CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 3, No. 1
April 2024
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2024 Review Board

Higher Education Model for Security Literacy using Bloom's Revised Taxonomy

Garry L. White
gw06@txstate.edu
Department of Computer Information Systems
and Quantitative Methods
Texas State University – San Marcos
San Marcos, TX 78666

ABSTRACT

This paper presents and explains a model for the design and content of cyber security literacy curricula for postsecondary education and how Bloom's Revised Taxonomy supports a model of teaching different levels of information security programs at different levels of higher education. Specifically, this paper shows three different security literacy levels (awareness, training, education) for the six different cognitive levels as defined by Bloom's Taxonomy and applies them to different levels of postsecondary education. A summary table is presented to show how and why cognitive levels fit awareness, training, and education. Questions are presented for further research as to unique designs and development of different security literacy programs.

Keywords: Bloom's Taxonomy, technical skills, computer security, training, education, higher education.

Recommended Citation: White, G., (2024). Higher Education Model for Security Literacy using Bloom's Revised Taxonomy. *Cybersecurity Pedagogy and Practice Journal*, 3(?), pp.?. https://doi.org/10.62273/TRBS2965

1. INTRODUCTION

The cyber security battle is being lost because *technology* is the focus of defense instead of the *people* who operate the computers (Jacobson, et al., 2012). "Often, organizations and countries invest in the technologies, forgetting that it is impossible to assure information security without raising awareness among users" (Ismailova, et al., 2019). Technology alone cannot shield computer systems from threats (Rhee et al., 2012). In today's world of computing, everyone is a target (Idziorek, et al., 2011). As Rhee et al. (2012) indicated, since technology alone cannot protect data and information systems from potential threats, there should be more effort made in addressing the human dimensions of information security (Rhee et al., 2012).

The information security field requires standardized education. (Spruit, 2022). The question is how to develop a standardized education that meets the needs of the security profession. There is little agreement about the competences with respect to information security that should be taught to meet the needs of the security profession (Bishop et al., 2017; Butler et al., 2018; Parker and Brown, 2019). This paper presents a framework of education in security literacy for higher education based on Bloom's Taxonomy.

To address the different characteristics of users this paper relates the three types of security literacy (awareness, training, education) with the different levels of cognition as defined by Bloom's Revised Taxonomy, and then focuses on which security literacy content best fits different postsecondary degree levels. Using this model of security structure will better address academic security literacy programs and curriculum needs.

2. LITERATURE REVIEW

Organizations should focus their security efforts equally on people *and* technology (Hewitt & White, 2020). Every person heading into the workforce needs to be educated about cyber security (Harris & Patten, 2015). Unfortunately, employees and employers fail to see security as a people issue (Ayyagari, 2012; Bulgurcu, et al., 2010; Kirkpatrick, 2006; Rezui & Marks, 2008).

"People are a crucial factor in ensuring the security of computer systems and valuable information resources" (Nieles, et al., 2017). People are fallible and are the weakest link in securing information systems (Caldwell, 2012; Ismailova, et al., 2019; Kirkpatrick, 2006; Mitnick, 2002; Nieles, et al., 2017; Thomason, 2013). Studies have shown 95% of cyber security issues can be traced to human error (Mee & Brandenburg, 2020). "Each day, people are inundated with alerts and pop-ups informing them about patch updates, antivirus signatures, firewall exceptions, suspicious emails, and malware threats. These notifications fail to educate the user on how to make value-based decisions regarding the benefits and consequences of taking specific action on these items" (Security Literacy, 2022)

Security issues are people issues (Rezu & Marks, 2008). Yet people can be the first line of defense, first to detect and respond when an attack occurs. However, past research has focused on protective behavior rather than detection and response (Britt, 2008; Claar & Johnson, 2012; McLaughlin, 2006; Mensch & Wilkie, 2011; Pollitt, 2005; Puhakainen & Siponen, 2010; Wagley, 2010).

Since people are a primary target, education is one of the "secret weapons" in the cyber security battlefield. Further, if everyday users are the targets, then all audiences, not just technical and professional staff, need training and education in cyber security basics (Jacobson, et al., 2012). There is a need for users and professionals to learn information security. To get users to "think security" is to create a culture of security (Haber, 2009). Hence, information security literacy is needed (Piazza, 2006) and is an important defense (Jacobson, et al., 2012). "Just as drivers and passengers are taught how to wear seatbelts and to follow the rules of the road, citizens should be taught how to safely navigate the internet highway" (Mee & Brandenburg, 2020).

Computer security education is the key to combating the risks and vulnerabilities of information systems (Jacobson, et al., 2012). In the past, cyber security education was only a concern for computer and Internet experts (Idziorek, et al., 2011). "Universities have introduced technical degree programs in cyber security to meet industry demand for graduates with specialized skills" (Frydenberg & Lorenz, 2020). What a formal pedagogical approach to practical computer security education provides is the context and knowledge for students to apply computer security best practices before a cyber-attack. Then when faced with a critical situation, the user can be proactive rather than reactive in the face of new threats (Jacobson, et al., 2012). Applying countermeasures after an attack is too late (White, 2021).

"Most governments' strategies to improve cyber security overlook the importance of continued cyber risk education for its citizens across all ages and social demographics" (Mee & Brandenburg, 2020). Security education should not only prepare security professionals and IT technicians but the average end-user as well. Security literacy is for everyone.

However, one size does not fit all. Education programs need to be customized according to the needs of specific user groups (Bauer, et al., 2017). Harris & Patten (2015) used Bloom's Taxonomy to identify specific learning outcomes for courses in Information Technology curricula (Harris & Patten, 2015).

3. BLOOM'S REVISED TAXONOMY[1]

In 1956 Benjamin Bloom and co-authors developed a classification of learning levels known as Bloom's Taxonomy. In 2001, the Taxonomy was updated to reflect 21st century educational goals (Anderson & Krathwohl, 2001; Krathwohl, 2002). This revised Taxonomy was used because of the different levels and types of cognition that were outlined in the paper. The levels are interdependent: Progress requires the ability to master the lower levels first.

> "The interdependence of Bloom's different learning levels can be articulated through logic:
> - Before we can understand a concept, we must be able to remember it.
> - Before we can apply the concept, we must be able to understand it.
> - Before we analyze it, we must be able to apply it.
> - Before we can evaluate its impact, we must have analyzed it.
> - Before we can create something based on the concept, we must have remembered, understood, applied, analyzed and evaluated the concept" (McNulty, 2019)

Subsequently, learning can move back and forth between the different levels depending on the learning situation. What follows is a brief synopsis of the six cognitive levels of Bloom's Revised Taxonomy, known as an "Education Framework" by McNulty (2019).

1. Remembering - Verbs: Describe, Identify, Label, List, Name, Recite, Repeat.

   "Remembering is the act of retrieving knowledge and can be used to produce things like definitions or lists. It is the lowest of the taxonomic levels but is essential for the learning process because learners need to have knowledge in place before they can engage with it at higher cognitive levels. . . Remembering requires no understanding of the knowledge, only to have it accurately and thoroughly in mind." (McNulty, 2019).

2. Understanding - Verbs: Examine, Generalize, Group, Order, Paraphrase, Rephrase, Sort.

   "The next level in the taxonomic structure is Understanding, which is defined as the construction of meaning and the building of relationships." (McNulty, 2019).

3. Applying - Verbs: Compute, Demonstrate, Direct, Dramatize, Formulate, Make, Present.

   "The third level in Bloom's taxonomy, Applying, marks a fundamental shift from the pre-Bloom's learning era because it involves remembering what has been learnt, having a good understanding of the knowledge, and then being able to apply it to real-world exercises, challenges or situations." (McNulty, 2019).

4. Analyzing - Verbs: Simplify, Criticize, Distinguish, Explain, Illustrate, Inspect, Question.

   "Analyzing is the cognitive level where a learner can take the knowledge they have remembered, understood and applied, then delve into that knowledge to make associations, discernments or comparisons. Analyzing would mean a learner can take complex information and simplify it or summarize it . . . or critically examine aspects of Bloom's original taxonomy and explain why his students later updated them." (McNulty, 2019).

5. Evaluating - Verbs: Decide, Forecast, Judge, Prioritize, Revise, Value, Weigh.

   "The fifth level in Bloom's Digital Taxonomy is evaluation. This level requires the learner to make criteria-based judgements through the processes of critiquing and checking. Evaluating could involve reading a book and writing a review on its merits . . . suggesting ways to introduce digital technology into the classroom environment." (McNulty, 2019).

6. Creating - Verbs: Construct, Write, Develop, Design, Invent, Originate, Set up.

> "The final taxonomic level is concerned with taking various elements and creating a new, coherent product. This level draws on all the other levels, with the learner remembering, understanding and applying knowledge; analyzing and evaluating outcomes and processes, and then constructing the end product, which may be either physical or conceptual. For example, . . . designing a 3D model of a house on a computer would both be examples of Creating. Another example would be a Learner taking the knowledge of Bloom's taxonomy which they have remembered, understood, applied, analyzed and evaluated, and creating a brand new model for the tiers of cognitive thinking and learning." (McNulty, 2019).

4. SECURITY LITERACY BASED ON BLOOM'S TAXONOMY[1]

> "The prime goal of practical computer security literacy is to provide students with security context for many of the activities they encounter throughout their everyday use of computers and the Internet. As a result, the topics and objectives of the corresponding modules are designed specifically to meet this goal and presented in a tangible format for students of all backgrounds to learn" (Security Literacy, 2022).

Security literacy is a combination of awareness, knowledge, and skills (Tills, 2017). "Starting with **awareness**, it builds to **training**, which evolves into **education"** (Wilson, et al., 1998). This flow moves people to higher cognitive levels. A Comparative Framework for awareness, training, and education is contained in NIST SP 800-27 Handbook, authored by Nieles, et al. (2017). See Table 1.

Awareness with Bloom's Taxonomy: Remembering, Understanding (what)

The first component of security literacy is an accurate and well-informed awareness of security issues (Tills, 2017). This involves the *recall* (remembering) of definitions and *concepts* along with the meaning and relationships (understanding) of these issues (McNulty, 2019). Cyber security awareness builds on basic information technology concepts (Frydenberg & Lorenz, 2020). And awareness reminds users of these issues and security practices to avoid failure, such as logging off a computer system or locking doors (Nieles, et al., 202). Awareness deals with what is remembered and what concepts are understood.

From Bloom's Taxonomy perspective, the foremost course objective is for all the students to exhibit knowledge of practical computer security. In this context, knowledge is defined as student's ability to *recall* definitions of specific keywords (e.g., virus, phishing, keylogger), describe fundamental *concepts* (e.g., defense-in-depth, social engineering, security vs. privacy) and state computer security best practices (Idziorek, et al., 2011).

Training with Bloom's Taxonomy: Apply, Analyze (how to)

"The purpose of training is to teach people the skills (how to do it) that will enable them to perform their jobs more securely" (Nieles, et al., 202). Training provides the skills and abilities specific to an individual's roles and responsibilities relative to information security (Wilson, et al., 1998).

Skills training is learning how to apply knowledge and how to compare and summarize what is remembered and understood. A person must have this knowledge before applying it to new challenges or new situations. Teaching skills, such as understanding how data is gathered and how a digital identity is tracked online, can dramatically improve cyber security and the safety of a nation's citizens (Mee & Brandenburg, 2020). For example, a person who learns privacy skills will lead them to manipulate their privacy settings effectively, thus regulating the amount of their personal information that's exposed. Effective use of privacy settings after training can be a skill for security literacy (Tills, 2017).

Education with Bloom's Taxonomy: Evaluate, Create (why)

"Security education is more in-depth than security training and is targeted for security professionals and those whose jobs require expertise in security" (Nieles, et al., 202). This includes knowledge of laws, policies, and institutional practices and other concepts external to Information Security. Knowledge of technology resources to guide security behavior is also included in education (Tills, 2017). Education focuses on developing the ability and vision to perform complex multi-disciplinary activities and the skills needed to keep pace with threat and technology changes (Wilson, et al., 1998). With this in-depth and external knowledge, professionals are better able to *evaluate* the *whys* of security breaches and *create* countermeasures

and solutions that will protect data and systems in the event of a cyberattack.

From Harris & Patten (2015), examples showing associations with Literacy and Bloom's Levels are shown in Figure 1.

Figure 1. Three Literacy Types and Bloom's Taxonomy Levels (Harris & Patten, 2015)

Literacy	Bloom's	Outcomes	Examples
Awareness	Remember	- recall	Discuss user passwords. -recognize a phishing e-mail
Awareness	Understand	- meaning	Explain auditing. -know what a phishing e-mail can do
Train Skill	Apply	- new situation	Use access control in scenarios. -delete and report phishing e-mail.
Train Skill	Analyzing	- break into parts	Qualitative risk analysis. -determine phishing e-mail's characteristics
Educate	Evaluate	- judgments	Evaluate threats based on risk. -decide if e-mail is phishing and decide what to do.

5. HIGHER EDUCATION LEVELS BASED ON FIVE COMPETENCE LEVELS

Competence is the ability to apply knowledge, skills and attitude for achieving observable results (CEN, 2014). A competence statement of the required knowledge and skills. Spruit & van Noord (2014) developed five competence levels. See List 1. In Table 3, these competence levels are associated with Security Literacy categories to further show the progressing competencies.

Competence Levels 1 and 2 involve Bloom's remembering and understanding. They fit well with an Associate degree. Spruit (2022) describes Level 3 for a Bachelor's degree that stresses information security analysis of critical assets and implementing (apply) recovery plans. This level deals with Bloom's apply and analyze thinking skills. Spruit (2022) also describes Level 4 for a Master's degree that stresses technical research, design (create), execute a scientific research project and formulate conclusions. This level deals with Bloom's evaluation and creates thinking skills. Level 5 is an advanced version of Level 4.

List a: Competence levels 1 to 5 & Knowledge Skills by Spruit & van Noord (2014).

1. Basic knowledge and understanding of the subject. Carrying out the activity in a simple context.
2. Knowledge and understanding of all major aspects of the subject. Carrying out the activity in a simple context.
3. Knowledge and understanding of the subject in detail. Carrying out the activity in a difficult context.
4. Very extensive and detailed knowledge and understanding of the subject. Carrying out the activity in a very complex context.
5. Exceptionally comprehensive and detailed knowledge and understanding of the subject. Guiding others who carry out the activity in a very complex context.

6. HIGHER EDUCATION LEVELS BASED ON SEVEN INFORMATION SYSTEMS COMPONENTS[2]

Information security can be viewed as being different, at the varying levels of postsecondary education through seven components of information security. The seven components are *people, security, processes, technology, policies, standards,* and *procedures* (Rangaswami, 2005; Merkow & Breithaupt, 2006. p 70-74). These seven information security components best summarize the three higher education levels of security literacy curriculum.

Master's degree:
A Master's degree is people and policy focused and prepares future managers. Education at this level should involve the why's of security *policies*, dealing with *people* issues, and evaluation of threats and risks. (White, 2009). People with a Master's level education should be able to **create** security policies, to **evaluate** internal and external issues, and to **understand** the "why," when making decisions. This is what security professionals do.

Bachelor's degree:
A Bachelor's degree teaches *how* the security systems are developed and implemented to meet policy requirements. (White, 2009). Instruction should focus on *processes* and *standards* for development of security systems. When completed, a bachelor's candidate should know *how* to **analyze** security problems, and *how* to **apply** solutions and standards. This is what security managers do.

Associate degree:
An Associate degree curriculum should teach which security procedures and practices are to be maintained and monitored. (White, 2009). The curriculum should focus on the *technologies* and *procedures* to maintain and monitor data and systems. A person with an associate degree should **remember** and **understand** what to do to maintain and monitor operational security. This is what security technicians do.

6. HIGHER EDUCATION LEVELS BASED ON THREE SECURITY LITERACY TYPES AND BLOOM'S TAXONOMY[2]

Master's degree:
Why do security problems exist? This question of security leads to creating security policies that deal with people issues and evaluating internal and external risks. Creation of enterprise security architecture requires a common vision shared by planners, constructors, and administrators. It integrates management processes and policies for enterprise information security (Kim & Leem, 2005). The security professional must be able to evaluate needs to make security decisions.

Information security is a multi-disciplined subject. A security professional requires a wide range of backgrounds such as top-level management knowledge, external knowledge of laws, and awareness of social issues and trends. Security professionals must be educated in business functions such as accounting, finance, marketing, and management to better understand information security in a holistic business context (Rainer et. al., 2007). Along with core computer courses, other liberal arts studies are also needed because information security requires perspective of the environment computer systems work within to understand the whys. A wide range of educational experiences provides a good foundation for a career in Information Security. (Merkow & Breithaupt, 2006, p 7-8). Three universities Master's degrees stress critical thinking, strategic thinking, decision making, and research (ASU, 2023; Bellevue, 2023; ERAU, 2023).

Bachelor's degree:
How are security problems mitigated? This question of security involves **how** the security systems are developed and implemented to satisfy policies. Activities include planning, designing, establishing standards, and implementing security tasks. These activities included defining tasks and responsibilities of personnel, determining how information needs are related to tasks, how information is shared, and the identification, valuation and classification of data assets (Kim & Leem, 2005; Steinke, 1997; Whitman & Mattord, 2005, p. 186). The training aspect of information security can be viewed as how to develop and **apply** security standards and effective security management practices (Whitman & Mattord, 2005, p. 187).

Required skills for such a security curriculum are problem solving (**analyze)**, project management, risk management and technical skills (Armstrong & Jayaratna, 2002). Three universities describe their Bachelor's degrees as risk "analysis" and "applying" analytical tools to contemporary security (OU, 2023) as well as concepts and applications of information systems and technology in organizations (TSU, 2023). A Bachelor's degree stresses detect, manage, and prevent cyber-attacks (CIAT, 2023). Such undergraduate security courses provide a balance between theory and practice (Hsu & Backhouse, 2002).

By applying these skills, confidence and accountability are assured, and compliance with regulatory and legal requirements is provided. Risks are then lowered, control increases, and usable information is made available. These tactical benefits have a positive impact on an organization's relationship with its partners (Ezingeard et al, 2004).

Pending on the nature of the subject of the Bachelor's degree, it can be considered either Training for technical subjects (no theory) or education when considering theory.

Associate degree:
What security procedures and practices are to be utilized? This question of security requires remembering procedures and involves an understanding of what practices should be utilized in any given situation. These procedures lead to successful daily maintenance and monitoring of technology and information and the enforcement of information security policies. (White, 2009).

These operation security procedures provide business continuity, secure and reliable access to information. The integrity and availability of an organization's data and systems are assured. Strict control procedures stop unauthorized access or software use in daily operations, and business processes and customer service improve. (Ezingeard et al, 2004). Four colleges describe their Associate's degrees as acquiring "fundamental" working knowledge and technical skills in cyber security (CIAT, 2023; UST, 2023; CCIS, 2023; DeVry, 2023). Courses at this degree

level are technical and vendor specific and focus on the operational aspects of a business.

7. SUMMARY: EXAMPLES AND SUGGESTIONS

Because security literacy is different at the different levels of higher education, ascertaining the educational needs of students can become easier. Also, information security educators must be aware of current issues in the information security field to create curriculums that deal with a variety of current security issues. Using the new comparative framework of awareness, training and education helps instructors and administrators gain better insight into security literacy in higher education. (Surendran et. al., 2002).

As shown by Figure 2, higher education can be divided into three categories. These categories focus on different and progressive levels of thinking and competencies. This provides better insight into the development of college degrees.

Figure 2. Comparative Framework for Higher Education with Bloom's Taxonomy and Security Literacy.

NIST SP 800:	Awareness	Training	Education
Attribute:	What is	How to	Why – reasons
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Bloom's Taxonomy:	1. Remember 2. Understand	3. Apply 4. Analyze	5. Evaluate 6. Create
Higher Education:	Associate	Associate Bachelor	Bachelor Master

8. FUTURE QUESTIONS TO RESEARCH[1]

Here are four questions for further research from Tills (2017) that can lead to the development of a variety of security literacy curricula (Tills, 2017). Bloom's Taxonomy provides better understanding and insight to answer these questions.

1. What are the issues people need to be aware of for security literacy? (Tills, 2017).

2. Should there be multiple standards of security literacy (e.g., do some people need more advanced security training?)? (Tills, 2017). In other words, consider the different levels of thinking and cognition and the different characteristics of higher education degrees.

3. What is the minimum level of security awareness needed? (Tills, 2017). For example, recognizing an attack, i.e., phishing e-mail.

4. When should security literacy be more focused on awareness, rather than skills? (Tills, 2017).

Other questions: Are there limits for different people when it comes to Bloom's Taxonomy of thinking and Spruit's companies? Do some people function only at the lower thinking levels while others can progress to higher thinking levels? Do some people excel in security management issues while others can excel in security technology?

9. FUTURE RESEARCH

White (2009) authored a paper showing a model relating management levels and security needs. A future research paper could be the merging of the two models: Security Literacy and Bloom's Taxonomy with different management levels' security needs. A research question: What are the Bloom's Taxonomy levels and Security Literacy levels associated with operational, tactical, and strategic management levels?

Here are two other possible future research projects: 1) Empirical research on three-degree type (AA, BA, MA) competencies and see how well they align with Bloom's Taxonomy. 2) To determine if some students have limits as to how far they can progress up Bloom's Taxonomy. Such findings can provide guidance as to what areas of security best fit them. Are high level thinkers best for security technology while low level thinkers are best for security management?

10. ENDNOTES

1. Parts of this paper came from a conference submission - White, G. (2022). "Security Literacy & Bloom's Taxonomy." ISECON 2023, March 30-April 1, 2023, Plano, Texas.

2 . Parts of this paper came from a journal paper – White, G. (2009). Strategic, Tactical, & Operational Management security model. *Journal of Computer Information Systems,* 49:3, 71-75, DOI:10.1080/08874417.2009. 11645326. To link to this article: https://doi.org/10.1080/08874417. 2009.11645326

11. REFERENCES

Anderson, L. & Krathwohl, D. (Eds.) (2001). A Taxonomy for Learning, Teaching, and

Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. Boston: Allyn & Bacon, Pearson Education Group.

Armstrong, H. & Jayaratna, N. (2002). "Internet Security Management: A Joint Postgraduate Curriculum Design." *Journal of Information Systems Education*, 13(3), 249-258.

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security,* 8(2), 33-56.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68, 145-159.

Bloom, B. & Krathwohl, D. (1956). Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain. New York: Longmans, Green.

Britt P. (2008). You've got mail….and security breaches. *Inf Today* 25(7), 1–1, 44.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.

Caldwell, T. (2012). Training – The Weakest Link. *Computer Fraud & Security*, 2012(9), 8-14.

Claar C.L. & Johnson J. (2012). Analyzing home PC security adoption behavior. *J Comput Inf Syst*. 52(4), 20–29.

Ezingeard, J.N. & McFadzean, E. & Birchall, D. (2004). Board of Directors and Information Security: A Perception Grid. Paper No. 222 in Proceedings of British Academy of Management Confrerence, Harrogatte.

Frydenberg, M., & Lorenz, B. (2020). Lizards in the Street! Introducing Cybersecurity Awareness in a Digital Literacy Context. *Information Systems Education Journal*, 18(4), 33–45.

Haber, L. (Apr 2009). SECURITY TRAINING 101. *Network World*, 26(16), 30, 32-33.

Harris, M. A., & Patten, K. P. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum. *Journal of Information Systems Education, 26*(3), 219-234. https://libproxy.txstate.edu/login?url=https://www.proquest.com/scholarly-journals/using-blooms-webbs-taxonomies-integrate-emerging/docview/1810013990/ se-2?accountid=5683

Hewitt, B. A., & White, G. (2020). Optimistic Bias and Exposure Affect Security Incidents on Home Computer. *Journal of Computer Information Systems.* On-line access: https://www.tandfonline.com/doi/abs/10.1080/08874417.2019.1697860?journalCode=ucis20. DOI: 10.1080/08874417.2019.1697860.

Idziorek, J., Tannian, M., Jacobson, D., & Jacobson, D. (2011). TEACHING COMPUTER SECURITY LITERACY TO STU- DENTS FROM NON-COMPUTING DISCIPLINES. *American Society for Engineering Education*. AC 2011-600.

Ismailova, R. & Muhametjanova, G. & Medeni, T. D. & Medeni, I. T. & Soylu, D. &; et al. (2019). Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan. *Information Security Journal,* 28(4-5), 1Puhakainen & Siponen, 2010). -135. DOI:10.1080/19393555.2019.1685142

Jacobson, D. & Rursch, J. & Idziorek, J. (2012). "Workshop: Teaching computer security literacy to the masses: A practical approach," 2012 Frontiers in Education Conference Proceedings, 2012, pp. 1-2, doi: 10.1109/FIE.2012.6462423.

Kim, S. & Leem, C. S. (2005). Enterprise security architecture in business convergence environments. *Industrial Management + Data Systems*, 105(7), 919-936.

Kirkpatrick, J. (2006). Protect your business against dangerous information leaks. *Machine Design,* 78(3), 66.

Krathwohl, D. (2002). A Revision of Bloom's Taxonomy: An Overview. *Theory into Practice*, 41(4), 212-218.

McLaughlin K. (2006). COMPTIA: end-user training is critical to security. *CRN* 1194, 35.

McNulty, N. (2019). Everything you've ever wanted to know about Bloom's Taxonomy. Niall McNulty - Learning by Design, April 19, 2022. https://www.niallmcnulty.com/2019/12/introduction-to-blooms-taxonomy/#:~:text=Bloom's%20Taxonomy%20provides%20a%20learning,%2C%20analysing%2C%20evaluating%20and%20creating (accessed 6/16/2022).

Mee, P. & Brandenburg, R. (17 Dec 2020). After reading, writing and arithmetic, the4th 'r' of literacy is cyber-risk. *World Economic Forum*. Geneva, Switzerland. https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/ (accessed 5/Puhakainen & Siponen, 2010). /2022).

Mensch, S. & Wilkie, L. (2011). Information security activities of college students: an exploratory study. *Acad Inf Manage Sci J*. 14(2), 91–116.

Merkow, M. & Breithaupt, J. (2006). *Information Security: Principles and Practices*. Pearson/Prentice Hall, Upper Saddle River, NJ.

Mitnick, K. (2002). The Art of Deception. John Wiley & sons, Hoboken, NJ. (p. 3).

Nieles, M., Dempsey, K., & Pillitteri, V.Y. (2017). SP 800-12: An Introduction to Computer Security: The NIST Handbook, Chapter 13. Computer Security Division-Computer Security Resource Center, NIST, Department of Commerce. https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter13.html (accessed 5/30/2022).

Piazza, P. (2006). Security goes to school. *Security Management*, 50(12), 46.

Pollitt D. (2005). Energis trains employees and customers in IT security. *Hum Res Manage Digest.* 13(2), 25–28.

Puhakainen P, & Siponen M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quart*. 34(4), 757.

Rainer, R. K. & Marshall, T. E., & Knapp, K. J., & Montgomery, G. H. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? *Information Systems Security*, 16(2), 100-108.

Rangaswami, M. R. (Feb, 2005). Finding Security. *Optimize*, 4(2), 67-68.

Rezui, Y. & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27 (7/8), 241.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221-232.

Security Literacy. Partnership for a Healthy Iowa. https://ahealthyiowa.org/programs/security-literacy/ (accessed 5 29 2022).

Surendran, K. & Ki-Yoon, K. & Harris, A. (2002). "Accommodating Information Security in our Curricula." *Journal of Information Systems Education*, 13(3), 173-176.

Thomason, S. (2013). People - The Weak Link in Security. The Global Journal of Computer Science & Technology, 13(11), 6-12.

Tills, C. (Aug 16, 2017). Security Literacy? Clear Security Communication. https://www.clairetills.com/post/2017/08/16/security-literacy (accessed 5 29 2022)

Wagley J. (2010). Breaches lead to employee training. *Secur Manage*; 54(4), 44.

White, G. (2009) Strategic, Tactical, & Operational Management Security Model. *Journal of Computer Information Systems*, 49:3, 71-75, DOI: 10.1080/08874417.2009.11645326. To link to this article: https://doi.org/10.1080/08874417.2009.11645326

White, G. (2021). Generation Z: Cyber-attack Awareness Training Effectiveness. *Journal of Computer Information Systems,* 62(3), 560-571. DOI: 10.1080/08874417.2020.1864680.

Wilson, M., de Zafra, D.E., Pitcher, S. I., Tiressler, J.D., Ippolito, J.B. (1998). NIST SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST, Department of Commerce. https://nvlpubs.nist.gov/

nistpubs/legacy/sp/nistspecialpublication800
-16.pdf (accessed 5/30/2022).