PeerJ Computer Science

Developing and evaluating cybersecurity competencies for students in computing programs

Abdullah Alammari[1], Osama Sohaib[2] and Sayed Younes[1,3]

[1] Faculty of Education, Curriculums and Teaching Department, Umm Al-Qura University, Makkah, Saudi Arabia
[2] Faculty of Engineering and IT, University of Technology Sydney, Sydney, Australia
[3] College of Education, Al Azhar University, Educational Technology Dept, Cairo, Egypt

ABSTRACT

Changes due to technological development in the workplace are putting pressure on academia to keep pace with the changing nature of work. Due to the growing need for cybersecurity professionals, universities improve their cybersecurity programs to develop qualified cybersecurity competencies. The purpose of this study is to validate the cybersecurity knowledge, skills, and abilities (KSAs) competencies of cybersecurity degree programs using a fuzzy linguistic group decision-making method. This study shows that cybersecurity knowledge is essential, along with technical skills and human abilities for cybersecurity professionals.

Subjects Computational Linguistics, Computer Education, Social Computing
Keywords Computer education, Cybersecurity competency, Multi-criteria

INTRODUCTION

Information technology professionals lacking cybersecurity competencies can result in considerable financial, information and intellectual property losses for organizations worldwide (*Choi, Levy & Hovav, 2013*). *Draganidis & Mentzas (2006)* described competency as distinguishable, obvious, and quantifiable skill, knowledge, ability or/and possessing any other deployment-related attributes (such as behaviour, attitude, physical competence) essential for the execution within a specific context. Cybersecurity competencies are a dynamic combination of knowledge, skills, and abilities (KSAs) (*Parrish et al., 2018*).

Alavi & Leidner (2001) consider knowledge an acceptable belief by which an individual's ability to create a practical action method is enhanced. As per *Prager, Moran & Sanchez (1997)*, the power to perform mental and physical acts required by tasks is referred to as 'ability'. *Boyatzis & Kolb (1995)* stated that skill is a well-organized and goal-directed behaviour accomplished with effort and learned through practice.

Cybersecurity professionals can significantly prevent cyber threats with the implemented policies (*Paulsen et al., 2012*). In addition, cybersecurity professionals need to possess an advanced level of combined knowledge, skills, and abilities (KSAs) competencies to establish and implement the tools and technologies (*Paulsen et al., 2012*; *National Institute of Standards and Technology (NIST), 2014*). On the other hand, not all IT professionals are

Submitted 15 July 2021
Accepted 2 December 2021
Published 17 January 2022

Corresponding author
Osama Sohaib,
Osama.Sohaib@uts.edu.au

Academic editor
Muhammad Asif

Additional Information and Declarations can be found on page 16

DOI 10.7717/peerj-cs.827

How to cite this article Alammari A, Sohaib O, Younes S. 2022. Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Comput. Sci.* **8**:e827 http://doi.org/10.7717/peerj-cs.827

cybersecurity experts. IT professionals may not be familiar with the modern concepts and lack expertise in cybersecurity and information technology (IT) (*Happ, Melzer & Steffgen, 2016*; *Hazari, Hargrave & Clenney, 2008*).

Cybersecurity competencies of computing professionals continue to be an emerging issue (*Behrens, Alberts & Ruefle, 2012*; *Toth & Klein, 2013*). Moreover, there is a strong likelihood of advanced and persistent threats on the organizations, resulting from which the confidential data, valuable resources and critical targets are at risk (*Marchetti et al., 2016*). In addition, despite technical cybersecurity controls, the IT professionals can negate them because they usually don't possess cybersecurity competencies (*Behrens, Alberts & Ruefle, 2012*; *Al Neaimi, Ranginya & Lutaaya, 2015*). One of the most effective vectors to gain access to a secure system is none. Still, phishing attacks since the IT professionals lack the required cybersecurity competencies to a large extent (*Bowen, Devarajan & Stolfo, 2012*). Likewise, new vulnerabilities are also expected to introduce new technologies, highlighting the need to evaluate cybersecurity competencies (*Pittenger, 2016*) consistently and precisely. Therefore, recent studies have exhibited the need to assess skills and competencies (*Grus et al., 2016*).

Implementing cybersecurity can uplift any organization's security and financial prosperity (*Hoffman & Branlat, 2016*). In addition, cybersecurity competencies play a vital role in adherence to the regulations, laws and Constitutional requirements (*National Institute of Standards and Technology (NIST), 2014*). *Behrens, Alberts & Ruefle (2012)* developed a Competency Lifecycle Roadmap (CLR) for sustainable cybersecurity competencies. *Toth & Klein (2013)* suggested that all IT professionals are necessitated to acquire essential cybersecurity competencies. However, the dynamic technological changes in the professional workplace call for changes in academic curriculum and strategies. It is important to note that skilled cyber-specialized personnel are essential for mitigating or combating cyber-attacks targeting critical infrastructure. *ABET, Inc (2018)* continue to develop new criteria for a cybersecurity degree program. ABET is a not-for-profit international organization that accredits computing and engineering programs.

However, acquiring skills involves a decision-making process. Cybersecurity experts face several challenges related to cyber systems. This represents a multiple criteria decision-making (MCDM) issue in assessing cybersecurity competencies. Cybersecurity risk management and assessment is a multi-criteria decision problem (*Ganin et al., 2020*). MCDM involves the selection of the most appropriate alternative from among various available options with multiple criteria. Several methods could be used for addressing any MCDM issue; however, the effectiveness of each method may vary. The choice of the best method for addressing any MCDM issue is not straightforward due to the ever-increasing complexity of organizational decision-making. Hence, the incorporation of group decision-making strategies in MCDM yields multi-criteria group decision-making (MCGDM). It allows taking decisions involving all members of the groups (*Ma, Lu & Zhang, 2010*).

Therefore, individuals must perform decision-making in their day-to-day activities to process qualitative information available in a natural or artificial language. Humans commonly perform linguistic decision-making by computing with words (CW) technique (*Martinez, Ruan & Herrera, 2010*). Experts have put forward several models for linguistic decision-making. But, the processing of information through the CW technique for linguistic decision-making becomes complex when it comes to group decision-making. This may be attributed to the nature of linguistic modelling and the linguistic computational model involved in the process. *Herrera & Martinez (2000)* were the first ones to introduce the 2-tuple linguistic model, which is extensively employed for CW during group decision-making. This technique offers the advantages of retention of info throughout the CW processes.

Moreover, it allows decision processes to yield error-free and accurate linguistic outcomes. The effectiveness of the 2-tuple model linguistic model was reported for handling data containing uniform and symmetrical distribution of linguistic expressions (*Li et al., 2017*; *Rodríguez & Martinez, 2013*). Various applications are based on the 2-tuple semantic as indicated in earlier research (*Li et al., 2017*; *Rodríguez & Martinez, 2013*). This study involves the application of the fuzzy linguistic 2-tuple model. This selection may be attributed to the features offered by this model like fuzzy representation, comprehensive and flexible nature and precise decision-making (*Rodríguez & Martinez, 2013*).

Therefore, this paper adopted a novel 2-tuple fuzzy linguistic group decision-making TOPSIS method developed by *Sohaib et al. (2019)* to evaluate the cybersecurity required competencies in higher education IT programs. This study follows the work of *Behrens, Alberts & Ruefle (2012)*, *Toth & Klein (2013)* and *Nilsen (2017)*, who proposed cybersecurity knowledge, skills, and abilities (KSAs) competencies in detail. Thus, this study evaluates the cybersecurity knowledge, skills, and abilities (KSAs) required for cybersecurity competencies. The research question this study addresses. What are the different cybersecurity KSAs criteria needed to meet the cybersecurity competencies in higher education cybersecurity programs in Saudi Arabia?

The paper is organized as follows. The following section provides the literature review of the key concepts studied. Then the study method is presented, followed by the case study analysis. The results are then presented, followed by a discussion and conclusion.

LITERATURE REVIEW

Cybersecurity education models

According to the *ACM Joint Task Force on Cybersecurity Education (2017)*, there is a need to develop a comprehensive curriculum in cybersecurity education. The primary purpose of cybersecurity programs is to equip the future generation with cybersecurity knowledge and experience (*ACM/IEEE-CS Joint Task Force on Computing Curricula, 2013*; *ACM/IEEE-CS Task Group on Information Technology Curricula, 2017*; *ABET, Inc, 2018*).

The US National Institute of Standards and Technology (*National Institute of Standards and Technology (NIST), 2017*) commenced a framework for cybersecurity workforce through collaborative efforts by the educational sector, public and private sectors. The framework also outlines the knowledge, skill, and ability (KSA) essential for organizations and entities who wish to implement cybersecurity in their workplace. Knowledge, Skills, and Abilities (KSAs) define the attributes and traits necessary for individuals and organizations to deliver the required level of performance. Such characteristics may be evident in expertise, skills and experience, acquired through performance-based learning.

ABET, Inc (2018) has specified the accreditation criteria for undergraduate cybersecurity degree programs in addition to current accreditation criteria specified for computer science, Information Systems (IS) and IT programs. ABET is an American private organization serving as an accreditation board for approving various intermediate education programs in engineering, computing and technology. ABET specifies and modifies the criteria to be fulfilled by university programs. ABET, Inc (2017) and ABET, Inc (2018) has contributed to incorporating cybersecurity in existing programs in Saudi Universities. ABET introduced the Engineering Accreditation Commission (EAC) program criteria and made all cybersecurity engineering programs mandatory to meet the Computing Accreditation Commission (CAC) standards besides other existing requirements. CAC criteria make it compulsory to equip the curriculum with rules and activities that ensure safe computing (ABET, Inc, 2017; Parrish et al., 2018).

However, ABET, Inc (2018) also acknowledge the concept of developing independent cybersecurity programs. The measures issued by ABET, Inc (2018) has made it mandatory for undergraduate programs to incorporate cybersecurity principles. In addition, ACM ACM Joint Task Force on Cybersecurity Education (2017) specified comprehensive curriculum criteria in cybersecurity education.

Cybersecurity competencies

Envisioning the future of cybersecurity is not a simple task. The current cybersecurity activities have been highlighted in the ACM Joint Task Force on Cybersecurity Education (2017) and Institute of Information Security Professionals (2018). Therefore, every IT degree program must incorporate cybersecurity. Hence, the significance of learning about cybersecurity becomes evident from implementing cybersecurity in multiple disciplines, including science, engineering, and business *etc*. This also implies that some knowledge and experience of cybersecurity is essential for every workplace.

The NIST Cybersecurity Framework contains five synchronized and continuous functions: identity, protect, detect, respond, and recover. These functions are fulfilled by having cybersecurity competencies (National Institute of Standards and Technology (NIST), 2014). Moreover, there should be focused measures of competency assessments; hence, the focus of the evaluation must be the functional or technical competencies (Succar, Sher & Williams, 2013). It is worth mentioning that the competency level needs to be established while evaluating an individual (Garavan & McGuire, 2001). Precisely, the experts may design the competency assessments to determine the superior performance level (expert) or a threshold level (minimum competency) (Shahidi et al., 2015). Therefore, all IT users must acquire cybersecurity necessary competency, a dynamic combination of cybersecurity knowledge, cybersecurity skills, and cybersecurity abilities (Parrish et al., 2018; Nilsen, 2017).

Knowledge, skills, and abilities (KSAs)

All the combined KSAs formulate competencies, which reveals the performance level of the combined KSAs (Chen et al., 2014). The specific actions needed to complete job tasks are directly associated with the KSAs (Baker, 2013). Therefore, the competency gaps

Table 1 Cybersecurity knowledge competencies.

Cybersecurity knowledge competencies	References
Access control Antivirus software Cyber threats and vulnerabilities Email encryption and use File permissions Incident reporting Information privacy Strong password and reuse Phishing Policy compliance Sensitive information	*Gross & Rosson (2007)*; *Ifinedo (2012)* *Parsons et al. (2014)*; *Dye & Scarfone (2014)*; *Ives, Walsh & Schneider (2004)*; *Nilsen (2017)*; *Safa, Von Solms & Furnell (2016)*

involving additional training will be identified once the KSAs are determined (*Chen et al., 2014*). Besides discovering competency gaps, *Baker (2013)* expressed that the measures determining the level of task performance are none other than the KSAs.

Different jobs relate to several KSAs in the context of cybersecurity (*Campbell, O'Rourke & Bunting, 2015*). Specific jobs require a low level of combined KSAs. In contrast, some need a high level of combined KSAs (*Lu et al., 2015*). Moreover, KSAs are not certainly exchangeable between job functions or career fields (*Conklin, Cline & Roosa, 2014*). Hence, while determining cybersecurity KSAs, \an initial set of KSAs for all job functions must be the prime area of concentration (*Chen et al., 2014*; *Conklin, Cline & Roosa, 2014*).

Cybersecurity knowledge

According to *Alavi & Leidner (2001)*, knowledge is defined as a reasonable belief that strengthens an individual's capacity to initiate suitable action. Knowledge can be split into tacit knowledge and explicit knowledge. According to their explanation, the knowledge that can be taught is known as explicit knowledge. In contrast, the knowledge acquired from experience is not easily exchangeable is referred to as tacit knowledge.

As per *Parsons et al. (2014)*, the following cybersecurity knowledge units were described for the students, namely: incident reporting, email use, Internet use, information handling, password management, mobile computing, strong passwords and social networking site use. At the same time, the following IT professionals cybersecurity knowledge units were recorded by *Gross & Rosson (2007)*, *i.e.*, antivirus software, access control, cybersecurity responsibilities, cyber vulnerabilities, cyber threats, file permissions, email encryption, policy compliance, phishing, privacy and sensitive information *etc.* Another cybersecurity knowledge unit is believed to be password reuse (*Ives, Walsh & Schneider, 2004*). Table 1 shows cybersecurity knowledge competencies.

Cybersecurity skills

The skills required to avoid a loss to IT infrastructure through the Internet are cybersecurity skills (*Carlton & Levy, 2015*). Cybersecurity skills can be associated with the required tasks or specific sets of actions (*Conklin, Cline & Roosa, 2014*). Acquisition of skill to prevent unauthorized access to an IT is critical to ensure access control within an organization. It is realized when the individual controls systems (*Gross & Rosson, 2007*; *Ifinedo, 2012*). Unauthorized access to sensitive information can only be reduced through proper access control.

The protection offered by antivirus software can be maximized by gaining skill in antivirus software (*Dhepe & Akarte, 2013*). The automatic update facility of antivirus software is activated by many organizations (*i.e.*, auto-update configurations). However, organizations can come across the times where the update is required to be facilitated by a cyber-security expert (*Dhepe & Akarte, 2013*). Students must be well aware of handling an antivirus application, especially when the computer system notifies the user to update the antivirus application (*Gross & Rosson, 2007*).

The students should know the cookie usage skills because they may have unencrypted sensitive information to track the activity (*DISA, 2015*). Moreover, the students should be familiar with their Internet browser setting to manage their web cookie storage policy (*DISA, 2015*). Students must have practical skills in email security (*DISA, 2015*; *Parsons et al., 2014*). They must know the skill to configure the Email in such a way that prevents leaking confidential data (*DISA, 2015*; *Parsons et al., 2014*). Therefore, students must illustrate how they can control the downloading of malicious items besides carrying out the task of exchanging private information with the help of encryption (*Barlow et al., 2013*; *DISA, 2015*). Moreover, digitally signing emails must also be demonstrated to provide added security (*DISA, 2015*; *Foster et al., 2015*). In addition, the task of scanning all email attachments before use must also be illustrated (*DISA, 2015*).

Students must also acknowledge the skills in cybersecurity incident reporting to ensure denial of service to an unauthorized person (*Imgraben, Engelbrecht & Choo, 2014*; *Parsons et al., 2014*). Students need to know the personal mistakes required to be reported besides identifying suspicious individuals involved in security breaches (*Parsons et al., 2014*).

During internet connectivity at the workplace, the students must prevent opening the links to malicious Websites (*Carlton & Levy, 2015*). Hence, students must responsibly demonstrate that they will not click on malicious pop-up windows (*DISA, 2015*; *Kumar, Chaudhary & Kumar, 2015*). In addition, students ought to have skills in preventing such activities, through which the systems become vulnerable to malicious code (*Barlow et al., 2013*; *DISA, 2015*). As a result of this malicious code, hackers can access the system/network, corrupt the files, and erase hard drives (*DISA, 2015*). The worms, viruses, spyware, Trojan horses and scripts are included among the examples of malicious code (*DISA, 2015*). While most students do freelance works, carry out online studies or perform telework, it is appreciated to have skills in securely operating mobile computing devices (*DISA, 2015*). The task of locking the mobile computing device when inactive must also be demonstrated by the students (*Parsons et al., 2014*). Skills required by students are the stoppage of password reuse (*Ives, Walsh & Schneider, 2004*). Concerning confidential data, the skill to prevent phishing attempts is obligatory for the students (*Carlton & Levy, 2015*; *DISA, 2015*; *Furnell, Tsaganidi & Phippen, 2008*). As exposed in the literature review, students need several cybersecurity skills (Table 2).

Table 2 **Cybersecurity skills competencies.**

Cybersecurity skills competencies	References

Preventing unauthorized access	Gross & Rosson (2007);
	Ifinedo (2012)
	Parsons et al. (2014);
	DISA (2015);
	Deshpande et al. (2015)
	Carlton et al. (2015);
	Nilsen (2017);

Using an antivirus application	
Managing cookie settings and usage	
Using incident reporting	
Avoiding suspicious and malicious sites	
Securely operating mobile devices	
Using unique passwords	
Avoiding a phishing attempt	
Securely using social networking sites	
Physically protecting information systems	
Using encryption	
Creating strong passwords	

Cybersecurity abilities

The physical or/and mental ability to apply skills to execute a task is called the ability (Tobey, 2015). Likewise, the foundation for skills and knowledge application is the ability (Prager, Moran & Sanchez, 1997). The primary cybersecurity abilities are written communication, near vision, advanced written comprehension, written expression and problem sensitivity (Campbell, O’Rourke & Bunting, 2015; Trippe et al., 2014) Nilsen, 2017). The close-up viewing defined for objects almost sixty centimetres or less than two feet from the eyes is described as near-vision or accurate near vision (Colman, 2015). Researchers believe that a cybersecurity ability to view computer screens also corresponds to the near vision concept. According to them, the ability to express when something goes wrong or is likely to go wrong is known as problem sensitivity (Nilsen, 2017). It is nothing to do with problem-solving. Instead, it is only to identify a problem (Trippe et al., 2014).

The ability to read and comprehend government or/and technical documents refers to advanced written comprehension (Trippe et al., 2014). Researchers recommend advanced written understanding as one of the cybersecurity abilities, which can read cybersecurity policies and guidance. The broadcast of a message in written symbols is known as written communication (Terkan, 2013, p. 149). According to Poteet (1980), a visible representation of feelings, thoughts, and ideas is described as written expression, where the writer’s language symbols are used to record or communicate. The experts conclude that written expression is guided as cybersecurity ability. The potential investigators could transcribe cybersecurity incident reports besides speaking to a cybersecurity contact for the relevant issues.

Siponen, Mahmood & Pahnila (2014) support the argument that an entry-level step to follow and implement cybersecurity procedures and policies is the ability to understand cybersecurity terminology. According to the findings of Hagen & Albrechtsen (2009), the ability to anticipate, monitor and respond to cybersecurity challenges are the three fundamental abilities, such as awareness, knowledge and behaviour are needed to measure the information security intervention. Table 3 shows cybersecurity abilities criteria.

Table 3 Cybersecurity abilities competencies.

Cybersecurity abilities	References
Oral comprehension Near vision Problem sensitivity Written communication Written expression	*Campbell, O'Rourke & Bunting (2015)*; *Trippe et al. (2014)*; *Nilsen (2017)*;

Fuzzy linguistic decision-making methods

Acquiring knowledge, skills, and abilities involves a decision-making process. According to *Ganin et al. (2020)*, cybersecurity risk management and assessment is a multi-criteria decision problem. Experts have proposed several techniques for complex decision-making issues in the practical world, particularly those involving multiple choices. The selection of a specific method depends on the nature of info available to decision-making individuals. Dominance technique proves effective in case of lack of information available to decision-makers while maximin or maximax technique is used when pessimistic or optimistic information is available.

Moreover, the selection of the method is further categorized into sub-categories in case of the availability of attributes. The conjunctive and disjunctive methods are usually employed if a standard level of information relevant to each attribute is available. However, simple additive weighting (SAW), analytic hierarchy process (AHP), TOPSIS (a technique for order preference by similarity to ideal solution) and the ELECTRE (elimination and choice expressing the reality) method *etc.* are used when ordinal or cardinal scales are used in the analysis of attribute weights (*Lu et al., 2007*). Although various MCDM techniques are available, the TOPSIS method has been extensively used by previous researchers (*Sohaib et al., 2019*). The main features offered by TOPSIS that make it favourable are that it is based on the logic of an individual's preference; moreover, it makes use of simple computation processes and considers the ideal and the anti-ideal solutions concurrently (*Shih, Shyur & Lee, 2007*). TOPSIS has made it possible to consider criteria and alternatives together (the situation in our study), which is not the case with pairwise comparison techniques. Besides these benefits and the extensive popularity of TOPSIS, it has been our preference because of the features of extensions applicable in fuzzy environments. In this proposal, we will highlight and demonstrate the effectiveness of this feature concerning the ranking of alternatives.

The central underlying concept behind the TOPSIS method is that an alternative is deemed the best one. It needs to correspond to the ideal positive solution and to be contrary to the negative ideal solution besides adhering to the subsequently mentioned steps (*Hwang & Yoon, 1981*).

Fuzzy group decision-making methods

Due to the complex nature of the issues faced in the practical world, it is imperative to consider various viewpoints when solving a case. Usually, a group of experts give their opinion, which serves as the solution to the concerned problem; the process is commonly known as multi-criteria group decision making (MCGDM). Previously, group decision-making involved the participation of multiple experts $E = \{e_1, e_2, \ldots, e_k\} (k \geq 2)$ who present their opinion regarding alternative X to solve the issue at hand. The alternative was chosen in two steps, including the aggregation and exploitation stages. The aggregation stage involves using an aggregation operator to compile all the views expressed by different experts. The aggregation operator merges all this data to develop a collective preference matrix containing all the proposed solutions to the concerned problem. This is followed by the exploitation stage, which involves analyzing the joint preference matrix and choosing the most appropriate alternative from all the available options proposed for solving the problem (*Rodrıguez, & Martinez, 2013*). *Sohaib et al. (2019)* explain the use of a general scheme which is only possible when experts give their preference from among various available alternatives through the employment of fuzzy linguistic variables. The steps mentioned below are involved in the development of solution scheme (*Rodrıguez, & Martinez, 2013*):

- The first step involves the selection of a set of linguistic terms that contains semantics. Consequently, linguistics implies meaning and is deemed linguistic descriptors, which experts analyze to determine their preferences from various available alternatives and assign weights to criteria weights in light of their knowledge and experience.
- The subsequent step involves selecting an aggregation operator that compiles all the preferences given by individual experts to present collective linguistic information.
- The final step involves the selection of the best alternative(s) among the available ones.

The aggregation phase involves the application of various models of linguistic computing, including the models proposed by *Degani & Bortolan, (1988)*, *Delgado, Verdegay & Vila (1993)*, *Herrera & Martinez (2000)*. On the other hand, the exploitation phase involves the application of conventional MCDM methods.

A 2-Tuple fuzzy linguistic group TOPSIS model

TOPSIS techniques and the fuzzy extensions offered by this technique are known for their extensive use in various applications (*Ju, Wang & You, 2015*; *Lu et al., 2016*; *Wei, 2010*). However, this technique fails to meet the computing with words (CW) criteria due to the inaccuracy of the linguistic domain or non-linguistic outcomes indicated by applying the domain of the preferences for distances instead of the linguistic domain. Hence, this drawback called for proposing a novel linguistic TOPSIS model. Such a model is presented in this study. Such a model uses a 2-tuple linguistic model wherein the fuzzy linguistic variables are used to assign weightings to each criterion. Thus, this proposed model satisfies the CW criteria since it involves the use of appropriate syntax and semantics for preferences and distances, leading to precise, flexible and understandable linguistic outcomes.

Let's consider a set of alternatives $A = A_1, A_2, \ldots, A_m$ for the criteria $C = C_1, C_2, \ldots, C_n$ being evaluated by a set of decision-makers $D = D_1, D_2, \ldots, D_k$. Moreover, considering that the set of the linguistic term for assigning weightage to criteria is $U = u_1, u_2, \ldots, u_p$ andconsidering that the set of the linguistic term for the analysis of alternatives is $S = s_1, s_2, \ldots, s_t$. Also, consider that the set of the linguistic term to determine the similarity

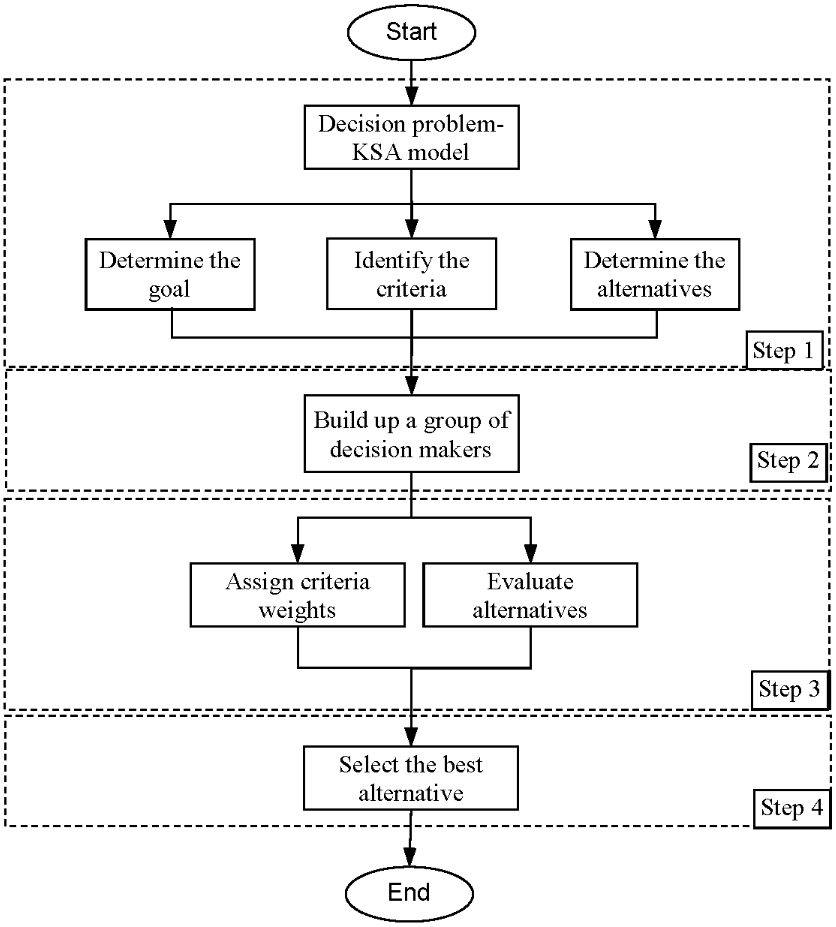

Figure 1 **The proposed methodology.**

Full-size DOI: 10.7717/peerjcs.827/fig-1

of a linguistic term s_p with another linguistic term $s_r$be $S' = l_1, l_2, \ldots, l_{t'}$ and the set of the linguistic term to determine the distance of the linguistic term s_p from another linguistic term (s_r) $isS'' = r_1, r_2, \ldots, r_{t''}$. Let's consider a weight vector $U_t = \left(u_j^t\right)^T_{1*n}$ for which the decision-maker $D_t \in D$ proposes a linguistic value preference $u_j^t \in U$ concerning criteria $C_j \in C$. Moreover, consider the decision matrix $X_t = \left(r_{ij}^t\right)_{m*n}$ for which the proposed linguistic value preference is $r_{ij}^t \in S$ as per the decision-maker $D_t \in D$ considering the alternative $A_i \in A$ and the criteria $C_j \in C$. In such a case, all decision-makers are supposed to carry an equal level of significance. The steps involved in the advanced version of TOPSIS have been mentioned subsequently. Please see Sohaib et al. (2019) previous work on a novel 2-tuple fuzzy TOPSIS method discussed in detail.

METHOD

Figure 1 shows the proposed methodology consists of the following four steps.

Table 4 **Linguistic terms for criteria weighting the criteria.**

Symbol	Linguistic term	Fuzzy number
u_1	Very low (VL)	(0, 0, 0.1)
u_2	Low (L)	(0, 0.1, 0.3)
u_3	Medium low (ML)	(0.1, 0.3, 0.5)
u_4	Medium (M)	(0.3, 0.5, 0.7)
u_5	Medium high (MH)	(0.5, 0.7, 0.9)
u_6	High (H)	(0.7, 0.9, 1.0)
u_7	Very high (VH)	(0.9, 1.0, 1.0)

Step 1

This research aimed to evaluate the cybersecurity KSAs competencies for computing students of Saudi higher education institutions. The KSA model was used to measure a core set of required cybersecurity knowledge, skills, and abilities (KSAs) essential as cybersecurity competencies (*Nilsen, 2017*). The three criteria and twenty-seven sub-criteria were determined based on the KSA model. The alternatives are University A (Uni. A), University B (Uni. B) and University C (Uni C.). The criteria structure of the KSA competencies is discussed in the above sections.

Step 2

In the second step, three professors from three different universities attempted to collectively evaluate cybersecurity knowledge, skills, and abilities essential as cybersecurity competencies. A Delphi method using a ’consensus rule’ was used to improve the process of decision making. Delphi method consensus rule in fuzzy group decision-making aims at making a mutual agreement about an opinion (*Lu et al., 2007*). Thus, a consensus rule was approved using a questionnaire to build interdisciplinary understanding about the different views.

Step 3

In step 3, the relative importance of criteria and the alternatives under study was weighted using linguistic terms. The linguistic terms for weighting the criteria and the alternatives are presented in Tables 4 and 5. Triangular fuzzy numbers denote the membership functions of all linguistic terms for the sake of simplicity. Finally, Table 6 shows the linguistic variables for measuring the distance to choose the best alternative.

Step 4

Finally, in step 4, the novel 2-tuple group TOPSIS method (*Sohaib et al., 2019*) was used to obtain the desired ranking. Out of the three alternatives, the best alternative was selected as the ideal strategy based on the maximum closeness degree to the ideal solution.

CASE ANALYSIS AND IMPLEMENTATION

As discussed in the research methodology section, cybersecurity competencies criteria in higher education programs in Saudi Universities were evaluated. Three professors teaching

Table 5 Linguistic terms for rating the alternatives.

Symbol	Linguistic term	Fuzzy number
s_1	Very poor (VP)	(0, 0, 1)
s_2	Poor (P)	(0, 1, 3)
s_3	Medium poor (MP)	(1, 3, 5)
s_4	Fair (F)	(3, 5, 7)
s_5	Medium good (MG)	(5, 7, 9)
s_6	Good (G)	(7, 9, 10)
s_7	Very good (VG)	(9, 10, 10)

Table 6 Linguistic terms for calculating the distance.

Symbol	Linguistic term	Fuzzy number
r_1	Equal	(0, 0, 1)
r_2	Almost equal	(0, 1, 3)
r_3	A bit close	(1, 3, 5)
r_4	Neither close nor far	(3, 5, 7)
r_5	A bit far	(5, 7, 9)
r_6	Far	(7, 9, 10)
r_7	Far away	(9, 10, 10)

cybersecurity from three different institutions were invited to rank three alternatives (Uni. A, Uni. B, and Uni. C) of required cybersecurity knowledge, skills, and cybersecurity abilities vital to cybersecurity competencies. The name of the universities and the participants are preserved to maintain confidentiality. All three universities are based in Saudi Arabia. All experts have more than ten years of industry experience.

Criteria weights

The criteria weights and the linguistic terms as presented in Table 4; the experts' judgments have resulted in Table 7.

Alternative evaluation

Table 8 shows an alternative evaluation decision matrix was resulted using linguistic terms (Table 5).

Finally, the novel 2-tuple group TOPSIS method (reference) was applied to deliver a decision as discussed in step 4 of the research methodology. Table 9 shows the 2-tuple linguistic values. The 2-tuple arithmetic mean was to obtain collective values.

Table 10 shows the results of the 2-tuples evaluation matrix and their mean. In the experts' view, cybersecurity threats and vulnerabilities with a 2-tuple of (u_7, 0 in Table 9) are the most important criteria with the importance of Very High, followed by access control and policy compliance.

Table 7 Criteria weight matrix.

Criteria	Sub-criteria	DM1	DM2	DM3
Knowledge	Access control	VH	VH	H
	Antivirus software	MH	MH	M
	Cyber threats and vulnerabilities	VH	VH	VH
	Email encryption and use	H	VH	VH
	File permissions	ML	M	M
	Incident reporting	VH	H	VH
	Information privacy	H	MH	MH
	Strong password and reuse	H	H	H
	Phishing	VH	VH	VH
	Policy compliance	VH	H	VH
	Sensitive information	H	M	M
Skills	Preventing unauthorized access	VH	MH	H
	Using an antivirus application	M	MH	MH
	Managing cookie settings and usage	MH	MH	MH
	Using incident reporting	H	VH	H
	Avoiding suspicious and malicious sites	M	MH	M
	Securely operating mobile devices	MH	H	MH
	Creating and using unique passwords	VH	VH	VH
	Avoiding a phishing attempt	VH	H	VH
	Securely using social networking sites	M	ML	M
	Physically protecting information systems	M	MH	VH
	Using encryption	H	M	M
Abilities	Oral comprehension	M	ML	ML
	Near vision	ML	ML	ML
	Problem sensitivity	L	L	VL
	Written communication	ML	M	M
	Written expression	MH	H	MH

RESULTS

The distance of the alternatives to the negative ideal and the positive ideal solutions were calculated. All the criteria were benefits except problem sensitivity was considered only cost criteria. Table 11 shows the relative closeness degree of each alternative. The results show Uni. B. has the best cybersecurity KSA model as it has a "Far" distance from the anti-ideal solution. There is no need to perform any sensitivity analysis further, as the difference between closeness degrees of alternatives is substantial (*Sohaib et al., 2019*).

The result of this study demonstrates that Uni. B has the ideal cybersecurity knowledge, skill, and ability (KSA) model, followed by Uni. A. Knowledge, Skills, and Abilities (KSA) defines the attributes and traits essential for individuals and organizations to deliver the required level of cybersecurity competencies and performance. Hence, a practical cybersecurity education framework must accommodate all kinds of cybersecurity competencies as defined by KSAs competencies.

Table 8 **Alternative evaluation matrix.**

Criteria	Sub-criteria	Alternatives	DM1	DM2	DM3
Knowledge	Access control	Uni. A	MG	MG	MG
		Uni. B	G	MG	MG
		Uni. C	VG	MG	MG
	Antivirus software	Uni. A	F	F	F
		Uni. B	MG	MG	G
		Uni. C	VG	VG	G
	Cyber threats and vulnerabilities	Uni. A	VG	G	VG
		Uni. B	VG	VG	VG
		Uni. C	VG	G	G
	Email encryption and use	Uni. A	VG	VG	VG
		Uni. B	MG	G	MG
		Uni. C	F	F	G
	File permissions	Uni. A	P	MP	P
		Uni. B	F	MG	MG
		Uni. C	VG	VG	VG
	Incident reporting	Uni. A	MG	MG	MG
		Uni. B	G	MG	MG
		Uni. C	VG	MG	MG
	Information privacy	Uni. A	F	F	F
		Uni. B	MG	MG	G
		Uni. C	VG	VG	G
	Strong password and reuse	Uni. A	G	G	G
		Uni. B	MG	MG	MG
		Uni. C	MG	F	G
	Phishing	Uni. A	G	G	MG
		Uni. B	MG	MG	G
		Uni. C	G	G	G
	Policy compliance	Uni. A	G	VG	VG
		Uni. B	MG	G	MG
		Uni. C	MP	F	G
	Sensitive information	Uni. A	MG	MP	P
		Uni. B	VG	G	G
		Uni. C	VG	G	G
	Preventing unauthorized access	Uni. A	VG	VG	VG
		Uni. B	MP	MP	P
		Uni. C	F	F	F
	Using an antivirus application	Uni. A	VG	VG	VG
		Uni. B	F	MP	P
		Uni. C	F	F	MP
	Managing cookie settings and usage	Uni. A	VG	VG	G
		Uni. B	MP	P	VP
		Uni. C	MP	P	VP

(*continued on next page*)

Table 8 (*continued*)

Criteria	Sub-criteria	Alternatives	DM1	DM2	DM3
Skills	Using incident reporting	Uni. A	G	VG	G
		Uni. B	P	P	VG
		Uni. C	MP	MG	MP
	Avoiding suspicious and malicious sites	Uni. A	G	VG	F
		Uni. B	VP	VP	VG
		Uni. C	P	P	MP
	Securely operating mobile devices	Uni. A	G	G	F
		Uni. B	P	VP	VG
		Uni. C	P	P	G
	Using strong and unique passwords	Uni. A	G	G	G
		Uni. B	VG	VG	G
		Uni. C	VG	VG	MG
	Avoiding a phishing attempt	Uni. A	MG	MP	G
		Uni. B	F	F	MG
		Uni. C	G	G	G
	Securely using social networking sites	Uni. A	MG	MG	G
		Uni. B	G	G	VG
		Uni. C	G	MG	MG
	Physically protecting information systems	Uni. A	VG	MG	G
		Uni. B	G	G	P
		Uni. C	MG	MG	MG
	Using encryption	Uni. A	G	G	MG
		Uni. B	VG	G	G
		Uni. C	MG	MG	G
Abilities	Oral comprehension	Uni. A	P	MP	MG
		Uni. B	G	MG	MP
		Uni. C	G	G	F
	Near vision	Uni. A	P	MP	MG
		Uni. B	G	MG	MP
		Uni. C	G	G	F
	Problem sensitivity	Uni. A	MP	MP	P
		Uni. B	VP	VP	VP
		Uni. C	P	VP	P
	Written communication	Uni. A	MG	G	MG
		Uni. B	MP	P	MP
		Uni. C	P	MP	F
	Written expression	Uni. A	G	MG	G
		Uni. B	VP	VP	MP
		Uni. C	P	MP	F

Table 9 **The 2-tuples weights.**

Criteria	Sub-criteria	DM1	DM2	DM3
Knowledge	Access control	$(u_4,0)$	$(u_4,0)$	$(u_7,0)$
	Antivirus software	$(u_5,0)$	$(u_6,0)$	$(u_5,0)$
	Cyber threats and vulnerabilities	$(u_7,0)$	$(u_7,0)$	$(u_7,0)$
	Email encryption and use	$(u_6,0)$	$(u_7,0)$	$(u_6,0)$
	File permissions	$(u_6,0)$	$(u_4,0)$	$(u_4,0)$
	Incident reporting	$(u_7,0)$	$(u_6,0)$	$(u_7,0)$
	Information privacy	$(u_6,0)$	$(u_5,0)$	$(u_5,0)$
	Strong password and reuse	$(u_6,0)$	$(u_6,0)$	$(u_6,0)$
	Phishing	$(u_6,0)$	$(u_7,0)$	$(u_7,0)$
	Policy compliance	$(u_7,0)$	$(u_6,0)$	$(u_6,0)$
	Sensitive information	$(u_6,0)$	$(u_4,0)$	$(u_3,0)$
Skills	Preventing unauthorized access	$(u_6,0)$	$(u_5,0)$	$(u_6,0)$
	Using an antivirus software	$(u_6,0)$	$(u_6,0)$	$(u_5,0)$
	Managing cookie settings and usage	$(u_6,0)$	$(u_6,0)$	$(u_5,0)$
	Using incident reporting	$(u_7,0)$	$(u_5,0)$	$(u_7,0)$
	Avoiding suspicious and malicious sites	$(u_4,0)$	$(u_5,0)$	$(u_5,0)$
	Securely operating mobile devices	$(u_5,0)$	$(u_5,0)$	$(u_6,0)$
	Using unique and strong passwords	$(u_6,0)$	$(u_7,0)$	$(u_7,0)$
	Avoiding a phishing attempt	$(u_5,0)$	$(u_4,0)$	$(u_6,0)$
	Securely using social networking sites	$(u_5,0)$	$(u_5,0)$	$(u_3,0)$
	Physically protecting information systems	$(u_4,0)$	$(u_3,0)$	$(u_4,0)$
	Using encryption	$(u_7,0)$	$(u_4,0)$	$(u_6,0)$
		$(u_5,0)$	$(u_5,0)$	$(u_5,0)$
Abilities	Oral comprehension	$(u_4,0)$	$(u_3,0)$	$(u_7,0)$
	Near vision	$(u_3,0)$	$(u_3,0)$	$(u_7,0)$
	Problem sensitivity	$(u_2,0)$	$(u_2,0)$	$(u_4,0)$
	Written communication	$(u_4,0)$	$(u_6,0)$	$(u_4,0)$
	Written expression	$(u_2,0)$	$(u_4,0)$	$(u_2,0)$

DISCUSSIONS AND CONCLUSION

Cybersecurity competencies is a dynamic combination of knowledge, skills, and abilities (*Parrish et al., 2018*; *Nilsen, 2017*). Cybersecurity competencies focus on performance, which means knowledge alone doesn't guarantee a successful practising professional in cybersecurity. Technical skills along with human abilities are equally important as knowledge.

Due to the ever-evolving technology and the multidisciplinary field of cyberspace, it has become imperative to develop more comprehensive methodologies and training for equipping future individuals, organizations and institutes with the novel skills and expertise essential for practical implementation of cybersecurity. Cybersecurity is a multidisciplinary field of study covering various legal, human resource, moral and risk management factors. Hence, a helpful cybersecurity education framework needs to accommodate different kinds of competencies.

Table 10 **The aggregated 2-tuples of the decision matrix.**

Criteria	Sub-criteria	Alternatives	Mean
Knowledge	Access control	Uni. A	(s_7,-0.2)
		Uni. B	(s_2,0.4)
		Uni. C	(s_4,0)
	Antivirus software	Uni. A	(s_7,-0.2)
		Uni. B	(s_2,0.2)
		Uni. C	(s_3,0)
	Cyber vulnerabilities	Uni. A	(s_6,-0.4)
		Uni. B	(s_5, 0)
		Uni. C	(s_5,-0.2)
	Email encryption and use	Uni. A	(s_6,0.2)
		Uni. B	(s_4,0)
		Uni. C	(s_5,-0.2)
	File permissions	Uni. A	(s_6,0.4)
		Uni. B	(s_6,-0.4)
		Uni. C	(s_5,0.4)
	Email encryption and use	Uni. A	(s_2,0.4)
		Uni. B	(s_5,0)
		Uni. C	(s_7,-0.4)
	Incident reporting	Uni. A	(s_5,0.4)
		Uni. B	(s_6,0)
		Uni. C	(s_6,0.2)
	Information privacy	Uni. A	(s_4,0)
		Uni. B	(s_5,-0.2)
		Uni. C	(s_6,0.4)
	Strong password and reuse	Uni. A	(s_6,-0.4)
		Uni. B	(s_5,0.4)
		Uni. C	(s_5,0)
	Phishing	Uni. A	(s_7,-0.4)
		Uni. B	(s_7,-0.2)
		Uni. C	(s_2,0.4)
	Policy compliance	Uni. A	(s_4,0)
		Uni. B	(s_7,-0.2)
		Uni. C	(s_2,0.2)
	Sensitive information	Uni. A	(s_3,0)
		Uni. B	(s_6,0.4)
		Uni. C	(s_2,-0.2)
	Preventing unauthorized access	Uni. A	(s_7,-0.2)
		Uni. B	(s_2,0.4)
		Uni. C	(s_4,0)
	Using an antivirus software	Uni. A	(s_7,-0.2)
		Uni. B	(s_2,0.2)
		Uni. C	(s_3,0)

(*continued on next page*)

Table 10 (*continued*)

Criteria	Sub-criteria	Alternatives	Mean
Skills	Managing cookie settings and usage	Uni. A	$(s_6,0.4)$
		Uni. B	$(s_2,-0.2)$
		Uni. C	$(s_2,0)$
	Managing cookie settings and usage	Uni. A	$(s_4,0)$
		Uni. B	$(s_5,-0.2)$
		Uni. C	$(s_6,0.4)$
	Using incident reporting	Uni. A	$(s_6,-0.4)$
		Uni. B	$(s_5,0.4)$
		Uni. C	$(s_5,0)$
	Avoiding suspicious and malicious sites	Uni. A	$(s_6,-0.2)$
		Uni. B	$(s_6,-0.4)$
		Uni. C	$(s_6,-0.2)$
	Securely operating mobile devices	Uni. A	$(s_5,0)$
		Uni. B	$(s_7,-0.4)$
		Uni. C	$(s_7,-0.2)$
	Using unique and strong passwords	Uni. A	$(s_2,0.4)$
		Uni. B	$(s_4,0)$
		Uni. C	$(s_7,-0.2)$
	Avoiding a phishing attempt	Uni. A	$(s_2,0.2)$
		Uni. B	$(s_3,0)$
		Uni. C	$(s_6,0.4)$
	Securely using social networking sites	Uni. A	$(s_2,-0.2)$
		Uni. B	$(s_2,0)$
		Uni. C	$(s_6,-0.4)$
	Physically protecting information systems	Uni. A	$(s_3,-0.2)$
		Uni. B	$(s_3,0)$
		Uni. C	$(s_6,-0.2)$
	Using encryption	Uni. A	$(s_2,0.2)$
		Uni. B	$(s_3,0.4)$
		Uni. C	$(s_2,0.2)$
Abilities	Oral comprehension	Uni. A	$(s_6,-0.4)$
		Uni. B	$(s_3,-0.2)$
		Uni. C	$(s_3,0)$
	Near vision	Uni. A	$(s_6,-0.2)$
		Uni. B	$(s_2,0.2)$
		Uni. C	$(s_3,0.4)$
	Problem sensitivity	Uni. A	$(s_2,0.2)$
		Uni. B	$(s_2,-0.4)$
		Uni. C	$(s_1,0.4)$
	Written communication	Uni. A	$(s_7,-0.2)$
		Uni. B	$(s_2,0.2)$
		Uni. C	$(s_3,0)$
	Written expression	Uni. A	$(s_6,0.4)$
		Uni. B	$(s_2,-0.2)$
		Uni. C	$(s_2,0)$

Table 11 **Alternatives and their closeness degrees.**

Alternative	Closeness degree to the negative ideal solution	Linguistic term
Uni. A	(r_5,0.3)	A bit Far
Uni. B	(r_6,0.2)	Far
Uni. C	(r_4,-0.3)	Neither close nor far

The implications of this study include providing universities with a validated cybersecurity competencies model for creating cybersecurity assessments. The learning processes for cybersecurity key competencies should attain the three described knowledge, skills, and abilities (KSA) model objectives. The KSA model will also allow students to understand better cybersecurity jobs in a domain that is still undergoing various changes.

Furthermore, the implications of this study include establishing Saudi universities cybersecurity degree programs based on the Knowledge, Skills and Abilities (KSAs) model to meet the accreditation requirements such as *ABET, Inc (2017)* and *ABET, Inc (2018)*. The US *National Institute of Standards and Technology (NIST) (2017)*, *ACM Joint Task Force on Cybersecurity Education (2017)* and *ABET, Inc (2018)* have specified comprehensive criteria in cybersecurity education. It is also imperative for universities and higher education institutes to meet the specified criteria. Such criteria require universities to house a cybersecurity department to offer comprehensive programs with a curriculum covering many mandatory topics related to cybersecurity to equip the students with the Knowledge, Skills and Abilities (KSAs).

A potential limitation of this study includes the use of the Delphi method consists of three experts only. Future work should target in-depth interviews with the industry experts to identify more a comprehensive list of cybersecurity knowledge, skills, and abilities (KSAs).

ADDITIONAL INFORMATION AND DECLARATIONS

Funding

This work was supported by the Deanship of Scientific Research at Umm Al-Qura University, Saudi (Grant Code: DSR-UQU-A2-19-EDU-1-02-00002). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Grant Disclosures

The following grant information was disclosed by the authors:
The Deanship of Scientific Research at Umm Al-Qura University, Saudi: DSR-UQU-A2-19-EDU-1-02-00002.

Competing Interests

Osama Sohaib is serving as an Academic Editor for PeerJ Computer Science.

Author Contributions

- Abdullah Alammari conceived and designed the experiments, prepared figures and/or tables, authored or reviewed drafts of the paper, and approved the final draft.
- Osama Sohaib performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, authored or reviewed drafts of the paper, and approved the final draft.
- Sayed Younes analyzed the data, prepared figures and/or tables, authored or reviewed drafts of the paper, and approved the final draft.

Data Availability

The following information was supplied regarding data availability:

The raw data is available in the Supplemental File.

Supplemental Information

Supplemental information for this article can be found online at http://dx.doi.org/10.7717/peerj-cs.827#supplemental-information.

REFERENCES

ABET, Inc. 2017. Criteria for accrediting computing programs, effective for review during the 2019-20 accreditation cycle. *Available at https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2019-2020* (accessed on 06 May 2021).

ABET, Inc. 2018. ABET approves accreditation criteria for undergraduate cybersecurity programs. *Available at https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/* (accessed on 22 June 2021).

ACM/IEEE-CS Joint Task Force on Computing Curricula. 2013. Computer Science Curricula 2013. Technical Report. New York, Piscataway: ACM and IEEE (accessed on 15 May 2021).

ACM/IEEE-CS Task Group on Information Technology Curricula. 2017. Information Technology Curricula 2017. Technical Report. New York, Piscataway: ACM and IEEE (accessed on 14 May 2021).

ACM Joint Task Force on Cybersecurity Education. 2017. Cybersecurity curricula 2017 curriculum guidelines for post-secondary degree programs in cybersecurity, version 1.0. ACM, IEEE Computer Society, AIS SIGSEC, and IFIPS WG 11.8. *Available at https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf* .

Al Neaimi A, Ranginya T, Lutaaya P. 2015. A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics* **4(1)**:290–301 DOI 10.17781/P001502.

Alavi M, Leidner DE. 2001. Review: knowledge management and knowledge management systems: conceptual foundations and research issues. *MIS Quarterly* **25(1)**:107–136 DOI 10.2307/3250961.

Baker M. 2013. State of cyber workforce development. Pittsburgh: Software Engineering Institute, Carnegie Mellon University. *Available at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=83504* (accessed on 20 June 2021).

Barlow JB, Warkentin M, Ormond D, Dennis AR. 2013. Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & security* **39**:145–159.

Behrens S, Alberts C, Ruefle R. 2012. Competency lifecycle roadmap: toward performance readiness. Software Engineering Institute, Carnegie Mellon University. *Available at http://www.sei.cmu.edu/library/abstracts/reports/12tn020.cfm* (accessed on 21 May 2021).

Bowen B, Devarajan R, Stolfo S. 2012. Measuring the human factor of cyber security. *Homeland Security Affairs* **5(2)**:1–7.

Boyatzis RE, Kolb DA. 1995. From learning styles to learning skills: the executive skills profile. *Journal of Managerial Psychology* **10(5)**:3–17.

Campbell SG, O'Rourke P, Bunting MF. 2015. Identifying dimensions of cyber aptitude: the design of the cyber aptitude and talent assessment. In: *Proceedings of the human factors and ergonomics society annual meeting*. Los Angeles, California, 721–725.

Carlton M, Levy Y. 2015. Expert assessment of the top platform independent cybersecurity skills of non-IT professionals. In: *Proceedings of the 2015 IEEE SoutheastCon, Ft. Lauderdale, Florida*. Piscataway: IEEE, 1–6.

Carlton M, Levy Y, Ramim MM, Terrell SR. 2015. Development of the MyCyberSkills^{TM} iPad app: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills. In: *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC - Workshop on Information Security and Privacy (WISP) 2015, Ft. Worth, Texas.*

Chen T, Shore D, Zaccaro S, Dalal R, Tetrick L, Gorab A. 2014. An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy* **12(5)**:61–67.

Choi M, Levy Y, Hovav A. 2013. The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. In: *Proceedings of the pre-international conference of information systems (ICIS) SIGSEC - Workshop on information security and privacy (WISP) 2013*. Milan, Italy, 1–16.

Colman A. 2015. Near vision. A dictionary of psychology. *Available at http://www.oxfordreference.com/view/10.1093/acref/9780199657681.001.0001/acref-9780199657681-e-5379* (accessed on 01 June 2021).

Conklin WA, Cline RE, Roosa T. 2014. Re-engineering cybersecurity education in the US: an analysis of the critical factors. In: *Proceedings of the of the 2014 47th Hawaii international conference on system sciences*. Waikoloa, HI, 2006–2014.

Defense Information Systems Agency (DISA). 2015. Cyber awareness challenge version 2.0. *Available at https://www.disa.mil/NewsandEvents/Training* (accessed on 12 July 2020).

Degani R, Bortolan G. 1988. The problem of linguistic approximation in clinical decision making. *International Journal of Approximate Reasoning* **2(2)**:143–162 DOI 10.1016/0888-613X(88)90105-3.

Delgado M, Verdegay JL, Vila MA. 1993. On aggregation operations of linguistic labels. *International Journal of Intelligent Systems* **8(3)**:351–370 DOI 10.1002/int.4550080303.

Deshpande PM, Joshi Sand Dewan, P, Murthy K, Mohania M, Agrawal S. 2015. The Mask of ZoRRo: preventing information leakage from documents. *Knowledge and Information Systems* **45(3)**:705–730 DOI 10.1007/s10115-014-0811-6.

Dhepe Y, Akarte S. 2013. Security issues facing computer users: an overview. *International Journal of Computer Science and Applications* **6(2)**:263–267.

Draganidis F, Mentzas G. 2006. Competency based management: a review of systems and approaches. *Information Management & Computer Security* **14(1)**:51–64 DOI 10.1108/09685220610648373.

Dye SM, Scarfone K. 2014. A standard for developing secure mobile applications. *Computer Standards & Interfaces* **36(3)**:524–530 DOI 10.1016/j.csi.2013.09.005.

Foster ID, Larson J, Masich M, Snoeren AC, Savage S, Levchenko K. 2015. Security by any other name: on the effectiveness of provider-based email security. In: *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*. New York: ACM, 450–464.

Furnell S, Tsaganidi V, Phippen A. 2008. Security beliefs and barriers for novice Internet users. *Computers & Security*. 235–240.

Ganin AA, Quach P, Panwar M, Collier ZA, Keisler JM, Marchese D, Linkov I. 2020. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis* **40(1)**:183–199 DOI 10.1111/risa.12891.

Garavan TN, McGuire D. 2001. Competencies and workplace learning: some reflections on the rhetoric and the reality. *Journal of Workplace Learning* **13(4)**:144–164 DOI 10.1108/13665620110391097.

Gross JB, Rosson MB. 2007. Looking for trouble: understanding end-user security management. In: *Proceedings of the 2007 symposium on computer human interaction for the management of information technology*. Cambridge, MA, 1–10.

Grus CL, Falender C, NA Fouad, Lavelle AK. 2016. A culture of competence: a survey of implementation of competency-based education and assessment. *Training and Education in Professional Psychology* **10(4)**:198–205 DOI 10.1037/tep0000126.

Hagen J, Albrechtsen E. 2009. Effects on employees' information security abilities by e-learning. *Information Management & Computer Security* **17(5)**:388–407 DOI 10.1108/09685220911006687.

Happ C, Melzer A, Steffgen G. 2016. Trick with treat–reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior* **61**:372–377 DOI 10.1016/j.chb.2016.03.026.

Hazari S, Hargrave W, Clenney B. 2008. An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy & Security* **4(4)**:3–20.

Herrera F, Martinez L. 2000. A 2-tuple fuzzy linguistic representation model for computing with words. *IEEE Transactions on Fuzzy Systems* **8(6)**:746–752 DOI 10.1109/91.890332.

Hoffman RR, Branlat M. 2016. To know or not to know, what is the need? *IEEE Intelligent Systems* **31(1)**:78–82.

Hwang C-L, Yoon K. 1981. *Multiple attribute decision making: methods and applications*. New York: Springer-Verlag.

Ifinedo P. 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* **31(1)**:83–95 DOI 10.1016/j.cose.2011.10.007.

Imgraben J, Engelbrecht A, Choo KKR. 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology* **33(12)**:1347–1360 DOI 10.1080/0144929X.2014.934286.

Institute of Information Security Professionals. 2018. IISP skills framework. *Available at https://apmg-international.com/sites/default/files/documents/products/iisp_skills_framework_v1_0.pdf* (accessed on 03 March 2021).

Ives B, Walsh KR, Schneider H. 2004. The domino effect of password reuse. *Communications of the ACM* **47(4)**:75–78.

Ju YB, Wang AH, You TH. 2015. Emergency alternative evaluation and selection based on ANP, DEMATEL, and TL-TOPSIS. *Natural Hazards* **75**:S347–S379 DOI 10.1007/s11069-014-1077-8.

Kumar A, Chaudhary M, Kumar N. 2015. Social engineering threats and awareness: a survey. *European Journal of Advances in Engineering and Technology* **2(11)**:15–19.

Li C-C, Dong Y, Herrera F, Herrera-Viedma E, Martínez L. 2017. Personalized individual semantics in computing with words for supporting linguistic group decision making. An application on consensus reaching. *Information Fusion* **33**:29–40 DOI 10.1016/j.inffus.2016.04.005.

Lu B, Guo X, Luo N, Chen G. 2015. Corporate blogging and job performance: effects of work-related and wonwork-related participation. *Journal of Management Information Systems* **32(4)**:285–314.

Lu C, You JX, Liu HC, Li P. 2016. Health-care waste treatment technology selection using the interval 2-tuple induced TOPSIS Method. *International Journal of Environmental Research and Public Health* **13(6)**:562 DOI 10.3390/ijerph13060562.

Lu J, Zhang G, Ruan D, Wu F. 2007. *Multi-objective group decision making: methods, software and applications with fuzzy set techniques*. London: Imperial College Press.

Ma J, Lu J, Zhang G. 2010. Decider: a fuzzy multi-criteria group decision support system. *Knowledge-Based Systems* **23(1)**:23–31 DOI 10.1016/j.knosys.2009.07.006.

Marchetti M, Pierazzi F, Colajanni M, Guido A. 2016. Analysis of high volumes of network traffic for advanced persistent threat detection. *Computer Networks* **109**:127–141 DOI 10.1016/j.comnet.2016.05.018.

Martinez L, Ruan D, Herrera F. 2010. Computing with words in decision support systems: an overview on models and applications. *International Journal of Computational Intelligence Systems* **3(4)**:382–395.

National Institute of Standards and Technology (NIST). 2014. Framework for improving critical infrastructure cybersecurity. *Available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf* (accessed on 07 June 2021).

National Institute of Standards and Technology (NIST). 2017. National initiative for cybersecurity education, national cybersecurity workforce framework. *Available at https://www.nist.gov/file/359261* (accessed on 06 June 2021).

Nilsen R. 2017. Measuring cybersecurity competency: an exploratory investigation of the cybersecurity knowledge, skills, and abilities necessary for organizational network access privileges. Doctoral dissertation, Nova Southeastern University, Davine, FL, USA. *Available at https://nsuworks.nova.edu/gscis./1017*.

Parrish A, Impagliazzo J, Raj RK, Santos H, Asghar MR, Jøsang A, Stavrou E , et al. 2018. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In: *Proceedings companion of the 23rd annual ACM conference on innovation and technology in computer science education*. New York: ACM, 36–54.

Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security* **42**:165–176 DOI 10.1016/j.cose.2013.12.003.

Paulsen C, McDuffie E, Newhouse W, Toth P. 2012. NICE: creating a cybersecurity workforce and aware public. *IEEE Security & Privacy* **10(3)**:76–79.

Pittenger M. 2016. Addressing the security challenges of using containers. *Network Security* **2016(12)**:5–8.

Poteet JA. 1980. Informal assessment of written expression. *Learning Disability Quarterly* **3(4)**:88–98.

Prager IG, Moran G, Sanchez J. 1997. Job analysis of felony assistant public defenders: the most important tasks and most useful knowledge, skills, and abilities. *Psychology, Crime and Law* **3(1)**:37–49 DOI 10.1080/10683169608409793.

Rodríguez RM, Martinez L. 2013. An analysis of symbolic linguistic computing models in decision making. *International Journal of General Systems* **42(1)**:121–136 DOI 10.1080/03081079.2012.710442.

Safa NS, Von Solms R, Furnell S. 2016. Information security policy compliance model in organizations. *Computers & Security* **56**:70–82 DOI 10.1016/j.cose.2015.10.006.

Shahidi N, Ou G, Telford J, Enns R. 2015. When trainees reach competency in performing ERCP: a systematic review. *Gastrointestinal Endoscopy* **81(6)**:1337–1342 DOI 10.1016/j.gie.2014.12.054.

Shih H-S, Shyur H-J, Lee ES. 2007. An extension of TOPSIS for group decision making. *Mathematical and Computer Modelling* **45(7)**:801–813 DOI 10.1016/j.mcm.2006.03.023.

Siponen M, Mahmood MA, Pahnila S. 2014. 'Employees' adherence to information security policies: an exploratory field study. *Information & Management* **51(2)**:217–224 DOI 10.1016/j.im.2013.08.006.

Sohaib O, Naderpour M, Hussain W, Martinez L. 2019. Cloud computing model selection for e-commerce enterprises using a new 2-tuple fuzzy linguistic decision-making method. *Computers & Industrial Engineering* **132**:47–58 DOI 10.1016/j.cie.2019.04.020.

Succar B, Sher W, Williams A. 2013. An integrated approach to BIM competency assessment, acquisition and application. *Automation in Construction* **35**:174–189 DOI 10.1016/j.autcon.2013.05.016.

Terkan R. 2013. Effective marketing at education: importance of communication materials. *International Review of Management and Marketing* **3(4)**:146–152.

Tobey D. 2015. A vignette-based method for improving cybersecurity talent management through cyber defense competition design. In: *Proceedings of the 2015 ACM SIGMIS conference on computers and people research, Newport Beach, CA*. 31–39.

Toth P, Klein P. 2013. A role-based model for federal information technology/cyber security training. *NIST Special Publication* **800(16)**:1–152.

Trippe D, Moriarty K, Russell T, Carretta T, Beatty A. 2014. Development of a cyber/information technology knowledge test for military enlisted technical training qualification. *Military Psychology* **26(3)**:182–198 DOI 10.1037/mil0000042.

Wei G-W. 2010. Extension of TOPSIS method for 2-tuple linguistic multiple attribute group decision making with incomplete weight information. *Knowledge and Information Systems* **25(3)**:623–634 DOI 10.1007/s10115-009-0258-3.