Integrating Cybersecurity Education in University Curriculum

An-Mari Varbanova, University of Twente, The Netherlands
a.varbanova@student.utwente.nl

As our world is becoming increasingly reliant on technology, cybersecurity awareness has become vital. Cyber-crimes can be harmful to both individuals and companies, by causing data breaches, monetary loss or preventing the normal operation of institutions. Education is an important element of cultivating cybersecurity awareness. In this research, we aim to discover the current level of cybersecurity awareness among Business Information Technology (BIT) students at the University of Twente (UT) and gain insight into their preferred methods of education. The study involved 28 Business Information Technology students and showed their preference for combining methods of hybrid (combining online and in-person) education. The most preferred hybrid options were also analysed. Students with higher levels of cybersecurity awareness choose to learn cybersecurity through workshops, tutorials, lectures and project-based learning, while those with lower scores on this scale most often choose lectures. Additionally, the conducted literature review showed that practical sessions, hands-on exercises and exercises with competitive elements are suitable for effectively teaching cybersecurity concepts to university students. The correlation between cybersecurity awareness and various variables involved in the research was also tested. This research aims to bring valuable insight into the most desirable and effective methods of instruction on the topic of cybersecurity, and assist the successful integration of this course in the programme curriculum.

Additional Key Words and Phrases: cybersecurity, cybersecurity awareness, methods of education, user-behaviour.

1 INTRODUCTION

In 1988, a Cornell University student developed a self-replicating program which effectively stopped 10% of computers connected to ARPANET (The Advanced Research Projects Agency Network) at the time [17]. This event has started the discussion on technology vulnerabilities [17]. Nowadays, cybersecurity awareness has become increasingly relevant in a tech-driven world. For businesses, cyber-attacks can have detrimental consequences, ranging from financial loss to damaged integrity or reputation. According to the Cyber Security Assessment from 2021, the Netherlands has suffered a broad range of cyber-attacks, and the damages can be substantial [18]. Indeed, during the pandemic there has been an increase in the number of cyber-crimes [18]. Dutch healthcare organizations, for instance, have been subject to malware attacks via email, however, adequate measures are not always taken to address cyber-issues [18]. Cybersecurity is undoubtedly essential for the normal operation of governments, businesses and society.

On a global scale, many cyberattacks have taken place in 2021. Issues for companies can range from data theft to fraud, and fighting these crimes is vital [13]. Among the most common attacks are denial of service attacks (DoS), viruses, and trojans [7]. Their impact can often result in revenue loss and leaked sensitive data [7]. One example is the Volkswagen and Audi attack, which led to data breach and over 3 million customers' private data being leaked [33]. Another example, relates to the conference platform Zoom, and the instance is commonly referred to as "zoombombing" [8]. It resulted in attackers entering meetings unauthorised and distributing inappropriate or offensive messages to participants [8]. In fact, it can be seen cyber-awareness is crucial for businesses. Researchers suggest that leadership needs to ensure that cybersecurity is an integral component of work across the institution, rather than being confined to an issue which only IT departments deal with [10]. Cybersecurity education is therefore a vital element of one's expertise and can bring substantial value to companies, preventing capital loss and harm.

Individuals, along with companies, can also be victims of cyber-attacks. Breaches of privacy and compromised personal information can have undesirable psychological effects [12]. Cybersecurity researchers from Oxford University have discovered that cyber-crimes can lead to reputation loss and negatively influence personal relationships [32]. The extent to which individuals can be affected by cyber-attacks outlines the importance of cybersecurity education, and its role in cultivating feelings of safety and psychological comfort among society.

Modern research has recognized the need to match technological potential with education, to ensure a safer cyber environment [24]. In fact, cybersecurity is vital for higher educational institutions. The transparent and open nature of educational institutions can pose cybersecurity threats and create room for exploitation of vulnerabilities [10]. The online threats, which universities can fall victim to and their consequences can range from damaged reputation to leak of sensitive information or research data [10]. If identified and addressed early, the damages of cyber-attacks can be mitigated [24]. However, there are several challenges cybersecurity education is faced with, ranging from lack of resources or expertise, to difficulties with keeping up to date with rapid technological change [24]. Although addressing these issues is challenging, equipping students with the tools needed to successfully navigate possible cyber threats has an immense impact on both an individual and national level [24].

Researchers have discovered that high school education in the Netherlands rarely addresses the topic of cyber safety [31]. Students, therefore, acquire information on the topic through their family or merely through their own experiences on the internet [31].

TScIT 37, July 8, 2022, Enschede, The Netherlands

In recent years, there has been extensive research on the consequences of cyber-attacks and the importance of cybersecurity to businesses, governments and individuals. However, it has also become clear that education needs to match technological potential and current threats to cybersecurity. Cybersecurity education can support a more conscious use of technology, as well as increase the overall security among students. The focal point of discussion in this paper will be the integration of cybersecurity education in the Business Information Technology programme at the University of Twente. The research objective will be to conduct a literature review, in order to find the most suitable methods of integrating this subject into the curriculum, as well as conducting surveys to assess the current level of cybersecurity awareness of students and their preferred methods of teaching. This study aims to add a valuable contribution by offering a view on cybersecurity in higher educational institutions, as well as proposing a practical plan for the introduction of this topic in the Business Information Technology programme at the University of Twente.

2 RESEARCH QUESTION

The main objective of this research is to answer the following research question:

How can universities effectively integrate cybersecurity in education?

This will be answered through addressing the following sub-questions:

- **Sub-question 1**: What are the most suitable educational methods to integrate the subject of cybersecurity in the curriculum of the Business Information Technology programme at the University of Twente?
- **Sub-question 2**: What is the current level of cybersecurity awareness of Business Information Technology students at the University of Twente?

3 RESEARCH METHODOLOGY

In this section we will outline the methods of data collection and how each sub question was addressed. The variables involved in the study are cybersecurity awareness score, age, sex, study, preference for online/in-person education, preferred method of education, workload preference and attendance preference.

3.1 Sub-question 1

In order to answer sub-question 1, a guideline for the successful execution of the course needs to be developed. This entails suggesting the methods of instruction, assessment, course topics, and workload to be used throughout the course. To do so, surveys and literature review were used. The literature review was conducted parallel to the survey, so that we can match the preferences of students with the findings in literature and, in the end, propose a solution which takes both into consideration.

A number of literature sources have been consulted, via Google Scholar and Scopus, with the aim of discovering effective ways of implementing cybersecurity in education. The main objective was finding literature which investigates successful cybersecurity courses at a university level and discusses the methods of instruction of such courses, their structure and curriculum. The queries used on Scopus were:

- TITLE-ABS-KEY (cybersecurity AND (education OR educational) AND methods AND university)
- TITLE-ABS-KEY (teaching AND cybersecurity AND education AND (university OR college))

A survey was also used to answer Sub-question 1. It was intended to help gain insights into students' preferences in terms of teaching, assessment, workload, attendance and the topics in the course. In the first section informed consent was obtained from participants, allowing them to decide whether they feel comfortable participating in the research. Participants were made aware of their right to withdraw from the study, as well as how their data would be used. Additionally, they were given the exact purpose of the survey and how their contribution would impact the progress in this field of research. The second section was used in order to understand students' preferences in terms of educational methods, attendance, assessment, workload and topics of the course and answer Sub-question 1. The final section addressed Sub-question 2 and investigated cybersecurity awareness (section 3.2).

Firstly, in order to gain insight into suitable methods to integrate cybersecurity in the curriculum of the Business Information Technology programme, several brainstorm sessions were conducted. The outcome of those served as input for the survey. The aim was to gather ideas from Business Information Technology students and learn more about their preferred methods of education. The sessions were carried out with two students in a mostly informal setting, where participants were students acquainted with the Business Information Technology curriculum. The researcher was also involved in the discussion, by actively suggesting ideas along with participants and supporting the process. The ideas proposed by students in the discussion were used to construct several questions which survey participants had to answer. During the discussion teaching online or in-person was discussed and consequently the survey also investigated which of those two methods is preferred by students. Participants in the brainstorm sessions had interesting propositions as to the methods of teaching. While some suggested having a pre-recorded set of lectures, others suggested lectures on campus. Therefore, in the survey we wanted to understand which of these options are more desirable or suitable to the student population. Survey participants were given several methods of teaching to choose from based on their preferences for education online or in-person. For instance, if a student selected that they want to participate in education on campus, then they chose among several different options; lecture, tutorial, project-based learning and workshops, with the possibility to select more than one answer. Alternatively, those who chose online education selected between online tutorials, online lectures and a pre-recorded set of lectures, with the ability to select more than one answer. If the participant selected "hybrid" as their desired method of teaching, then they chose among all of the above. A Chi-square test of independence was chosen with 5% level of significance to investigate the potential correlation between preferred methods of teaching (online/in-person) and study programme. The reason for choosing this test was the nature of the data and the need to test a correlation between categorical variables.

The null and alternative hypotheses are as follows:

- H0: There is no correlation between the two variables.
- H1: There is a relationship between the two variables.

Examination and assessment are also important aspects of the integration of the course. For this reason, the survey investigated to what extent students are in favour of several different methods of grading. The survey provided four different grading options, including multiple choice examination, report writing, conducting presentations and completing graded exercises. Below each of these four options, participants had to specify their level of agreement with two statements on a 7-point Likert scale. In order to allow for a comprehensive evaluation of each assessment method, the first statement related to the suitability of the method of grading and the second one investigated whether the participant believes this can result in fair grading.

The next step was to evaluate students' preferences in terms of course attendance. In this multiple choice question participants could choose between enforcing mandatory presence in all classes or alternatively having to attend only some or no activities in the course.

Afterwards, the workload and duration of the cybersecurity course were discussed. Participants were presented with four options, each one representing the time (in hours) needed per week for the successful completion of the course, as well as the activities which the student would dedicate time to. In this way, we learned which methods of teaching students believe to be manageable, within the given time.

Additionally, it is crucial to identify the most valuable skills students need to obtain as a result of the course. This approach also helps concretely establish the study objectives, so that the course is effective in providing up-to-date and comprehensive education. Relevant cybersecurity skills and topics were found in literature. At the same time, the topics students believe should be included in the course were investigated in the survey. In one of the last questions, participants were presented with a set of topics and were given the opportunity to indicate their level of agreement with including each topic in the curriculum on a 7-point Likert scale, form Strongly Disagree to Strongly Agree (Appendix A). This allowed us to understand not only which topics students believe are suitable for the course, but also which subjects participants think they can benefit from learning. In order to understand which topics students believed were most appropriate for the course, bar charts were created to see the most frequently chosen item on the 7-point Likert scale. The same procedure was used when determining the most preferred methods of assessment.

3.2. Sub-question 2

In order to answer sub-question 2, the current level of cybersecurity awareness of Business Information Technology students had to be determined.

For the measurement of cybersecurity awareness, a suitable scale had to be selected. Upon consulting literature and researching several scientific methods, the Security Behaviour Intentions Scale (SeBIS) was chosen. The scale is created in 2015 by Serge Egelman and Eyal Peer, supporting the assessment of cybersecurity user-behaviours [21]. This measurement was an integral part of the survey process. According to the work of Egelman and Peer, cybersecurity awareness can be evaluated through measuring device securement, proactive awareness, password generation, and updating behaviours [21]. The scale consists of 16 statements, measuring these constructs, to which respondents specify their level of agreement on a 5-point Likert scale. Additionally, the Human Aspects of Information Security Questionnaire (HAIS-Q) [22] was considered for the measurement of cybersecurity awareness. However, when evaluating both of these measures, the SeBIS scale fit better the context of the research and the research population. Although the Human Aspects of Information Security Questionnaire (HAIS-Q) gives important insight into security behaviours and information security awareness, it had a focus on cybersecurity in the workplace and was conducted among working people in Australia [22]. Therefore, some of the elements of the HAIS-Q questionnaire, such as "While I am at work I shouldn't access certain websites" or "I can't be fired for something I post on social media" were not a good fit for the purpose of this research [22]. However, the focal point of this research is education and our research population consists of university students. The SeBIS, on the other hand, covered important cybersecurity behaviours, which should undoubtedly be evaluated among a student population, such as caution prior to visiting website or links, software updates and privacy over one's devices [21].

Conducting regression analysis was intended to establish whether there is a relation between one's age and level of cybersecurity awareness. Cybersecurity awareness was inputted as the dependent variable. The independent variable was age. The null hypothesis stated that there is no correlation between the two variables. The alternative hypothesis stated the variables are correlated.

- H0: There is no correlation between the two variables.
- H1: There is a relationship between the two variables.

The chosen level of significance was 5%.

In order to test whether one's preferred methods of teaching and their cybersecurity awareness score are correlated, the sample was split in half based on the mean cybersecurity score. Then we investigated the preferences of those who scored above and alternatively those who scored below the mean.

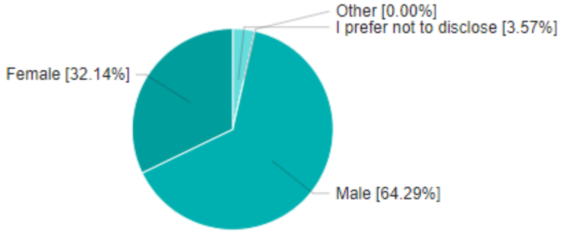


Fig. 1. Research population.

4 RESULTS

Upon obtaining permission from the Ethics Committee to continue with this research, the survey was distributed to bachelors and masters Business Information Technology students. This was done digitally, via email. Among the research population there were 10 women and 18 men, while 1 preferred not to disclose their sex (Fig. 1).

The total number of participants was 29, with 20 currently enrolled in the bachelors programme, 8 following the masters programme and 1 enrolled in another programme. There were 3 additional responses which were not taken into consideration due to incompleteness. The responses of students from other study programmes were excluded in the data analysis, in order to be able to answer the main research objective.

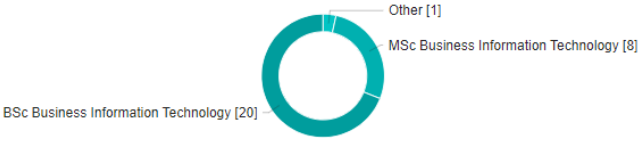


Fig. 2. Research population.

Scientific articles were found on Scopus as well as Google Scholar. The mostly highly cited works were scanned first, however, the date of publication was also taken into consideration, to ensure relevant information is gathered. Firstly, research began on Scopus, where the search:

- TITLE-ABS-KEY (cybersecurity AND (education OR educational) AND methods AND university)

was used. This search gave 42 results, 13 of which proved to be relevant for the research objectives. The second one:

- TITLE-ABS-KEY (teaching AND cybersecurity AND education AND (university OR college))

was slightly different from the first one and yielded 88 results, where several interesting articles also surfaced: [25], [3], [4], [9]. The above mentioned articles gave useful insight into the topic. Table 1 and Table 2 illustrate what the most prominent research findings were and the contribution of literature.

4.1 Sub-question 1

This section covers the data and insights gathered from the conducted literature review and surveys, in relation to constructing the cybersecurity course.

4.1.1. Online or in-person teaching

The survey results indicate students have a strong preference for a combination of online and in-person teaching (Fig. 3). The Chi-square test of independence conducted on the variables study and preference for online or in-person teaching returns a p-value of 0.1043 and Chi-square test statistic of 7.6729 and does not indicate a statistically significant relationship between the two variables. It is interesting to note, however, that that none of masters students chose fully online teaching. Among bachelors students 3 selected online teaching. Nevertheless, for the entire study population hybrid methods of education are still most desirable.

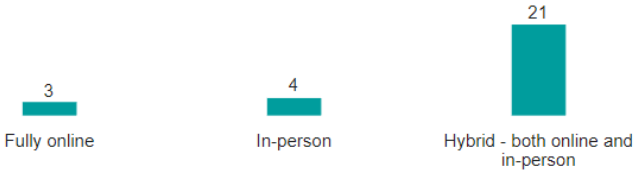


Fig. 3. Teaching preferences of BIT students.

4.1.2 Methods of education

Identifying suitable methods of teaching cybersecurity to university students is an essential step of constructing the course.

	Methods of education
[30], [16], [15], [3], [11], [4], [28]	Hands-on learning and labs
[26], [2]	Peer instruction and peer learning
[3], [4]	Project-based learning
[28], [19]	Adversarial thinking
[27]	Learning through cloud computing platforms
[11]	Gamification

Table 1. Main findings in literature - methods of teaching.

The consulted literature proposed many different methods of teaching cybersecurity. However, hands-on learning, practical courses and lab exercises were distinguished as the most commonly suggested methods in the considered scientific literature [30], [16], [28], [15], [3], [11], [4]. Participants in our survey also demonstrate a preference for practical methods of teaching such as tutorials, workshops and project-based learning. Paper [30] suggests developing hands-on labs helps students easily and quickly process information. The practical approach to teaching cybersecurity also engages students' attention and allows for the integration of real-world cybersecurity issues in education [30]. The authors further outline the benefits of the use of an online learning environment, where students can, among other, practice the executing Denial of Service (DoS) attacks and the exploitation of servers [30]. At the same time, hands-on labs and exercises can be integrated with textbook materials [15]. Practice connected to real-world cybersecurity issues can increase the effectiveness of cybersecurity training [15]. Additionally, standards set by the National Security Agency (NSA) and the US's Department of Homeland Security (DHS) suggest lab exercise should be included in cybersecurity curricula [3]. Hands-on learning experience can also be achieved by learning through cloud computing platforms, which can be executed both remote and in-person [27]. Elastic Compute Cloud (EC2) are virtual machines which can run all types of software [27]. Furthermore, the Amazon Web Services (AWS) represents a collection of remote computing services [27]. Research suggests this can be used when conducting laboratories for students, who can learn to write and execute code using Elastic Compute Cloud (EC2) instances [27]. This approach has many benefits, however, its main contribution is that it allows students to complete cybersecurity exercises and gain practice in a safe environment [27]. Additionally, it can equip students with a variety of cloud computing skills, as well as establishing a better understanding of cybersecurity concepts [27].

For the successful execution of these practical sessions, it is also important to provide students with the tools and knowledge needed to solve the exercises. For this reason, research emphasises starting the course with very basic beginner exercises, in order to help students gain an in-depth understanding of the study materials [28].

Adversarial thinking also surfaces in the search for suitable teaching methods, presenting an interesting opportunity for conducting practical sessions such as workshops [20], [19]. The concept refers to reasoning about certain topics in a context where there are bad actors, who are working against specific goals [20]. If used in the context of cybersecurity, this approach requires in-depth understanding of risks and vulnerabilities, as well as clarity regarding the goals and objectives when preventing cyber-attacks [20].

Another method proven to improve engagement and motivation is gamification [11]. This technique can be best implemented in practical sessions such as workshops or alternatively, it can be incorporated into exercises. Experience points (XP), awards and checkpoints can keep students motivated and help them effectively learn the subject [11].

An approach which also increases student engagement is incorporating competitive elements into the educational model can contribute to higher levels of engagement [28]. Research conducted among technical students at university proposes that young people can benefit from challenge and competition-based courses in cybersecurity trainings [28].

Peer instruction was also a commonly encountered method of education the literature search. Peer instruction can be defined as an interactive teaching method, which requires students to prepare prior to a lecture, answer certain questions and discuss these with their peers [2]. Such classes typically divide the lecture material into questions, focusing on the key takeaways, while it is also important to note that students are required to prepare for the class ahead of time [2]. This also allows students to discuss their answers to given tasks in a group, which has numerous advantages [2]. In the study of researchers from the University of New Orleans, using peer instruction has clear benefits on the effectiveness of student learning [2]. It can bring be beneficial in the development of technical skills and interest in the field of study [26]. Straub [26] also suggests that peer learning can be effective by allowing students to discuss materials together and ask questions. Additionally, using peer assessment for open assignments has several advantages [4]. For students, this can be helpful in thoroughly learning the study material and lead to increased levels of motivation [4].

However, conducting classes in person is not always feasible. Alternatively, universities may choose not do so and to opt for online teaching instead. If this is the case, researchers from New Zealand suggest that project-based learning is effective in for online teaching [4]. Project-based work can equip students with valuable soft skills such as teamwork, successful communication and presentation [4]. Universities can consider the possibility of involving industrial partners in case studies, so that the educational institution can mitigate the risk of obtaining an answer on the Internet, without solving the problem [4]. Reflective practices also present a prominent benefit for distance learning [4]. Research has found that reflection on one's strengths and weaknesses can in fact support the learning process [25].

As observed in the survey results, the most commonly chosen method of teaching among students is hybrid. Therefore, we will only evaluate the most desirable hybrid methods of instructions, disregarding the fully online and fully in-person options, due to the lack of interest in these methods. Additionally, the hybrid options include both the online and in-person options, therefore, we still get a comprehensive idea of the actual preferences of students. The most commonly chosen methods of hybrid education are illustrated in Figure 4. Participants could select more than one answer in this question.

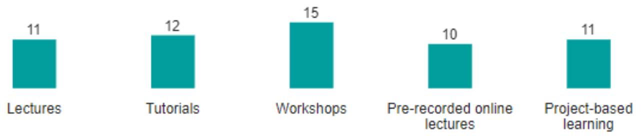


Fig. 4. Preferred methods of hybrid education of BIT students.

4.1.3 Content of the course

In this section we will cover the course topics which should be taught according to both students' preferences and scientific literature, as well as the key cybersecurity skills and abilities students need to possess.

	Course topics
[3], [19], [6]	Ethics
[3], [19], [6], [9], [14]	Risk management, analysing threats
[1], [5]	Phishing attempts
[1], [30]	Privacy
[1], [30]	Antivirus application
[1]	Sensitivity to cybersecurity problems
[1]	Encryption
[19]	Secure coding
[1]	Understanding key terminology

Table 2. Main findings in literature - the course topics.

Research in the field of cybersecurity education has identified the key topics which effective cybersecurity training entails. Researchers Alammari, Sohaib and Younes identify a comprehensive set of critical cybersecurity competencies, including prevention of unauthorised access, avoiding phishing attempts and malicious sites [1]. The research suggests that students need to possess a number of cybersecurity skills, among which are using unique passwords, using encryption, antivirus application and knowing how to avoid malicious content and phishing attempts [1]. This is also contained in the guidelines of the IEEE Computer Society, which suggest including areas such as network and human security in the cybersecurity course [3]. In this study, the majority of Business Information Technology students also are in favour of integrating the topic of encryption in the curriculum.

Recognising phishing emails and distinguishing them from non-malicious ones is also a key cybersecurity competency according to researchers, assessing cybersecurity knowledge among students at the Taif University in Saudi Arabia [5]. It appears that a large amount of Business Information Technology students also strongly believes that *cyber-attack prevention* should be in the course curriculum, along with the topic of *using firewalls*. Moreover, 82.14% of survey participants also select "Somewhat Agree" or higher regarding teaching the topic of *recognising phishing emails*.

Research on Delphi processes from 2014 also identifies various key cybersecurity topics [19]. Delphi processes consider the input of a set experts on a particular subject, in order to reach decisions [19]. Those key cybersecurity topics include privacy, ethics, integrity, secure coding and managing risks [19].

The abilities students need to have represent their application of skills in order to execute a task [1]. Researchers recommend that reading and understanding technical documents is one of these key abilities, students need to adapt [1]. Furthermore, a crucial cybersecurity ability is recognising cyber-threats as such, prior to their occurrence [1], along with analysing threats and attention to detail which are identified as key cybersecurity topics [19]. Researchers stress the importance of possessing the sensitivity to recognise the potential problem [1]. Research on the topic of using AI to improve cybersecurity education adds to this summary of key topics, by suggesting security of data, software, personnel and communications to be included [29]. 82.14% of survey participants also select "Somewhat Agree" or higher on the topic of having a *secure work and study environment*.

Additionally, the Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity proposes ways for constructing cybersecurity curricula. The document suggests an extensive list of topics and skills cybersecurity students need to possess [6]. However, several of them appear to be most relevant for the context of our research:

- **Human security**: personal data privacy and security
- **System security**: authentication, access control
- **Connection security**: connection attacks
- **Component security**: vulnerabilities of system components
- **Software security**: security requirements
- **Data security**: data integrity
- **Societal security**: cybercrime, cyber law, cyber ethics, policy
- **Organizational security**: risk management, law, ethics and compliance

It is worth noting that generally participants in our survey have agreed with all proposed topics (Appendix B). However, regarding the topic of *cybersecurity at the University of Twente*, there does not seem to be clear consensus among students that this is in fact a useful or relevant course topic. No significant differences are observed between the preferences of bachelors and masters students on this topic.

4.1.4. Attendance

The survey also brought up several interesting findings regarding the attendance requirements students prefer. Results demonstrate that 14 participants think no activities should be mandatory, while 12 believe some should be. However, this preference seems to differ between study programmes. The results show that more than half of masters students believe some activities or classes should be mandatory, while for bachelors students this is slightly different, with only 36.84% agreeing that certain classes should be compulsory to attend.

	No classes should be mandatory.	**Some classes** should be mandatory.	**All classes** should be mandatory.
MSc Business Information Technology	*37.50%*	*50.00%*	*12.50%*
BSc Business Information Technology	*55.00%*	*40.00%*	*5.00%*

Table 3. BSc / MSc students' attendance preferences.

4.1.5. Workload

The survey results indicate that 37.04% of bachelors students choose to have a weekly workload of 45 minutes for a lecture and 2 hours for project-work, during the cybersecurity course. Additionally, the second most commonly chosen option was having a 4- or 5-hour practical activity (e.g. workshop) once every quarter, while spending around 2 hours on self-study per week. The same applies for masters students, where 41.67% choose 45 minutes for a lecture and 2 hours for project-work.

4.1.6. Methods of assessment

When plotting these survey findings on a bar plot, several conclusions can be drawn. Firstly, is appears Business Information Technology students believe that having a multiple choice exam results in fair grading. However, when asked about the suitability of such method, 9 disagree with implementing it. The data shows that the most suitable method of assessment in the cybersecurity course according to students is doing graded exercises in a tutorial. 20 students agree that this assessment method is suitable. However, there is no clear consensus that this method can result in fair grading. The data does show, however, that students generally believe that having an assignment and conducting a group presentation or writing a group report is suitable for the course and can results in fair grading. Only two participants disagree that a report is a suitable or fair method of assessment.

4.2 Sub-question 2

This section covers the data and insights gathered from the conducted survey, in relation to the level of cybersecurity awareness among Business Information Technology students.

One of the assumptions which needs to be met when conducting regression analysis is that there is a linear relationship between the variables. However, when plotting the variables age and cybersecurity awareness score it became clear that they are not linearly related. It did not appear that the score increases nor decreases based on a participant's age. Therefore, the data does not suggest that one's level of cybersecurity awareness may be correlated to their age.

Afterwards, the correlation between cybersecurity awareness and preferred teaching methods was examined. In order to test this the sample was split in half, based on the mean cybersecurity awareness score. The maximum score a participant could obtain on the cybersecurity awareness scale was 80. A higher score would indicate a higher level of cybersecurity awareness. The mean cybersecurity score among all participants was 60.78. Those who have a cybersecurity awareness score above the mean, have most commonly chosen tutorials, workshops and project-based learning. Alternatively, those who scored below the mean preferred pre-recorded online lectures, as well as in-person lectures. This showed that there is indeed a correlation between one's preferred method of teaching and their level of cybersecurity awareness.

Finally, the potential correlation between sex and cybersecurity awareness were investigated. This was also done by splitting the sample in two parts, based on the mean cybersecurity score. The data does not suggest any clear correlation between these two variables.

5 RESULTS AND DISCUSSION

Based on the survey findings, a hybrid method of teaching would be most appropriate and effective for the Business Information Technology population. Combining online and in-person activities can provide students with a flexible schedule which suits their needs. However, the results showed for masters students fully online education is not desirable and this should be taken into consideration when creating the curriculum. Overall, ensuring a mix of various activities can be very beneficial for the learning process.

On the topic of attendance preferences there have been several interesting findings. Masters students choose that some classes should be mandatory, whereas bachelors students prefer no mandatory attendance policy altogether. This can help create a course tailored differently to bachelors and masters students. For instance, bachelors students can have a more flexible schedule with fewer compulsory activities. However, it is also important to reason about the effectiveness of such a course. When no mandatory attendance is present students may feel less inclined to attend classes. For this reason, it seems that enforcing mandatory attendance for some of the course activities remains reasonable.

A combination of lectures, workshops and tutorials can be beneficial for the learning progress of students. Those are not only among the most commonly chosen methods of education according to students, but are also recognised as highly effective in scientific literature. Group work and practical exercises are an essential element of the course, in order to promote the learning process and increase engagement. Involving gamification and competitive elements in the methods of teaching presents a very interesting opportunity to ensure students are engaged in the study process.

But it is also important to consider how we can use the findings from the cybersecurity awareness evaluation. It became evident that there is no correlation between variable such as age and sex and one's cybersecurity awareness. Therefore, it appears that the proposed methods can be implemented on all students with the intention of raising the overall cybersecurity awareness among them. At the same time, as mentioned above, the results demonstrate a correlation between a participant's cybersecurity awareness and their preferred methods of education. This finding is significant because it shows the ways in which students with different levels of awareness are willing to study the topic of cybersecurity. This can be used in implementing a more tailored method of education, which takes into consideration what a student's level of knowledge is and the most suitable method of teaching for them.

6 CONCLUSION

This research was conducted with the purpose of investigating the current level of cybersecurity awareness among Business Information Technology students at the University of Twente and proposing a way of cybersecurity education in the programme.

6.1 Sub-question 1

Research findings indicate that both bachelors and masters students prefer a combination of online and in-person education. Additionally, the most commonly preferred methods of teaching are workshops, tutorials and project-based learning. These methods of instruction are also recognised as effective in the considered scientific literature. Therefore, we propose combining these method of instruction to create an effective and flexible cybersecurity course. Additionally, efforts can be made to increase the engagement of students in the course, which in turn can also increase the effectiveness of education. Challenges and competition-based activities can help create a more diverse study programme and higher engagement, which can support the learning process.

The topics of *cyber-attack prevention*, *use of firewalls*, recognising *phishing emails*, *having a secure work and study environment*, and *encryption* have been chosen among students most frequently. Combining these subjects with *ethics*, *privacy* and *risk management* can also ensure relevant and up-to-date education, which provides students with some of the key competencies in the field.

Additionally, majority of students prefer graded group exercises as a form of assessment along with group assignments, report-writing and presenting. Peer assessment can be utilised in the report writing assignments, in order to promote better and more effective learning.

Regarding the duration of the course, participants in the research have indicated the most appropriate and manageable workload for the course would include one 45-minute lecture and 2 hours for project work per week. This workload appears to be sufficient for students to progress and develop cybersecurity skills, especially considering the implementation of project-work, which has been recognised as effective by scientific literature. Some of these activities should to be compulsory, however, not all of them should have a mandatory attendance policy, according to research participants.

6.2 Sub-question 2

In order to address the second research question regarding the current level of cybersecurity awareness among Business Information Technology students, the Security Behavior Intentions Scale (SeBIS) has been used in a survey distributed among all students in the programme. The results of this survey component indicated that those who have a higher cybersecurity awareness also preferred workshops, tutorials and project-based learning. On the other hand, the data does not suggest that variables like age, or sex influence cybersecurity awareness.

6.3 Effectively integrating cybersecurity in education

Overall, it appears that integrating cybersecurity in education can be challenging in ensuring a flexible, yet effective and useful course. For this purpose, above we suggest several ways of increasing the engagement of students and diversifying the programme. At this moment in time the research indicates the most suitable way of teaching cybersecurity is one which tackles relevant issues and topics, through various different hands-on exercises and activities. These methods can be used to increase the level of cybersecurity awareness among the entire Business Information Technology student population.

The insights gathered throughout this research can be valuable for the University of Twente and the Business Information Technology programme committee, to assist the successful integration of a cybersecurity course in the curriculum. This study also provides insight into the correlation between cybersecurity awareness and preferred methods of education which may be of interest in the further development of the course curriculum. Furthermore, higher educational institutions can implement the findings of this research by using the proposed methods of teaching to raise the level of cybersecurity awareness among their students.

7 LIMITATIONS AND FURTHER WORK

The short timeframe of this research project posed limitations to the research, especially during data gathering. Although in an ideal scenario a larger proportion of the Business Information Technology population would be involved in the study, in practice this was very challenging within the given time. Another potentially problematic aspect of the research was that the number of bachelors students participated in the study was higher than the number of masters student. Thus, in order to implement this method of teaching within the Business Information Technology programme it is best to evaluate the opinions of a larger sample of students.

To effectively assess the implications of cybersecurity education on the Business Information Technology student population it would be necessary to measure cybersecurity awareness again, to detect any potential changes among those who have participated in the cybersecurity course.

In the further development of this cybersecurity course, we additionally propose conducting a brainstorm session with the participation of professors involved in the Business Information Technology programme, cybersecurity professionals and module coordinators. We strongly believe such discussion can bring forward many valuable ideas and expand the possibilities for integrating cybersecurity in the curriculum. Furthermore, it can contribute to developing a concrete plan for the smooth and effective integration of the course.

ACKNOWLEDGEMENTS

I would like to thank the members of the BOZ (Office for Educational Affairs) at the University of Twente who kindly agreed to help in the distribution of the survey, as well as all students who participated in the research.

REFERENCES

[1] Abdullah Alammari, Osama Sohaib, Sayed Younes. 2022. Developing and evaluating cybersecurity competencies for students in computing programs. PeerJ Computer Science 8:e827 https://doi.org/10.7717/peerj-cs.827

[2] Ifran Ahmed and Vassil Roussev, 2018. Peer Instruction Teaching Methodology for Cybersecurity Education. *IEEE Security & Privacy*, 16, 4, 88-91. https://doi.org/10.1109/MSP.2018.3111242.

[3] Saed Alrabaee, Mousa Al-Kfairy, Ezedin Barka. 2022. Efforts and Suggestions for Improving Cybersecurity Education. *IEEE Global Engineering Education Conference (EDUCON).* 1161-1168. https://doi.org/10.1109/EDUCON52537.2022.9766653

[4] Ali Ahmed, Karsten Lundqvist, Craig Watterson, Nilufar Baghaei. 2020. Teaching Cyber-Security for Distance Learners: A reflective Study. In *IEEE Frontiers in Education Conference (FIE),* 1-7. https://doi.org/10.1109/FIE44824.2020.9274062.

[5] Althobaiti, Maha M. 2021. Assessing user susceptibility and awareness of cybersecurity threats. *Intelligent Automation & Soft Computing* 28, 1, https://doi.org/10.32604/iasc.2021.016660

[6] Association for Computing Machinery, IEEE Computer Society, Association for Information Systems Special Interest Group on Information Security and Privacy, International Federation for Information Processing Technical Committee on Information Security Education. 2017. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.

[7] A. Bendovschi. 2015. Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 28, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

[8] A. Benveniste. "Zoom settles 'zoombombing' and data privacy lawsuit for $85 million." 2021. Available: https://edition.cnn.com/2021/08/01/tech/zoom-privacy-settlement/index.html

[9] Tom Crick, James H. Davenport, Alastair Irons, Tom Prickett. 2019. A UK Case Study on Cybersecurity Education and Accreditation. *49th Annual Frontiers in Education Conference (FIE 2019),* 16 pages. https://doi.org/10.48550/arXiv.1906.09584

[10] Eric C. K. Cheng, Tianchong Wang. 2022. Institutional Strategies for Cybersecurity in Higher Educational Institutions. *Information*, 13. https://doi.org/10.3390/info13040192

[11] John Grady Hill, Abhinav Mohanty, Pooja Murarisetty, Ngoc Nguyen, Julio Bahamón, Harini Ramaprasad, Meera Sridhar. 2022. Criminal Investigations: An InteractiveExperience to Improve Student Engagement and Achievement in Cybersecurity courses. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education* V. 1, 7 pages https://doi.org/10.1145/3478431.3499417.

[12] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu and P. Laplante. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *Technology and Society Magazine*, 30(1), 28-38. https://doi.org/10.1109/MTS.2011.940293

[13] J. Jang-Jaccard, S. Nepal. A survey of emerging threats in cybersecurity. 2014. *Journal of Computer and System Sciences*, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005.

[14] Keith S. Jones, Akbar Siami Namin, Miriam Armstrong. 2018. The core cyber defense knowledge and skills and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Trans. Comput. Educ.* 18, 3, Article 11, 12 pages. https://doi.org/10.1145/3152893

[15] Matthew E. Luallen, and Jean-Philippe Labruyere. 2013. Developing a Critical Infrastructure and Control Systems Cybersecurity Curriculum. *46th Hawaii International Conference on System Sciences*. 1782-1791. https://doi.org/10.1109/HICSS.2013.176

[16] Akhtar Lodgher, Jeong Yang, Ummugul Bulut. 2018. An Innovative Modular Approach of Teaching Cybersecurity Across Computing Curricula. *IEEE Frontiers in Education Conference (FIE)*. 1-5. https://doi.org/10.1109/FIE.2018.8659040.

[17] T. Longstaff, J. Ellis, S. Hernan, H. Lipson, R. McMillan, L. Pesante, D. Simmel. 1998. Security of the Internet. Available: https://resources.sei.cmu.edu/asset_files/specialreport/1996_003_001_496597.pdf

[18] Ministry of Justice and Security. 2021. Cyber Security Assessment Netherlands. Available: https://securitydelta.nl/media/com_hsd/report/431/document/CSBN2021-EN-02.pdf

[19] Geet Parekh, David DeLatte, Geoffrey Herman, Linda Olivia, Dhananjay Phatak, Travis Scheponik, Alan Sherman. 2017. Identifying core concepts of cybersecurity: results of two Delphi processes. In *IEEE Transactions on Education*, 1-10. https://doi.org/10.1109/TE.2017.2715174.

[20] Geet Parekh, David DeLatte, Geoffrey Herman, Linda Olivia, Dhananjay Phatak, Travis Scheponik, Alan Sherman. 2016. How students reason about cybersecurity concepts. *IEEE Frontiers in Education Conference (FIE)*. 1-5.

[21] E. Peer, S. Egelman. Scaling the security wall: Developing a security behavior intentions scale (SeBIS). Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15), 2873–2882. April 2015. https://doi.org/10.1145/2702123.2702249

[22] Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, Tara Zwaans. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computer & Security*. 66. https://doi.org/10.1016/j.cose.2017.01.004

[23] Ibrahim Rhhal, Ibtissam Makdoun, Ghita Mezzour, Imane Khaouja, Kathleen Carley, Ismail Kassou. 2019. Analyzing Cybersceurity Job Market Needs in Morocco by Mining Job Ads. *IEEE Global Engineering Education Conference (EDUCON)*. 535-543.

[24] A. A. N. Rahman, H. I. Sairi, M. A. N. Zizi, F. Khalid. The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, 10(5), pp. 378-382. 2020. http://dx.doi.org/10.18178/ijiet.2020.10.5.1393

[25] Valdemar Svabensky, Richard Weiss, Jack Cook, Jan Vykopal, Pavel Celeda, Jens Mache, Radoslav Chudovsky and Ankur Chattopadhyay. 2022. Evaluating two approaches to assessing student progress in cybersecurity exercises. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education*, 7 pages. https://doi.org/10.1145/3478431.3499414

[26] Jeremy Straub. 2019 Assessment of the Educational Benefits Produced by Peer Learning Activities in Cybersecurity. *ASEE Annual Conference & Exposition, Tampa, Florida*. https://doi.org/10.18260/1-2--32131

[27] Khaled Salah, Mohmmad Hammoud and Sherali Zeadally. 2015. Teaching Cybersecurity Using the Cloud. *IEEE Transactions on Learning Technologies*, 8, 4, 383-392. https://doi.org/10.1109/TLT.2015.2424692.

[28] Shuzhen Tian, Xiaojun Wu. 2015. Student-centered learning in cybersecurity in summer semester. *IEEE Frontiers in Education Conference (FIE)*. https://doi.org/10.1109/FIE.2015.7344154

[29] Roumen Trifonov & Ognian Nakov & Slavcho Manolov & Georgi Tsochev & Galya Pavlova. (2020). Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods. 1-4. https://doi.org/10.1109/ICAI50593.2020.9311333.

[30] Lixin Wang, Jianhua Yang, Peng-Jun Wan. 2020. Educational modules and research surveys on critical cybersecurity topics. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1177/1550147720954678

[31] Jacob Willem Abraham Witsenboer, Klaas Sijtsma, Fedde Scheele. 2022. Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education*. 186. https://doi.org/10.1016/j.compedu.2022.104536.

[32] University of Oxford. “Researchers identify negative impacts of cyber attacks.” 2018. Available: https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks

[33] P. Valdes-Dalpena. “Volkswagen hack: 3 million customers have had their information stolen,” 2021. Available: https://edition.cnn.com/2021/06/11/cars/vw-audi-hack-customer-information/index.html

APPENDIX A.

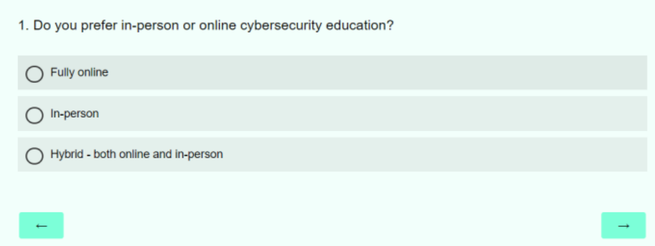
In this section the course topics among which students chose in the survey are listed. Each of these topics had to be evaluated by survey participants on a 7-point Likert scale.

1. Preventing cyber-attacks
2. How to ensure a secure work/study environment?
3. Two factors authentication, how it works and why we use it
4. How the UT addresses common cyber-threats and how students can identify them?
5. How to recognise phishing emails
6. Use of firewalls
7. Encryption

APPENDIX B.

In the section several different types of survey questions can be seen.

1. Online/in-person education



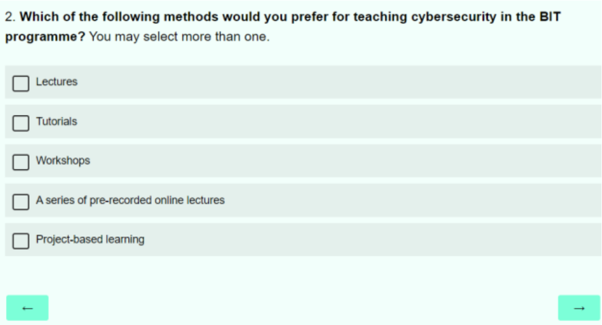
1. Do you prefer in-person or online cybersecurity education?

○ Fully online

○ In-person

○ Hybrid - both online and in-person

2. Preferred hybrid methods of teaching:



2. **Which of the following methods would you prefer for teaching cybersecurity in the BIT programme?** You may select more than one.

□ Lectures

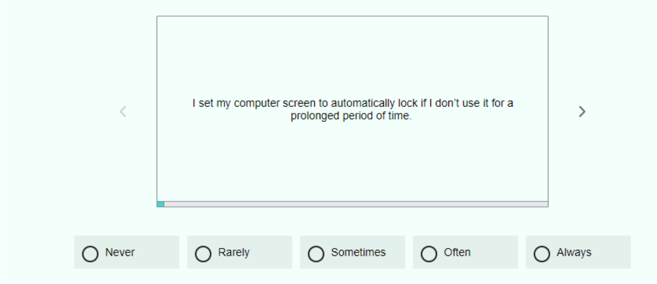
□ Tutorials

□ Workshops

□ A series of pre-recorded online lectures

□ Project-based learning

3. Cybersecurity awareness:



I set my computer screen to automatically lock if I don't use it for a prolonged period of time.