, the average of pre and postmarks for DCN1 are similar with insignificant differences between them. In contrast, the overall average of post-evaluation marks is higher than the average of pre-evaluation marks for DCN1 and DCN2. Thus, satisfactory improvements in student knowledge in the DCN course are generally shown, but this improvement did not show the expected level.

Table 6. Results of data communication and networking course, using paired t-test

ID	Cybersecurity Topic	Before	After	t-test	Effect size (Cohen's d)	win	tie	lose
DCN1	PCD	54.1±15.1	54.8±17.5	t=-0.24, p-value=0.814	0.04	11	0	10
DCN2	FT	50.0±19.1	57.3±13.6	t=-2.40, p-value=0.019*	0.44	13	0	8
DCN3	TFMA	42.4±16.0	48.6±18.3	t=-2.01, p-value=0.047*	0.36	12	1	8

\*Significant at 95%. PCD = protecting computing devices, FT = firewall types, TFMA = two factors, and mutual authentication

The results of significance tests for the database course are a little bit different than previous courses. Three cybersecurity topics were adopted, as mentioned in Table 7. The average of marks for post-test is larger in general than the pre-evaluation test, suggesting good improvements in students' awareness. The paired t-test results demonstrate a significant difference between pre-evaluation and post-evaluation marks for three cybersecurity topics: Creating and managing passwords and hash functions.

Table 7. Results of database systems course, using paired t-test

ID	Cybersecurity Topic	Before	After	t-test	Effect size (Cohen's d)	win	tie	lose
DB1	CMP	60.7±11.9	66.3±12.6	t=-2.6, p-value=0.01*	0.46	13	1	7
DB2	SIA	49.8±16.4	64.8±8.80	t=-6.4, p-value<0.001*	1.19	16	0	5
DB3	HF	38.6±15.4	45.4±10.1	t=-2.9, p-value=0.004*	0.54	14	0	7

\* Significant at 95%. CMP: creating and managing passwords, SIA: SQL injection attack, HF: hash functions

This result suggests that the student awareness significantly improved while taking these topics within the database course. However, the effect size revealed a strong justification to judge that the difference between two evaluation marks is significant for only two topics (DB2 and DB3) with Cohen's d over 0.5. Concerning the mobile programming course, Table 8 shows significant differences between pre-evaluation and post-evaluation tests for only MP2 topics, confirming that adopting these cybersecurity topics in a programming course would enhance student awareness about threats that can affect the mobile application. In contrast, a significant difference for MP1 was not found. Both findings are confirmed by Cohen's d effect size, which is less than 0.5 for MP1 and greater than 0.5 for MP2. It can also notice that the average marks of pre-evaluation tests for both engaged cybersecurity topics are quite acceptable, demonstrating that the student in this course is familiar with this kind of threat. Also, significant improvements in their marks after adopting MP1 were not noticed, which is confirmed by the number of wins and losses for MP1 that is so close.

Table 8. Results of mobile programming course, using paired t-test

ID	Cybersecurity Topic	Before	After	t-test	Effect size (Cohen's d)	win	tie	lose
MP1	MB	67.1±11.2	70.2±15.4	t=-1.3, p-value=0.20	0.23	12	0	9
MP2	ISD	53.5±12.7	73.7±13.4	t=-8.6, p-value<0.001*	1.54	19	0	2

\*Significant at 95%. MB=mobile breaches, ISD=implementing security defenses

### 3.2.2. Statistical test between experimental and control groups

The pre and post-test marks for both control and experimental groups for each course are infused cybersecurity topics in these tests were compared. The average of marks for each cybersecurity topic is converted to a scale from 0 to 100. Table 9 shows the statistical analysis using the Two-sample t-test between the experimental and control group for software engineering course. Results show no significant difference between the experimental and control groups in the pre-test of all software engineering topics. This confirms that students' knowledge in both groups is relatively similar with no significant difference. In contrast, we noticed positive significance for the post-test between the experimental and control group with a large effect size. These findings are consistent with our basic assumptions that presume that the student's marks in the experimental and control group must be relatively similar to the pre-test because they have no prior knowledge and are significantly different in terms of post-tests.

Table 9. Comparison between experimental and control group for software engineering course, using two-sample t-test

Test Type	ID	Cybersecurity topic	Experimental group	Control group	t-test	Effect size (cohen's d)
Pre-Test	SE1	SB	46.7±11.4	51.6±12.3	t=-1.44, p-value=0.19	0.41
	SE2	SV	48.3±18.1	46.7±11.8	t=0.34, p-value=0.74	0.10
	SE3	MTS	61.0±15.6	57.7±14.6	t=0.71, p-value= 0.48	0.21
Post-Test	SE1	SB	66.4±12.8	52.4±12.9	t=3.53, p-value=0.001*	1.09
	SE2	SV	72.7±13.7	48.3±10.2	t=6.54, p-value<0.001*	2.02
	SE3	MTS	65.7±13.4	55.5±15.2	t=2.31, p-value=0.02*	0.71

\*Significant at 95%. SB=security breaches, SV=software vulnerabilities, MTS=malware types and symptom

Table 10 shows the results for the web programming course. Here, a significant difference between both groups regarding the pre-test for the secure sockets layer (SSL) topic is shown. However, no difference was shown for the remaining topics between the two groups. In terms of post-test, no significant difference was shown between the two groups for the cryptography topic. This is due to the difficulty of this topic as it depends on complex math theory. However, a significant difference was shown for the remaining topics (e.g., email and web security and secure sockets layer).

Table 10. Comparison between experimental and control group for web programming course, using two-sample t-test

Test Type	ID	Cybersecurity topic	Experimental group	Control group	t-test	Effect size (cohen's d)
Pre-Test	WP1	CRP	41.1±14.5	46.3±11.2	t=-1.30, p-value=0.20	0.40
	WP2	EWS	44.8±11.9	43.6±10.5	t=0.347, p-value=0.73	0.11
	WP3	SSL	30.4±15.3	40.7±16.7	t=-2.08, p-value=0.044*	0.64
Post-Test	WP1	CRP	52.5±9.4	48.6±11.7	t=1.2, p-value=0.24	0.41
	WP2	EWS	57.6±15.9	47.3±12.3	t=2.35, p-value=0.025*	0.72
	WP3	SSL	46.5±13.7	38.2±10.1	t=2.23, p-value=0.032*	0.69

\* Significant at 95%. CRP=cryptography, EW=email and web security, SS=secure sockets layer (SSL)

Table 11 shows the results for the data communication and networking course. For the pre-test marks, no significant difference was shown between both groups for all topics. However, a significant difference was shown in the post-test marks for two topics (e.g., protecting computing devices and firewall types). On the other hand, students did not perform well in the two factor and mutual authentication topic.

Table 11. Comparison between experimental and control group for data communication and networking course, using two-sample t-test

Test Type	ID	Cybersecurity topic	Experimental group	Control group	t-test	Effect size (cohen's d)
Pre-Test	DCN1	PCD	54.1±15.1	52.3±12.4	t=0.42, p-value=0.68	0.13
	DCN2	FT	50.0±19.1	51.7±16.3	t=-0.31, p-value=0.76	0.10
	DCN3	TFMA	42.4±16.0	46.1±13.4	t=-0.81, p-value=0.42	0.25
Post-Test	DCN1	PCD	54.8±17.5	45.0±12.2	t=2.11, p-value=0.04*	0.65
	DCN2	FT	57.3±13.6	46.9±12.1	t=2.62, p-value=0.01*	0.81
	DCN3	TFMA	48.6±18.3	41.1±13.4	t=1.52, p-value=0.13	0.47

\* Significant at 95%. PCD=protecting computing devices, FT=firewall types, TFMA=two factor, and mutual authentication

Table 12 shows the results for the database systems course. The gained results of this course are similar to the previous course (e.g., data communication and networking). Specifically, results show no significant difference between both groups regarding the pre-test for all topics. In addition, a significant difference was shown between the two groups for all topics in terms of post-test. This is due to the popularity of these topics, as most students used the topics' techniques daily (e.g., creating and managing passwords, SQL injection attack, and hash functions).

Table 12. Comparison between experimental and control group for database systems course, using two-sample t-test

Test Type	ID	Cybersecurity topic	Experimental group	Control group	t-test	Effect size (cohen's d)
Pre-Test	DB1	CMP	60.7±11.9	64.9±13.3	t=-1.1, p-value=0.29	0.33
	DB2	SIA	49.8±16.4	51.4±11.8	t=-0.36, p-value=0.72	0.11
	DB3	HF	38.6±15.4	42.6±12.1	t=-0.94, p-value=0.36	0.29
Post-Test	DB1	CMP	66.3±12.6	57.1±12.4	t=2.38, p-value=0.02*	0.74
	DB2	SIA	64.8±8.80	52.3±14.6	t=3.36, p-value=0.002*	1.04
	DB3	HF	45.4±10.1	38.7±9.5	t=2.21, p-value=0.03*	0.68

\* Significant at 95%. CMP=creating and managing passwords, SIA=SQL injection attack, HF=hash functions

Table 13 shows the results for the mobile programming course. Due to the topic novelty, most of the topics did not significantly differ between the experimental and control groups. For instance, the mobile breaches and implementing security defenses topics have no significant difference between groups in pre-test marks. The same case for implementing security defenses post-test marks were noticed, where no significant difference was noticed between groups. However, a significant difference was shown for the Mobile Breaches topics, where students gain knowledge after Infusing this principle.

Table 13. Comparison between experimental and control group for mobile programming course, using two-sample t-test

Test Type	ID	Cybersecurity topic	Experimental group	Control group	t-test	Effect size (cohen's d)
Pre-Test	MP1	MB	67.1±11.2	64.3±12.4	t=0.77, p-value=0.44	0.24
	MP2	ISD	53.5±12.7	56.7±11.9	t=-0.84, p-value=0.40	0.26
Post-Test	MP1	MB	70.2±15.4	61.5±10.3	t=2.15, p-value=0.04*	0.66
	MP2	ISD	73.7±13.4	59.9±12.1	t=3.5, p-value=0.001	1.08

\* Significant at 95%. MB=mobile breaches, ISD=implementing security defenses

Indeed, from the above statistical test results, a conclusion can be drawn that, in general, the students have a quite low level of cybersecurity awareness, as confirmed in the averages and standard deviations of pre-evaluation marks. But these marks are significantly improved in almost all topics except for three topics, namely, SE3, DCN1, MP1. To test this hypothesis, the average marks for all pre marks of all topics (Say before) and average postmarks for all topics (say after) for the experimental group only were computed.

The paired t-test results ( $t=-17.3$ ,  $p\text{-value}<0.001$ ) between the before and after groups confirmed  $H_a$ 's hypothesis and revealed a significant difference between students' average marks in all topics. Furthermore, average marks for all postmarks of all topics for the experimental group (E) and average postmarks for the control group (C) are computed. Then two-sample t-test results ( $t=2.16$ ,  $p\text{-value}=0.031$ ) between them were applied. The obtained results confirmed  $H_a$ 's hypothesis and revealed a significant difference between students' average marks. Figure 1 summarizes these findings.

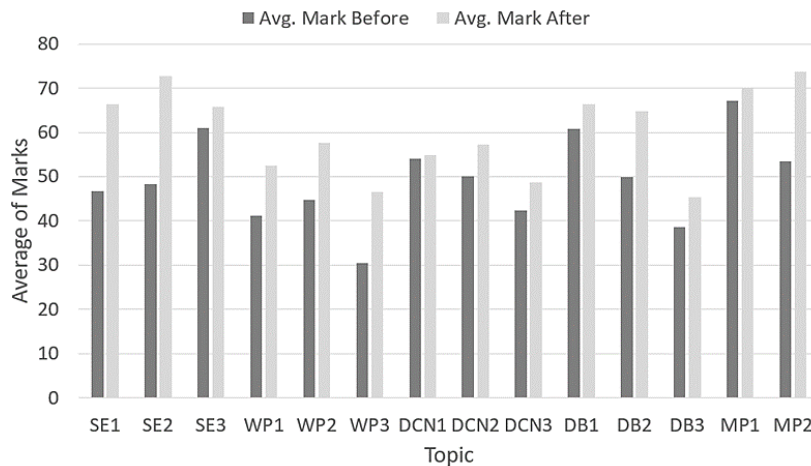


Figure 1. Courses results before and after the infusion

#### 4. CONCLUSION

This paper proposes a detailed approach for examining the effect of infusing cybersecurity principles in the IT curriculum's non-security courses on students' awareness and Cybersecurity knowledge. However, before determining that, our study is started with a pilot study conducted on 40 IT students to see how much students are aware of 7 principles related to Cybersecurity and what they do to protect themselves from cyber-attacks. The obtained results indicated that students do not have much knowledge of Cybersecurity and need to be aware of security precautions and online services risks. Also, results revealed that educational institutions do not actively approach cybersecurity awareness among students. Based on this finding, the study relied on the remarkable guideline (CSEC2017) and distilled the main security principles that the curriculum must include. Accordingly, these principles are mapped to the relevant curriculum courses and proposed a set of topics that will reflect the selected principles.

To determine the effects of infusing principles, the degree of improvements in the acquired knowledge for 42 students through pre and post-evaluation tests were assessed. The students were divided into two identical groups (experimental and control groups). All students were asked to undergo two tests, a pre-evaluation test (pre enrolling on the selected course) and a post-test (after the end of that course) on the cybersecurity topics. A paired t-test statistical test is then performed to examine the significant difference between experimental group students' marks in the pre-evaluation and post-evaluation.

In addition, the two-sample t-test is used to examine the difference between experimental and control groups for pre and post-tests. We noticed that the students often have a quite low level of cybersecurity awareness, as confirmed in the averages and standard deviations of pre-evaluation marks. Moreover, results show that the postmarks are in general higher than pre marks. The results demonstrate that engaging important cybersecurity topics within other computer science courses can increase students' awareness and knowledge regarding cybersecurity concepts. It is highly encouraged that education institutes integrate some important cybersecurity topics within existing courses based on the obtained results.

#### ACKNOWLEDGEMENTS




The authors are grateful to the Applied Science Private University, Amman-Jordan, for the full financial support granted to cover the publication fee of this research article.






## REFERENCES

- [1] J. M. Machimbarrena, E. Calvete, L. Fernández-González, A. Álvarez-Bardón, L. Álvarez-Fernández, and J. González-Cabrera, "Internet risks: An overview of victimization in cyberbullying, cyber dating abuse, sexting, online grooming and problematic internet use," *International Journal of Environmental Research and Public Health*, vol. 15, no. 11, p. 2471, Nov. 2018, doi: 10.3390/ijerph15112471.
- [2] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers and Security*, vol. 105. arXiv, Jun. 2021, doi: 10.1016/j.cose.2021.102248.
- [3] S. R. Iyer, B. J. Simkins, and H. Wang, "Cyberattacks and impact on bond valuation," *Finance Research Letters*, vol. 33, p. 101215, Mar. 2020, doi: 10.1016/j.frl.2019.06.013.
- [4] W. Primoff and S. Kess, "The Equifax data breach: What CPAs and firms need to know," *The CPA Journal*, vol. 87, no. 12, pp. 14–17, 2017, [Online]. Available: <https://www.ftc.gov/equifax-data-breach>
- [5] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Computers and Security*, vol. 88, p. 101640, Jan. 2020, doi: 10.1016/j.cose.2019.101640.
- [6] Q. Zhu, S. Rass, and P. Schartner, "Community-based security for the internet of things," *Smart Cities Cybersecurity and Privacy*, vol. SPECIAL IS, pp. 11–19, 2018, doi: 10.1016/B978-0-12-815032-0.00002-0.
- [7] R. B. Vaughn, "Application of security to the computing science classroom," *SIGCSE Bulletin (Association for Computing Machinery, Special Interest Group on Computer Science Education)*, vol. 32, no. 1, pp. 90–94, 2000, doi: 10.1145/331795.331822.
- [8] P. Mullins *et al.*, "Panel on integrating security concepts into existing computer courses," in *SIGCSE Bulletin (Association for Computing Machinery, Special Interest Group on Computer Science Education)*, 2002, pp. 365–366, doi: 10.1145/563517.563480.
- [9] D. Burley, M. Bishop, S. Kaza, D. S. Gibson, E. Hawthorne, and S. Buck, "ACM Joint Task Force on Cybersecurity Education," in *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*, Mar. 2017, pp. 683–684, doi: 10.1145/3017680.3017811.
- [10] J. R. S. Blair, C. M. Chewar, R. K. Raj, and E. Sobiesk, "Infusing Principles and Practices for Secure Computing Throughout an Undergraduate Computer Science Curriculum," in *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*, Jun. 2020, pp. 82–88, doi: 10.1145/3341525.3387426.
- [11] H. Topi *et al.*, "IS 2010: Curriculum guidelines for undergraduate degree programs in information systems," *Communications of the Association for Information Systems*, vol. 26, no. 1, pp. 359–428, 2010, doi: 10.17705/1cais.02618.
- [12] I. M. Venter, R. J. Bignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as 'the three R's,'" *Heliyon*, vol. 5, no. 12, p. e02855, Dec. 2019, doi: 10.1016/j.heliyon.2019.e02855.
- [13] L. Null, "Integrating security across the computer science curriculum," *Journal of Computing Sciences in Colleges*, vol. 19, no. 5, 2004.
- [14] "ISTE 2018 Resources | The Institute of Progressive Education and Learning." <http://institute-of-progressive-education-and-learning.org/home/resources/iste-2018/>
- [15] O. Ezenwoye, "Integrating Security into Computer Science Curriculum," in *Proceedings - Frontiers in Education Conference, FIE*, Oct. 2019, vol. 2019-October, doi: 10.1109/FIE43999.2019.9028523.
- [16] M. Khader, M. Karam, and H. Fares, "Cybersecurity awareness framework for academia," *Information (Switzerland)*, vol. 12, no. 10, p. 417, Oct. 2021, doi: 10.3390/info12100417.
- [17] T. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among students of Majmaah University," *Big Data and Cognitive Computing*, vol. 5, no. 2, May 2021, doi: 10.3390/bdcc5020023.
- [18] A. Garba, Maheyzah Binti Sirat, Siti Hajar, and Ibrahim Bukar Dauda, "Cyber Security Awareness Among University Students: A Case Study," *Science Proceedings Series*, vol. 2, no. 1, pp. 82–86, Apr. 2020, doi: 10.31580/sps.v2i1.1320.
- [19] I. Alshourbaji *et al.*, "An Approach To Weigh Cybersecurity Awareness Questions In Academic Institutions Based On Principle Component Analysis: A Case Study Of Saudi Arabia," *Independent Researcher in Social Media. Areas include research ethics*, 2021, [Online]. Available: [www.ijstr.org](http://www.ijstr.org)
- [20] Q. Hammouri, er Majali, D. Almajali, A. Aloqool, and J. Ahmad Al-Gasawneh, "Explore the Relationship between Security Mechanisms and Trust in E-Banking: A Systematic Review," *Annals of The Romanian Society for Cell Biology*, vol. 25, pp. 17083–17093, 2021, [Online]. Available: <http://annalsofscb.ro>
- [21] A. Siraj, S. Ghafoor, J. Tower, and A. Haynes, "Empowering faculty to embed security topics into computer science courses," in *ITiCSE 2014 - Proceedings of the 2014 Innovation and Technology in Computer Science Education Conference*, 2014, pp. 99–104, doi: 10.1145/2591708.2591741.
- [22] S. Kaza, B. Taylor, H. Hochheiser, S. Azadegan, M. O'Leary, and C. F. Turner, "Injecting Security in the Curriculum – Experiences in Effective Dissemination and Assessment Design," in *The Colloquium for Information Systems Security Education (CISSE)*, 2010, p. 8, [Online]. Available: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Injecting+Security+in+the+Curriculum+Experiences+in+Effective+Dissemination+and+Assessment+Design#0>
- [23] M. Whitney, H. L. Richter, B. Chu, and J. Zhu, "Embedding secure coding instruction into the IDE: A field study in an advanced CS course," in *SIGCSE 2015 - Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, Feb. 2015, pp. 60–65, doi: 10.1145/2676723.2677280.
- [24] C. Yue, "Teaching computer science with cybersecurity education built-in," 2016.
- [25] D. A. Almajali and R. Masa'deh, "Antecedents of students' perceptions of online learning through covid-19 pandemic in Jordan," *International Journal of Data and Network Science*, vol. 5, no. 4, pp. 587–592, 2021, doi: 10.5267/j.ijdns.2021.8.009.
- [26] W. F. W. Yaacob, S. A. M. Nasir, W. F. W. Yaacob, and N. M. Sobri, "Supervised data mining approach for predicting student performance," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 3, pp. 1584–1592, Dec. 2019, doi: 10.11591/ijeeecs.v16.i3.pp1584-1592.
- [27] I. D. Shetty, D. Shetty, and S. Roundhal, "Student Performance Prediction," *International Journal of Computer Applications Technology and Research*, vol. 8, no. 5, pp. 157–160, Apr. 2019, doi: 10.7753/ijcatr0805.1003.
- [28] N. Tomasevic, N. Gvozdenovic, and S. Vranes, "An overview and comparison of supervised data mining techniques for student exam performance prediction," *Computers and Education*, vol. 143, p. 103676, Jan. 2020, doi: 10.1016/j.compedu.2019.103676.
- [29] S. Al-Janabi and I. Al-Shourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East," *Journal of Information and Knowledge Management*, vol. 15, no. 1, Mar. 2016, doi: 10.1142/S0219649216500076.




**BIOGRAPHIES OF AUTHORS**

**Mohammad Azzeh**    is a professor of Computing at Princess Sumaya University for Technology. He holds PhD in computing from the University of Bradford, UK. His research interests focus on Data Science, Mining Software Repositories, Machine Learning for Software Engineering Problems, and Software Cost Estimation. Dr. Azzeh is an invited referee for high-quality journals and PC member of international conferences. He was a guest editor in the Journal of Neural Computing and Applications (Springer) and published over 40 research articles in reputable journals and conferences. He can be contacted at email: m.azzeh@psut.edu.jo.






**Ahmad Altamimi**    is an associate professor of Cybersecurity and Cloud Computing at Applied Science Private University. He has been received his PhD degree from Concordia University–Montreal, Canada, in 2014. His research interests are primarily in Cybersecurity, Online Education, and Machine learning. Dr Altamimi participated in the organization of many conferences and be a reviewer for different journals. He has many publications in reputable journals and international conferences. He can be contacted at email: a\_altamimi@asu.edu.jo.



**Mahmood AlBashayreh**    is an assistant professor of computer science at Applied Science Private University. He holds a Ph.D. in Software Engineering from University Utara Malaysia since 2014. His research interests include reuse-based software engineering, context-aware computing, mobile patient monitoring systems, and conceptual modeling of information systems. Dr. Mahmood has recently focused on using machine learning and deep learning techniques for Natural Language Processing (NLP). He has participated in the organization of many conferences. He has many publications in reputable journals and international conferences. He can be contacted at email: m\_albashayreh@asu.edu.jo.



**Mohammad A. AL-Oudat**    received the BS degree in Computer Science from Yarmouk University, Jordan, in 2004, and the MS degree in Information Technology from Universiti Utara Malaysia, Malaysia in 2008, and Ph.D. degree holder in computer science and engineering at the University of Bridgeport, Bridgeport, CT, USA. He is currently working at Applied Science Private University (ASU), Amman, Jordan as an assistant professor in the computer science dept. at the faculty of information technology. He can be contacted at email: m.aloudat@asu.edu.jo.