

Development of the cybersecurity scale (CS-S): Evidence of validity and reliability

Information Development
1–9
© The Author(s) 2021
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0266666921997512
journals.sagepub.com/home/idv



Ibrahim Arpaci 

Tokat Gaziosmanpasa University

Kadir Sevinc

Tokat Gaziosmanpasa University

Abstract

This study aimed to develop a cybersecurity scale to measure individuals' practices and perceptions regarding cybersecurity. The study tested psychometric properties of the Cybersecurity Scale (CS-S) by employing a multi-stage research design. In the first study, an Exploratory-Factor-Analysis (EFA) was conducted to explore the underlying factor structure and evaluate internal consistency reliability of the CS-S. The EFA results showed good internal consistency reliability ($\alpha = .88$) and a six-factor structure. In the second study, a Confirmatory-Factor-Analysis (CFA) was conducted to verify the factor structure. The CFA results indicated that the six-factor model (i.e., confidentiality, control/possession, integrity, authenticity, availability, and utility) fits the data well. Significant individual differences were observed in each dimension of the CS-S. Results indicated that the CS-S has evidence of convergent, discriminant, and construct validity along with internal consistency reliability. The results suggested that the CS-S is a valid and reliable instrument to measure individuals' cybersecurity practices and perceptions.

Keywords

cybersecurity, cybersecurity scale, cyberspace, scale development, CS-S

Submitted: 8 January, 2021; Accepted: 18 January, 2021.

Introduction

The National Institute of Standards and Technology (NIST) defined cybersecurity as “the process of protecting information by preventing, detecting, and responding to attacks” (National Institute of Standards and Technology - NIST, 2018, p.45). Likewise, the International Telecommunication Union (ITU) defined cybersecurity as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets” (International Telecommunication Union - ITU, 2008). User and organization assets consist of connected services, applications, devices, systems, and stored or transmitted data in the cyberspace (Reid and Van Niekerk, 2014; ITU, 2008).

From the definition above it is clear that cybersecurity is the “protection of cyberspace itself, information, and technologies that support users of cyberspace”, which is defined as “a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form” (International Organization for Standardization/International Electrotechnical Commission - ISO/IEC, 2012). Thus, cybersecurity involves the protection

Corresponding author:

Ibrahim Arpaci, Department of Computer Education and Instructional Technology, Tokat Gaziosmanpasa University, Tokat, Turkey.
Email: ibrahim.arpaci@gop.edu.tr

of cyberspace itself and the integrity, confidentiality, and availability of information and ICT in cyberspace (ISO/IEC, 2012).

Beginning from 1999 to the present, there are 3088 publications (1151 articles) on cybersecurity indexed in the Web of Science database. All these publications include the keywords ‘cybersecurity’ or ‘cyber security’ within the title. A bibliometric mapping analysis indicated that Wang and Lu (2013) (371 citations), Buczak and Guven (2015) (277 citations), Yan, Qian, Sharif, and Tipper (2012) (250 citations), Ten, Liu, and Manimaran (2008) (237 citations), and Liu, Xiao, Li, Liang, and Chen (2012) (225 citations) were the most cited articles. Further, ‘IEEE Security and Privacy’ (66 documents, 216 citations), ‘Computers and Security’ (49 documents, 529 citations), and ‘Computer’ (28 documents, 101 citations) were the most productive journals. The USA (1228 documents, 5939 citations), England (250 documents, 681 citations), China (174 documents, 793 citations), Australia (117 documents, 546 citations), and India (95 documents, 159 citations) were the most productive countries. Whereas the MIT (29 documents, 267 citations), Carnegie Mellon University (28 documents, 102 citations), and George Mason University (26 documents, 78 citations) were the most productive universities.

These bibliometric findings suggested that there is an increasing number of studies on cybersecurity. Most of the studies focused on the technical aspect of cybersecurity, whereas cybersecurity is a socio-technical concept and the social aspect has gained more importance in the age of the Internet of Things (IoT) or cyber-physical systems. The distributed nature of the interrelated computing devices creates vulnerabilities to cyberattacks, which attempt to violate security and privacy by targeting the integrity, confidentiality, and availability of personal information (Cherdantseva et al., 2016).

Further, cybersecurity is one of the main challenges in the age of the Internet of Things (IoT) or cyber-physical systems. Cyber-attacks are a growing risk, not only for organizations, but also for individuals. Anyone should be aware of cybersecurity risks, and thereby, be ready for such risks by proactive actions. Therefore, there is a need for a reliable and valid instrument to measure users’ cybersecurity practices and perceptions. Some previous studies have conducted descriptive surveys to investigate students’ information security practices, awareness, and perceptions (Teer, Kruck, and Kruck, 2007; Slusky and Partow-Navid, 2012). However, none of the studies

focused on the development of a reliable and valid measure to assess actual users’ cybersecurity practices and perceptions. Therefore, the purpose of this study is to develop a cybersecurity scale to measure practices and perceptions of the users, specifically undergraduate students.

Theoretical background and development of the scale items

The NIST Cybersecurity Framework (ver. 1.1) and the Parkerian Hexad model (Parker, 1992) were used as a basis for the development of the CS-S factors and items. The NIST Cybersecurity Framework was used to define cybersecurity risks and practices (NIST, 2018), whereas the Parkerian Hexad (PH) was used to identify critical security characteristics that may affect users’ cybersecurity perceptions and practices. The Parkerian Hexad, which is based on the CIA triad, is a cybersecurity model for critical security characteristics (Parker, 1992). The ‘Confidentiality, Integrity, and Availability’ (CIA) triad is a fundamental security framework that focuses on critical information characteristics. The characteristics are also regarded as the most critical aspects of cybersecurity. For example, confidentiality is defined as “a set of rules that limits access to information” (Li, Meng and Kwok, 2016, p. 130). Confidentiality is related to privacy and information security and refers to the protection of private information from exposure or disclosure to unauthorized individuals or systems (Von Solms and Van Niekerk, 2013). Integrity is related to the accuracy and reliability of data that has not been exposed to malicious or accidental alteration (Li et al. 2016, p. 131). Integrity also refers to the ability of preventing information from being altered in an undesirable or unauthorized manner (Andress, 2014). Availability is defined as “ensuring that authorized parties are able to access the switch and related information when needed” (Li et al. 2016, p. 131). It refers to the ability to access information when needed (Reid and Van Niekerk, 2014).

The Parkerian Hexad (PH) expanded the CIA triad with three additional critical characteristics (i.e., authenticity, possession/control, and utility) to provide a more comprehensive model. In the PH model, authenticity refers to the assurance that a transaction of information is from an original source (Von Solms and Van Niekerk, 2013). Possession/control refers to the state or quality of control or ownership of the confidential information, whereas utility refers to the

Table 1. The six dimensions of the CS-S.

Dimensions	Definition
Availability	The ability of allowing authorized users to access cyberspace.
Authenticity	The ability to retain legitimacy and eliminate the need for trust in the cyberspace.
Confidentiality	The ability to protect cyberspace from unauthorized access.
Integrity	The ability of preserving the consistency, accuracy and trustworthiness of the cyberspace.
Possession/ Control	The ability of providing quality of control or ownership in the cyberspace.
Utility	The usefulness and utilization of information and services in the cyberspace.

usefulness of information and services in cyberspace. The PH model is used as a guide for development of the CS-S factor structure. Table 1 shows the definition of the six dimensions adapted from Ashiku and Dagli (2019, p.143).

Method and Findings

This study involved a multi-stage research design for the scale development following Tabachnick and Fidell (2014). In stage 1, the item-pool was developed based on the relevant literature and theory. In stage 2, the initial item pool was reviewed by experts who evaluated the match between the items and dimensions. In stage 3, an Exploratory Factor Analysis (EFA) was conducted to explore the underlying factor structure and evaluate internal consistency reliability. In stage 4, a Confirmatory Factor Analysis CFA was conducted to verify the factor structure. The study used a different data set in the CFA as recommended by Schumacker and Lomax (2010).

Study 1: Exploratory Factor Analysis

Participants and Procedure. The population of the study was university students, and the study used the convenience sampling method. The first study consists of 320 participants (170 female and 150 male) with a mean age of 21.27 years \pm 2.50 (ranged between 17-41). Participants who willingly participated in the study were undergraduate students studying at Tokat Gaziosmanpasa University in Turkey. In terms of class level, 15% were freshmen, 42.5% were

sophomores, 19.1% were juniors, and 23.4% were seniors. Most of the participants stated that they live in a city (54.4%) or state 31.9(%). The participants stated that 16.3% of them use Internet 1-2 hours/day, 45.9% of them use Internet 3-4 hours/day, 30.3% of them use Internet 5-7 hours/day, and 7.5% of them use Internet more than 8 hours/day. The results show that most participants (99.7%) have a smartphone and use mobile Internet. About 60% of them use their smartphones 4-8 hours/day, while 75% and 67.2% of the participants use e-government and e-commerce services, respectively.

The institutional ethical committee of Tokat Gaziosmanpasa University granted ethical clearance and the procedures were consistent with ethical standards (File Number 20/02/2020-E.11621). Informed consent forms were obtained from all participants and they were informed about the aim of the research. The paper-based instrument included eight demographic questions (e.g., gender, age, Internet usage, etc.) and scale items. The instructions asked participants to indicate the degree to which each of the statements describes what they just experienced on a five-point scale from “1 = strongly disagree” to “5 = strongly agree.”

Face validity. The item-pool generated by the researchers consists of 74 items which aim to measure users cybersecurity perceptions (security and privacy issues) and practices regarding passwords, e-mails, websites, social engineering, antivirus programs, firewalls, social media applications, and online services. The face validity of the item-pool was confirmed by three field experts (professors in Information Systems, Psychometrics, and Linguistics). The experts investigated the items in different aspects based on their expertise and labeled the items as removed, revised or appropriate. In the initial evaluation, the experts suggested that 17 items should be removed, and 8 items should be revised. After the first revision, the item pool was presented to the experts for the second time. The experts suggested that 5 items should be removed, and 6 items should be revised. In the third round, the experts group provided a final approval, and the 52-item form was reached.

Results. The EFA was conducted to determine the underlying factor structure of the CS-S. In the initial runs, 25 items were removed since they either loaded strongly more than one factor or failed to load

Table 2. Pattern Matrix.

Factors	Items	Communalities	1	2	3	4	5	6
Confidentiality	Conf1	.543	.482					
	Conf2	.672	.713					
	Conf3	.578	.585					
	Conf4	.523	.628					
Control/Possession	Cont1	.509		.667				
	Cont2	.586		.824				
	Cont3	.736		.905				
	Cont4	.354		.377				
	Cont5	.395		.586				
	Cont6	.546		.676				
	Cont7	.397		.429				
Integrity	Inte1	.542			.716			
	Inte2	.353			.530			
	Inte3	.595			.754			
	Inte4	.502			.700			
Authenticity	Auth1	.413				.502		
	Auth2	.427				.507		
	Auth3	.421				.628		
	Auth4	.644				.846		
	Auth5	.582				.678		
Availability	Avai1	.840					.932	
	Avai2	.785					.897	
	Avai3	.402					.600	
	Avai4	.428					.621	
Utility	Util1	.389						.611
	Util2	.577						.776
	Util3	.510						.611

Table 3. Reliability, Normality, and Descriptive Statistics.

Factors	No. of items	Mean	SD	Alpha	Skewness (SE = .136)	Kurtosis (SE = .272)
Confidentiality	4	16.11	3.428	.820	-1.181	1.472
Control/Possession	5	20.61	3.848	.786	-1.438	2.776
Integrity	4	11.71	3.587	.773	.065	-.105
Authenticity	5	19.96	3.807	.816	-.954	1.507
Availability	4	13.78	3.870	.849	-.333	-.518
Utility	3	10.93	2.459	.720	-.661	.852

significantly on a factor. The final run was based on the remaining 27 items and suggested a six-factor solution. These six factors had an eigen value more than 1, and they together accounted for 52.778% of the total variation. The first and second factors account for about 27.275% and 7.672% of the explained variance, respectively. Bartlett's test results showed that the values were significant (χ^2 (df = 351) = 3875.544) and Kaiser's 'measure of sampling adequacy' was .889. This suggested that the variables were appropriate

for the factor analysis. Table 2 indicates the communalities and pattern matrix for maximum likelihood with promax rotation.

Internal Consistency Reliability. The normality test results shown in Table 3 were obtained after two more items (Cont2 and Cont3) having an extreme kurtosis and skewness were dropped from the CS-S. For a normal distribution, skewness and kurtosis values should range within ± 3 (Stuart and Ord, 1994), and

Table 4. Reliability of the subscales and items.

Factors	Items
Confidentiality ($\alpha = .784$)	1. I am cautious about personal information I share in cyberspace. 2. I do not share information and documents in cyberspace that I do not want to share with third parties in real life. 3. I ensure that the data I share in cyberspace can only be viewed by the necessary people. 4. I do not share my contact information in cyberspace.
Control/Possession ($\alpha = .810$)	5. I do not share my passwords for my accounts with anyone. 6. When creating my passwords, I choose a hard-to-guess password that contains symbols, numbers and capital letters. 7. I use the phone verification service to protect my email password. 8. I correctly answer the security question required to recover my account passwords. 9. I do not allow my credit card information to be saved while shopping in cyberspace.
Integrity ($\alpha = .795$)	10. It is safe to store data in cyberspace. 11. Information and documents I have stored in cyberspace are not lost or deleted. 12. Sharing data in cyberspace does not involve any risk. 13. Information and documents stored in cyberspace cannot be accessed by third parties.
Authenticity ($\alpha = .784$)	14. I do not trust e-mails from people I do not know. 15. I do not trust websites without a security certificate. 16. I do not open spam mails sent to my e-mail address. 17. I ignore social engineering e-mails sent to my e-mail address. 18. I do not open links and attachments from unknown sources.
Availability ($\alpha = .784$)	19. I use an up-to-date antivirus program on my devices. 20. I regularly scan my devices with an antivirus program. 21. I keep the firewall installed on my devices turned on. 22. I do not open the files I downloaded from the Internet without scanning with an anti-virus program.
Utility ($\alpha = .735$)	23. I use social media applications to share information in cyberspace. 24. I use services provided in cyberspace (such as Google Scholar, cloud applications, and social media) to solve problems. 25. I use the services provided in cyberspace for information management (information acquisition, storage, sharing and application).

therefore, the data can be considered as normally distributed. Reliability estimates were computed based on the remaining 25 items. The final 25 item-scale indicated a high internal reliability with a Cronbach's alpha value of .883.

Study 2: Confirmatory Factor Analysis

Participants and Procedure. The second study consists of 454 participants (262 female and 192 male) with a mean age of 21.35 years (S.D. = 2.36, ranged between 18-38). The participants stated that 15.6% of them use Internet 1-2 hours, 42.3% of them use Internet 3-4 hours, 30.6% of them use Internet 5-7 hours, and 11.5% of them use Internet more than 8 hours per day. The participants also stated that 67.8% and 57.7% of them use e-government and e-commerce services, respectively.

Internal Consistency Reliability. The subscales indicated a sufficient internal consistency ($.735 < \alpha < .810$), and the Cronbach's alpha of the total scale was .887. Reliability of the subscales and scale items are presented in Table 4 (See Appendix A for scoring of the CS-S).

Convergent and Discriminant Validity. Convergent validity of the CS-S was evaluated by using the 'composite reliability' (CR) and 'average variance extracted' (AVE) scores. Results indicated that the CR values were greater than the threshold values of .70 (Fornell and Larcker, 1981), whereas the AVE values were close to the threshold values of .50. This indicated an adequate convergent validity. The results showed that all factors were significantly correlated each other ($p < .01$). The square roots of the AVE were greater than the cross correlations, and thus, the

Table 5. Correlations matrix, discriminant and convergent validity.

Factors	CR	AVE	1	2	3	4	5	6
1. Availability	.827	.548	.740					
2. Confidentiality	.796	.497	.279*	.705				
3. Control/Possession	.803	.450	.386*	.557*	.671			
4. Integrity	.789	.496	.367*	.146*	.197*	.704		
5. Authenticity	.796	.441	.461*	.596*	.670*	.281*	.664	
6. Utility	.740	.489	.436*	.354*	.370*	.346*	.397*	.700

*p < .01.

Table 6. Model fit indices.

Fit Indices	Measurement Model	Reference Value(s)
χ^2	478.891	
p value	< .001	
χ^2/df	1.871	< 3
GFI	.922	≥ .90
AGFI	.901	≥ .80
NFI	.893	≥ .90
TLI	.938	≥ .90
CFI	.947	≥ .90
IFI	.947	≥ .90
RMSEA	.044	≤ .08
SRMR	.055	≤ .08

discriminant validity was ascertained. Table 5 indicates the correlations matrix, and the CR and AVE values.

Measurement Model. The CFA was used to test the measurement model with SPSS AMOS (v.23). Model fit estimates and reference values suggested by Kline (2005) indicate an acceptable model-fit for the measurement model: [$\chi^2/DF = 1.87$, $GFI = .92$, $AGFI = .90$, $TLI = .94$, $CFI = .95$, $IFI = .95$, $SRMR = .055$, $RMSEA = .044$, $LO90 = .038$, $HI90 = .050$]. Table 6 indicates the model fit indices for the measurement model illustrated in Figure 1.

Individual Differences. CS-S scores were ranged between 25 to 125 ($M = 94.87$, $SD = 14.19$) in which males ($n = 192$) scored higher on each subscale than did females ($n = 262$). A one-way multivariate analysis of variance (MANOVA) results show that there is a significant difference between males and females, Wilks' $\lambda = .021$, $F(6,447) = 3546.65$, $p < .001$, $\eta^2 = .979$, power = 1.00. On all subscales, males scored significantly higher than females ($p < .001$), where partial eta squared

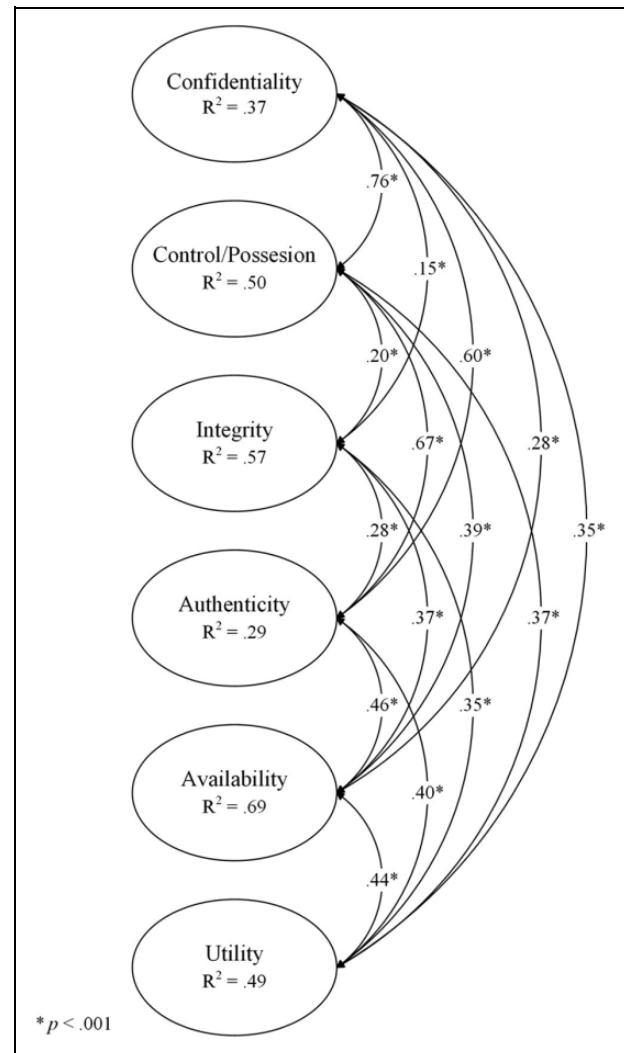


Figure 1. Measurement Model.

differences were small (ranged from .904 to .971). Further, in terms of age (ranged 18-38), there was also significant multivariate difference (Wilks' $\lambda = .189$, $F(6,433) = 310.02$, $p < .001$, $\eta^2 = .811$, power = 1.00), where elders scored higher on each subscale. By class standing (1-4), there was significant

multivariate difference (Wilks' $\lambda = .022$, $F(6,445) = 3372.33$, $p < .001$, $\eta^2 = .978$, power = 1.00), where seniors scored the highest on most subscales (i.e., confidentiality, control, and authenticity), while freshman scored the highest on utility subscale. Finally, independent sample t -test results showed a significant difference between the highest 27% ($M = 110.94$, $SD = 5.14$) and the lowest 27% ($M = 77.50$, $SD = 11.16$) groups in terms of the total score, $t(243) = 30.141$, $p < .001$. This suggested the CC-S can significantly differentiate these groups.

Discussion and Conclusion


Cybersecurity is an important concept in the age of IoT or cyber-physical systems. The distributed nature of the interrelated computing devices creates vulnerabilities to cyberattacks, which attempt to violate security and privacy by targeting integrity, confidentiality, and availability of the information. Therefore, anyone should be aware of cybersecurity risks, and be ready for cyberattacks by proactive actions. Accordingly, the current study aimed to develop and validate a self-report instrument (called CS-S for short) for measuring the individuals' cybersecurity practices and perceptions. The results suggested that the CS-S demonstrates a high internal consistency. A six-factor structure (confidentiality, control/possession, integrity, authenticity, availability, and utility) was determined in the initial sample and subsequently confirmed in the second sample. Correlations among the six CS-S factors was mostly as expected.

In conclusion, the results indicated that the CS-S is a valid and reliable measure of individuals' cybersecurity practices and perceptions. A high score of the CS-S indicates a high the level of perception and actual behavior toward cybersecurity. Significant individual differences were observed in each dimension of the CS-S. These findings could help policy makers to understand individuals' cybersecurity needs, and thereby set strategies to promote cybersecurity. For example, seminars or workshops can be designed and delivered for lower scored students in the CS-S to raise their awareness and knowledge about cybersecurity.

The proposed measurement model was limited to the assessment of users' - specifically undergraduate students' - cybersecurity perceptions and practices based on six cybersecurity characteristics (confidentiality, control/possession, integrity, authenticity, availability, and utility). However, the study acknowledged

that there may be other cybersecurity key performance attributes such as anonymity, accountability, affordability, privacy, and resilience that may affect users' cybersecurity perceptions and practices.

ORCID iD

Ibrahim Arpaci  <https://orcid.org/0000-0001-6513-4569>

References

- Andress J (2014) *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice*. Syngress, Elsevier, USA.
- Ashiku L and Dagli C (2019) Cybersecurity as a Centralized Directed System of Systems using SoS Explorer as a Tool. *14th Annual Conference System of Systems Engineering (SoSE)* (pp. 140–145). IEEE.
- Buczak AL and Guven E (2015) A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys and Tutorials*, 18(2), 1153–1176. Doi: 10.1109/COMST.2015.2494502
- Cherdantseva Y, Burnap P, Blyth A, Eden P, Jones K, Soulsby H and Stoddart K (2016) A review of cyber security risk assessment methods for SCADA systems. *Computers and Security*, 56, 1–27. <https://doi.org/10.1016/j.cose.2015.09.009>
- Fornell C and Larcker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. <https://doi.org/10.1177/002224378101800104>
- International Organization for Standardization/International Electrotechnical Commission (2012) ISO/IEC 27032: Information technology-security techniques-guidelines for cybersecurity.
- International Telecommunication Union (2008) International Telecommunication Union, ITU-TX.1205: Series X: Data networks, open system communications and security: Telecommunication security: Overview of cybersecurity. <https://www.itu.int/rec/T-REC-X.1205-200804-I>
- Kline RB (2005) *Principles and practice of structural equation modeling* (2nd ed). New York: Guilford.
- Li W, Meng W and Kwok LF (2016) A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. *Journal of Network and Computer Applications*, 68, 126–139. <https://doi.org/10.1016/j.jnca.2016.04.011>
- Liu J, Xiao Y, Li S, Liang W and Chen CP (2012) Cyber security and privacy issues in smart grids. *IEEE Communications Surveys and Tutorials*, 14(4), 981–997. Doi: 10.1109/SURV.2011.122111.00145
- National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology*. <https://doi.org/10.6028/NIST.CSWP.04162018>

- Parker DB (1992) *Fighting Computer Crime: A New Framework for Protecting Information*. New Jersey, ABD: John Wiley and Sons.
- Reid R and Van Niekerk J (2014) From information security to cyber security cultures. *IEEE Information Security for South Africa* (pp. 1–7). Doi: 10.1109/ISSA.2014.6950492
- Schumacker RE and Lomax RG (2010) *A beginner's guide to structural equation modeling* (3rd ed.). New York, NY: Routledge.
- Slusky L and Partow-Navid P (2012) Students information security practices and awareness. *Journal of Information Privacy and Security*, 8(4), 3–26. <https://doi.org/10.1080/15536548.2012.10845664>
- Stuart A and Ord JK (1994) *Kendall's advanced theory of statistics*. London, UK: Edward Arnold.
- Tabachnick BG and Fidell LS (2014) *Using multivariate statistics* (6th ed.). London: Pearson Education Limited.
- Teer FP, Kruck SE and Kruck GP (2007) Empirical study of students' computer security practices/perceptions. *Journal of Computer Information Systems*, 47(3), 105–110. 10.1080/08874417.2007.11645971
- Ten CW, Liu CC and Manimaran G (2008) Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, 23(4), 1836–1846. Doi: 10.1109/TPWRS.2008.2002298
- Von Solms R and Van Niekerk J (2013) From information security to cyber security. *Computers and Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Wang W and Lu Z (2013) Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5), 1344–1371. <https://doi.org/10.1016/j.comnet.2012.12.017>
- Whitman ME and Mattord HJ (2011) *Principles of Information Security*. Cengage Learning, Nelson Education, CA.
- Yan Y, Qian Y, Sharif H and Tipper D (2012) A survey on cyber security for smart grid communications. *IEEE Communications Surveys and Tutorials*, 14(4), 998–1010. Doi: 10.1109/SURV.2012.010912.00035

About the authors

Ibrahim Arpacı is an associate professor of Educational Technology at Tokat Gaziosmanpasa University. He holds a BSc in Computer Education and Instructional Technology (2005) from Anadolu University, a MSc in Information Systems (2009) and a PhD in Information Systems (2013) both from Middle East Technical University. He was a visiting scholar at Ryerson University, Ted Rogers School of Information Technology Management, Toronto, ON, Canada (2012-2013). His academic work focuses on how computational technology interacts with psychological, educational, and cultural dynamics. His research interests are in computational intelligence, instructional systems design and technology, cyberpsychology and behavior, culture, learning and technology. His publications have appeared in leading academic journals including *British Journal of Educational Technology*, *Telematics and Informatics*, *Computers in Human Behavior*, *Medical Internet Research*, *Personality and Individual Differences*, *Internet Research*, and *Cyberpsychology, Behavior, and Social Networking*. He received the Best Paper Award in the European and Mediterranean Conference on Information Systems (EMCIS, 2009). He received the Distinguished Researcher Award from London Journals Press (UK, 2019). Contact: Department of Computer Education and Instructional Technology, Tokat Gaziosmanpasa University, Tokat, Turkey. Email: ibrahim.arpaci@gop.edu.tr

Kadir Sevinc is a MSc student at the Department of Computer Education and Instructional Technology, Tokat Gaziosmanpasa University, Tokat, Turkey. His areas of interest include cybersecurity and cybernetics. Contact: Department of Computer Education and Instructional Technology, Tokat Gaziosmanpasa University, Tokat, Turkey. Email: kadirsevis@hotmail.com

Appendix A. Cybersecurity scale (CS-S).

Confidentiality	1. I am cautious about personal information I share in cyberspace. 2. I do not share information and documents in cyberspace that I do not want to share with third parties in real life. 3. I ensure that the data I share in cyberspace can only be viewed by the necessary people. 4. I do not share my contact information in cyberspace.
Control/ Possession	5. I do not share my passwords for my accounts with anyone. 6. When creating my passwords, I choose a hard-to-guess password that contains symbols, numbers and capital letters. 7. I use the phone verification service to protect my email password. 8. I correctly answer the security question required to recover my account passwords. 9. I do not allow my credit card information to be saved while shopping in cyberspace.
Integrity	10. It is safe to store data in cyberspace. 11. Information and documents I have stored in cyberspace are not lost or deleted. 12. Sharing data in cyberspace does not involve any risk. 13. Information and documents stored in cyberspace cannot be accessed by third parties.
Authenticity	14. I do not trust e-mails from people I do not know. 15. I do not trust websites without a security certificate. 16. I do not open spam mails sent to my e-mail address. 17. I ignore social engineering e-mails sent to my e-mail address. 18. I do not open links and attachments from unknown sources.
Availability	19. I use an up-to-date antivirus program on my devices. 20. I regularly scan my devices with an antivirus program. 21. I keep the firewall installed on my devices turned on. 22. I do not open the files I downloaded from the Internet without scanning with an anti-virus program.
Utility	23. I use social media applications to share information in cyberspace. 24. I use services provided in cyberspace (such as Google Scholar, cloud applications, and social media) to solve problems. 25. I use the services provided in cyberspace for information management (information acquisition, storage, sharing and application).

Scoring: The CS-S has six dimensions and 25 items scored on a “five-point Likert-type” scale ranged from “strongly disagree (1)” to “strongly agree (5).” The total scores range between 25 to 125, a higher score indicates a higher level of perceptions and practices of cybersecurity.