CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 4, No. 1
April 2025
ISSN: 2832-1006

In this issue:

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

2025 Review Board

Education Impact on Trust in Election Technology & Security: Research Proposal

Garry White
gw06@txstate.edu

Ju Long
julong@txstate.edu

Texas State University
San Marcos, TX 78666

ABSTRACT

The purpose of this paper is to propose a study to determine if and how education impacts trust on election security and election technology using the TAM and UTAUT models. This study uses a quantitative research design. Data will be collected through surveys administered to a sample of eligible voters. Variables related to TAM and ITAUT models will be measured using a 7-Likert scale. The survey will be administered before and after the educational session.

Keywords: voting systems, security, hash values, digital signatures, Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT).

Recommended Citation: White, G., Long, J., (2025). Education Impact on Trust in Election Technology & Security: Research Proposal. *Cybersecurity Pedagogy and Practice Journal.* v4, n1, pp 13-23. DOI# https://doi.org/10.62273/KPDB6245

Education Impact on Trust in Election Technology & Security: Research Proposal

Gary White and Ju Long

1. INTRODUCTION

In recent years, the integrity of electoral processes has come under increased scrutiny, particularly with the growing incorporation of technology in voting systems. The average U.S.A. public trust of the government from 1958 to 1968 was 69%. From 2011 to 2021, the average U.S.A. public trust was 20% (Pew, 2021). In the 2020 U.S. general election, only 65% of voters trusted the initial findings (Mercur & Neumann, 2021; Laughlin & Shelburne, 2021) with less than 25% of Republicans trusting (Coleman, 2020). Election distrust is a political weapon that undermines confidence in elections (Fried & Harris, 2020).

From electronic voting machines to blockchain-based voting applications, technology offers the potential for enhanced efficiency and accessibility in elections. However, these advancements have also raised concerns about security, transparency, and reliability, which, if left unaddressed, can undermine public trust in the electoral process. Education emerges as a critical tool in bridging this trust gap, equipping citizens with the knowledge and understanding necessary to navigate and trust technological advancements in voting systems.

Organizations realize the importance of user security education and awareness training (Dodge et al., 2007; Schultz, 2004). Education makes users more security conscious (Ng et al., 2009) and is needed to counter unrealistic thinking about ideas that sound good but lack evidence.
The integration of education and technology in elections is not merely about informing voters about how to use new systems, but also about instilling a deeper understanding of the underlying principles and safeguards that ensure their integrity. Research suggests that informed citizens are more likely to trust and engage with electoral technologies. This trust is paramount, as perceived vulnerability in electoral systems can lead to decreased voter turnout and increased susceptibility to misinformation (Norris, 2015).

Educational initiatives aimed at improving trust in election technology can take multiple forms, including public information campaigns, school curriculums, and community workshops. For instance, the Carter Center (2020) highlights the importance of comprehensive voter education programs in fostering transparency and confidence in electoral processes. Furthermore, providing voters with accessible information about the technical aspects of election technology, such as encryption and verification methods, can demystify these systems and reduce skepticism.

The necessity of these educational efforts is underscored by the rapid pace at which election technology is evolving. As newer, more complex systems are introduced, the gap between technology developers and the general public's understanding widens, potentially exacerbating distrust. Therefore, ongoing education must be a priority, ensuring that as technology advances, public comprehension and trust advance in tandem.

Can education override the psychological effect of voter fraud propaganda? With education, you can talk from a position of knowledge if you find yourself in a discussion on voter fraud. Having knowledge of election security and technology may increase trust in elections.

This paper explores the multifaceted role of education in enhancing trust in election technology. It analyzes the impact of different educational strategies on trust, and offers recommendations for policymakers. By illuminating the critical connection between education and trust, this research aims to provide a framework for strengthening democratic processes through informed and engaged electorates.

2. THEORETICAL BACKGROUND

To understand how education can impact trust in election technology, it is crucial to delve into theoretical models that explain technology acceptance and usage. Two prominent models

in this regard are the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). These models provide a framework for examining the factors that influence individuals' acceptance and trust in technology, highlighting the role of education in this process.

2.1. Technology Acceptance Model (TAM)

The Technology Acceptance Model, developed by Davis (1989), posits that two main factors determine the acceptance of technology: perceived usefulness (PU) and perceived ease of use (PEOU). According to TAM, individuals are more likely to adopt and trust a technology if they believe it will enhance their performance (PU) and if they find it easy to use (PEOU).

Education can significantly influence both PU and PEOU. By providing comprehensive knowledge about the functionalities and benefits of election technology, educational initiatives can enhance voters' perceptions of its usefulness. For example, training programs that demonstrate how electronic voting machines improve accuracy and efficiency in the electoral process can positively impact PU. Additionally, education can simplify the user experience by reducing the perceived complexity of the technology. Workshops and tutorials that familiarize voters with the operation of voting machines or online voting platforms can make these systems appear more user-friendly, thereby enhancing PEOU.

2.2. Unified Theory of Acceptance and Use of Technology (UTAUT)

The Unified Theory of Acceptance and Use of Technology, introduced by Venkatesh et al. (2003), expands upon TAM by incorporating additional determinants of technology acceptance. UTAUT identifies four key constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions. Each of these constructs can be influenced by educational interventions, thereby impacting trust in election technology.

1. Performance Expectancy: Similar to PU in TAM, performance expectancy refers to the degree to which an individual believes that using the technology will help them achieve better outcomes. Education can bolster performance expectancy by clearly communicating the advantages and effectiveness of election technology in ensuring fair and efficient elections.

2. Effort Expectancy: Comparable to PEOU, effort expectancy pertains to the ease of using the technology. Through targeted educational programs that simplify and demystify the use of election technology, voters are more likely to perceive it as easy to use, thereby increasing their likelihood of acceptance and trust.

3. Social Influence: This construct involves the extent to which individuals perceive that important others (e.g., family, friends, or societal figures) believe they should use the technology. Educational campaigns that include endorsements from trusted community leaders and influencers can positively shape social influence, encouraging broader acceptance and trust in election technology.

4. Facilitating Conditions: These refer to the availability of resources and support needed to use the technology. Education can enhance facilitating conditions by providing access to information, resources, and technical support that enable voters to effectively use election technology. This includes helplines, instructional materials, and community support centers that assist voters throughout the electoral process.

2.3. Integrating Education with TAM and UTAUT

By integrating educational strategies with the constructs of TAM and UTAUT, we can develop a comprehensive approach to fostering trust in election technology. Education serves as a crucial mediating factor that influences perceptions of usefulness, ease of use, performance expectancy, effort expectancy, social influence, and facilitating conditions. Through well-designed educational initiatives, voters can gain the confidence and competence needed to trust and utilize election technology effectively.

For instance, a study by Carter and Bélanger (2005) found that educating users about the security measures and benefits of e-government services significantly increased their trust and adoption rates. Similarly, in the context of election technology, providing voters with transparent information about security protocols, data privacy, and the reliability of electronic voting systems can mitigate concerns and build trust.

2.4. Adapt TAM and UTAUT to Address Election Technologies Challenges

While TAM and UTAUT provide a strong foundation for understanding technology adoption, applying these models to election technology requires specific adaptations to address its unique challenges. Election technology involves higher stakes and public scrutiny compared to other technologies, necessitating a focus on trust, security, and transparency. To enhance the theoretical depth and applicability of this research, we propose that TAM can be extended by incorporating constructs related to perceived security and transparency, which are critical for voter confidence. For instance, we aim to introduce a "Perceived Security" construct to measure the extent to which voters believe that election technology is secure from tampering and fraud. Similarly, we propose that UTAUT can be adapted by emphasizing the role of institutional trust and integrating constructs such as "Institutional Assurance," reflecting voters' trust in the institutions that deploy and manage the technology. These extensions will allow the models to more accurately capture the factors influencing trust in election technology. By addressing these unique challenges, we can develop a more robust theoretical framework that not only explains technology acceptance but also provides actionable insights for enhancing voter trust in election systems. This approach aligns with findings from previous studies on e-government services, where adaptations of TAM and UTAUT to include security and trust-related factors have proven effective in predicting user acceptance (Carter & Bélanger, 2005)

In summary, the TAM and UTAUT models offer valuable insights into how education can impact trust in election technology. By enhancing perceived usefulness, ease of use, performance expectancy, and other key constructs, education plays a pivotal role in promoting the acceptance and trust of technological advancements in elections. As we continue to integrate technology into electoral processes, ongoing educational efforts will be essential in ensuring that voters are informed, confident, and trusting participants in the democratic process.

3. METHODOLOGY

3.1. Research Design

This study employs a quantitative research design to investigate how education impacts trust in election technology using the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). The primary method of data collection will be through structured surveys administered to a sample of eligible voters. The survey will be designed to measure variables related to TAM and UTAUT constructs, as well as participants' levels of trust in election technology.

To ensure the robustness of our research, we will implement a stratified sampling method to ensure a diverse and representative sample that mirrors the demographic composition of the voting population. This approach will involve categorizing participants by key demographic variables such as age, gender, education level, socioeconomic status, and geographic location. By doing so, we aim to capture a broad spectrum of perspectives and experiences, which is crucial for understanding how education impacts trust in election technology across different voter groups. This stratified approach will allow us to conduct subgroup analyses to examine the differential impact of educational interventions on various demographic segments.

3.2. Hypotheses

Based on the theoretical frameworks of TAM and UTAUT, we propose the following hypotheses:

H1: Education on election technology positively impacts perceived usefulness (PU) of election technology.

H2: Education on election technology positively impacts perceived ease of use (PEOU) of election technology.

H3: Perceived usefulness (PU) of election technology positively impacts trust in election technology.

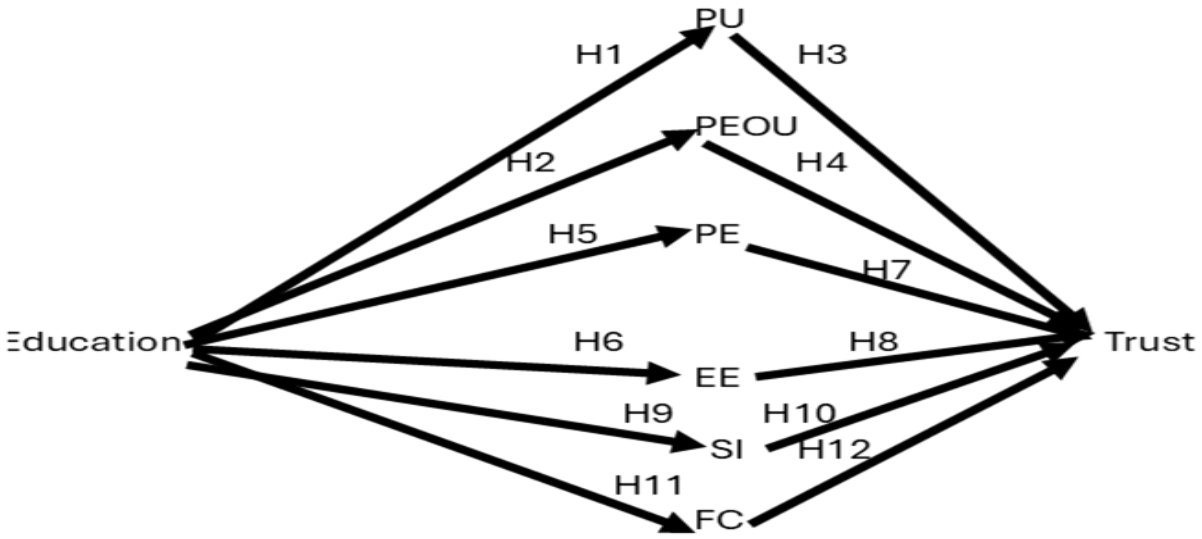
H4: Perceived ease of use (PEOU) of election technology positively impacts trust in election technology.

H5: Education on election technology positively impacts performance expectancy (PE) of election technology.

H6: Education on election technology positively impacts effort expectancy (EE) of election technology.

H7: Performance expectancy (PE) positively impacts trust in election technology.

Figure 1. Hypothesis Model



H8: Effort expectancy (EE) positively impacts trust in election technology. (See comment above)

H9: Education on election technology positively impacts social influence (SI) regarding the use of election technology.

H10: Social influence (SI) positively impacts trust in election technology.

H11: Education on election technology positively impacts facilitating conditions (FC) for the use of election technology.

H12: Facilitating conditions (FC) positively impact trust in election technology.

3.3. Survey Instrument

The survey will consist of several sections, each corresponding to different constructs from the TAM and UTAUT models. Participants will respond to statements on a Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The survey will include the following sections:

1. Demographics: Age, gender, education level, and voting history.

2. Education on Election Technology: Questions assessing the extent and type of educational interventions participants have received regarding election technology.

3. Perceived Usefulness (PU): Items measuring the degree to which participants believe that election technology enhances the electoral process.

4. Perceived Ease of Use (PEOU): Items assessing how easy participants find the use of election technology.

5. Performance Expectancy (PE): Questions regarding participants' expectations that election technology will improve electoral outcomes.

6. Effort Expectancy (EE): Items evaluating the effort required to use election technology.

7. Social Influence (SI): Questions measuring the influence of social factors on participants' use of election technology.

8. Facilitating Conditions (FC): Items assessing the availability of resources and support for using election technology.

9. Trust in Election Technology: Questions evaluating participants' trust in the security, reliability, and overall integrity of election technology.

3.4. Data Analysis

Data collected from the surveys will be analyzed using structural equation modeling (SEM) to test the hypothesized relationships between

constructs. SEM is chosen due to its capability to evaluate complex relationships among multiple variables simultaneously.

1. Descriptive Statistics: Initial analysis will involve descriptive statistics to summarize the demographic data and the distribution of responses for each survey item.

2. Reliability and Validity: Cronbach's alpha will be used to assess the internal consistency of the survey scales. Confirmatory factor analysis (CFA) will evaluate the validity of the constructs.

3. Hypothesis Testing: Path analysis within the SEM framework will be conducted to test the proposed hypotheses, examining the direct and indirect effects of education on trust in election technology through the TAM and UTAUT constructs.

4. FUTURE RESEARCH

The study's reliance on surveys administered before and after an educational session could raises concerns about capturing long-term changes in attitudes or behaviors, and the use of self-reported data may introduce biases affecting the validity of the findings. To address these concerns, in the future studies, we will incorporate a longitudinal design, following participants over an extended period to assess the persistence of educational impacts on trust in election technology. This approach will involve administering follow-up surveys at multiple intervals to evaluate long-term changes in attitudes and behaviors. Additionally, we plan to complement self-reported data with behavioral measures, such as tracking actual voter turnout and engagement with election technology during subsequent elections. By triangulating self-reported data with objective behavioral data, we can mitigate potential biases and enhance the validity of our findings.

Other interviewing variables to consider in future studies on trusting election technology and security are:

1. Narcissism - a personality trait associated with inflated views of oneself, egotism, and self-promotion.as well as positive and inflated self-views of intelligence, power, and physical attractiveness (Raskin and Terry 1988; Twenge, Konrath, Foster, Campbell, & Bushman, 2008).

2. Technology Readiness Index to measure optimism, innovation, discomfort, and insecurity (Parasuraman & Colby, 2000).

3. Cyber Self-Efficacy to measure confidence with technology. (Claar & Johnson, 2012; White & Ekin & Visinescu, 2017).

5. CONCLUSION

This methodology provides a structured approach to investigating the impact of education on trust in election technology. By leveraging the TAM and UTAUT models, this study aims to identify the key factors that mediate the relationship between education and trust, thereby offering insights into effective educational strategies to enhance public confidence in electoral systems.

6. REFERENCES

Carter Center. (2020). Building Confidence in U.S. Elections: A Summary of the Carter Center's Electoral Integrity Assessment Project. The Carter Center.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. Information Systems Journal, 15(1), 5-25. http://dx.doi.org/10.1111/j.1365-2575.2005.00183.x

Claar, C.I., & Johnson, J. (2012). Analyzing Home PC Security Adoption Behavior. Journal of Computer *Information Systems,* 52(4), 20-29. https://doi.org/10.1080/08874417.2012.11645573

Coleman, J. (Dec. 2020). Poll: Less than one-quarter of Republicans trust election results.

The Hill, Dec. 9, 2020. (Accessed on 8/31/21) https://thehill.com/homenews/campaign/529476-fewer-than-one-quarter-of-republicans-trust-election-results-poll

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340. http://dx.doi.org/10.2307/249008

Dodge, R. C. & Carver, C. & Ferguson, A. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73. http://dx.doi.org/10.1016/j.cose.2006.10.009

Fried, A., & Harris, D. B. (2020). In Suspense: Donald Trump's Efforts to Undermine Public Trust in Democracy. Society, 57(5), 527-533. http://dx.doi.org/10.1007/s12115-020-00526-y

Laughlin, N. & Shelburne, P. (2021). How Voters' Trust in Elections Shifted in Response to Biden's Victory. *Morning Consult*, Jam. 27, 2021. (Access 8/31/21) (on-line) https://morningconsult.com/form/tracking-voter-trust-in-elections/.

Mercur, R.T.i & Neumann, P.G. (June 2021). The Risks of Election Believability (or Lack Thereof). *Viewpoints: COMMUNICATIONS OF THE ACM*, 64(6), 24-30. https://doi.org/10.1145/3461464.

Ng, B.Y.,& Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief prospective. *Decision Support Systems*, 46(4), 815-825. http://dx.doi.org/10.1016/j.dss.2008.11.010

Norris, P. (2015). Why Electoral Integrity Matters. Cambridge University Press. http://dx.doi.org/10.1017/CBO9781107280861

Parasuraman, A. & Colby, C. L. (2000). An Update & Streamlined Technology Readiness Index (TRI). *Journal of Service Research*, 18(1), 59-74. https://doi.org/10.1177/109467051453973 0

Pew (2021). Public Trust in Government: 1958-2021. *Pew Research Center*, May 17, 2021. (Accessed 8/31/2021, online) https://www.pewresearch.org/politics/2021/05/17/public-trust-in-government-1958-2021/

Raskin, R. & Terry, H. (1988). A principal-components analysis of the Narcissistic Personality Inventory and further evidence of its construct validity. *Journal of Personality and Social Psychology*, 54(5), May 1988, 890-902. http://dx.doi.org/10.1037/0022-3514.54.5.890

Schultz, E. (2004). Security training and awareness – fitting a square peg in a round hole. *Computers & Security*, 23, 1-2. http://dx.doi.org/10.1016/j.cose.2004.01.002

Twenge, J. M., Konrath, S., Foster, J. D., Campbell, W. K., & Bushman, B. J. (2008). Egos inflating over time: A cross-temporal meta-analysis of the Narcissistic Personality Inventory. Journal of Personality, 76(4), 875-902. http://dx.doi.org/10.1111/j.1467-6494.2008.00507.x

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478. http://dx.doi.org/10.2307/30036540

White, G. & Ekin, T. & Visinescu, L. (2017). Analysis of Protective Behavior and Security Incidents for Home Computers. *Journal of Computer Information Systems,* 57(4): 353-363. http://dx.doi.org/10.1080/08874417.2016.1232991

APPENDIX A:

PILOT STUDIES

Four primary/pilot presentations were made. The first had a negligible positive impact on 8 college students. The second with 10 retirees, had a negligible negative impact. A third presentation, more structured, was made to students attending a high school information technology symposium in San Marcos, Texas (Oct. 8, 2021). Here are the results of their evaluation of the presentation (N = 17).

Presentation:
Excellent 82 %, Great 12%, Good 6%, Fair 0 %, Poor 0%.
Amount learned:
arge 41%, Good 59%, Acceptable 0% Little 0%. Very little if at all 0%

Comments included:

- "You're the only presenter I could understand. I am new to this"
- "This was the only class that I really understood and did not fall asleep"
- "You really connected everything instead of just talking about the topics."
- "I really thought that the entire lessons were deeply described and easily help me understand stuff I have never learned before."
- "Very knowledgeable about the subject, learned a lot. Great."

A fourth presentation was made to computer professionals attending a San Antonio, Texas, cyber summit (Oct. 30, 2021). Here are the results (N = 11):

Presentation:
Excellent 45 %, Great 36%, Good 18%, Fair 0 %, Poor 0%.
Amount learned:
Large 27%, Good 55%, Acceptable 18% Little 0%. Very little if at all 0%

Comments included:

- "This is an important topic, that is critical to preserving our Republic."
- "I understood the technical aspects, but the application of these technologies to detect fraud was new and interesting."
- "Presenter has found group of problems and proves it. Learned problem breakdown."
- "Interesting subject. I'd like to go deeper and learn if the Dominion voting machines were coded to do voter fraud?"
- "I learned how fraud can be proven in court and how fraud can be claimed but is proven false. This is very important for people to know."
- "Good talk"
- "It was an interesting presentation which made me think about and learn about the access of voting digitally.

APPENDIX B: Readings

Background

Hashing is the processing of a unique value for a data file through a mathematical function. An example is a check sum. Given an account number 4545, the digits sum up (4+5+4+5) to a check sum of 18. The hash value is a unique file identifier. If the file changes, the hash value changes. It provides security when the data is shared. It shows integrity, no changes. Hash collisions (different data files calculate the same hash values) are possible. However, this weakness is resolved by using a more powerful hash function or adding an arbitrary value, known as a salt value, to the calculations.

Digital Signatures use hashing functions to show no changes and uses certificates from a third party to show non-repudiation (data came from you and you cannot deny it). Computer laws from many countries have provided greater cyber-security by the acceptance of digital signatures as legal evidence in courts.

To prove in court election software was rigged.

The evidence needed to prove in court the program was rigged are 1) Hash Values of the program, 2) Digital Signature of the program, 3) Test data documentation, and 4) Separation of duties documentation, the testers are independent of the program's developers. The Hash Values show no changes in the program and properly identifies the program used. The Digital Signatures show non-repudiation, you wrote the program.

To prove in court there were Dead Voters

To prove in court that dead people voted requires the comparison of two databases, death certificates from the Department of Vital Statistics database and voter registration records from the Election Commission database. Both databases have common data fields: first name, last name, date of birth, gender, current address, etc.

The compared records from the two databases must be scrub and cleaned (fix mismatches & errors). Hash values of the database files need to be checked to insure nothing was changed so as to show in court. Digital Signatures also need to be presented to the court to show that the sources of the records were from the Dept. of Vital Statistics and the Election Commission.

CYBER SELF-EFFICACY (Claar & Johnson, 2012; White & Ekin & Visinescu, 2017).

Compared to others in the U.S. that are similar age as you, answer the following questions. (NOT at all confident; NOT confident; Somewhat NOT confident; Neutral; Somewhat confident; Confidant; Totally confident).

- I can select the appropriate security software for my home computer.
- I can correctly install security software on my home computer.
- I can correctly configure security software on my home computer.
- I can find the information needed if I have problems using security software on my home computer.
-

Cybersecurity Apprenticeships: Case-Study of a Four-Year Youth Apprenticeship Program

Paul Wagner
paulewagner@arizona.edu
Department Cyber, Intelligence, and Information Operations
University of Arizona
Tucson, Arizona 85747, USA

Cathleen Barton
cbarton673@gmail.com
Cathleen Barton Consulting
Scottsdale, Arizona

Abstract

The United States is facing a persistent cybersecurity workforce shortage, which has significant implications for national security and economic growth. Innovative solutions are required to address this challenge. Youth apprenticeships represent a possible solution for filling talent needs; preparing young people for high-growth careers; building more consistent talent pipelines; creating connections between secondary and postsecondary education institutions, workforce development systems, and community-based organizations; and solving workforce needs. This paper provides a case study of a youth apprenticeship program in cybersecurity. This four-year competency-based program is designed for Arizona high school students and represents a collaboration of an Arizona high school, Phoenix Coding Academy; an industry partner, Kudelski Security; and a non-profit intermediary, the Center for the Future of Arizona (CFA). The program builds upon Kudelski's Switzerland based IT apprenticeship model, adapting it to the U.S. context and incorporating industry partnerships and post-secondary education institutions. This case-study evaluates the effectiveness of the youth apprenticeship program in developing cybersecurity talent, with a focus on its impact on student outcomes, career readiness, and employer satisfaction. Program outcomes include reduced student debt, increased job readiness for entry-level cybersecurity professionals, and contributing to a more diverse and skilled cybersecurity workforce in Arizona and beyond.

Keywords: Youth Apprenticeship, Cybersecurity Education, Workforce Development, Competency-Based Learning, Industry Partnerships

Recommended Citation: Wagner, P., Barton, C., (2025). Cybersecurity Apprenticeships: Case Study of a Four-Year Youth Apprenticeship Program. *Cybersecurity Pedagogy and Practice Journal.* v4, n1, pp 13-23. DOI# https://doi.org/10.62273/UQKC5113

Cybersecurity Apprenticeships: Case-Study of a Four-Year Youth Apprenticeship Program

Paul Wagner and Cathleen Barton

1. INTRODUCTION

The cybersecurity workforce shortage continues to be a concern with over 450,000 unfilled positions within the United States (Cyberseek, 2024) and nearly four million globally (ISC2, 2023). Additionally, the cybersecurity threat continues to grow in sophistication, frequency, and scale increasing stress on the cybersecurity workforce which leads to high employee turnover. White and Bunce (2023) estimates that nearly 51% of cybersecurity professionals will leave the field due to stressors like staffing and resource limitations, rising complexity of technology, remote work challenges, and compliance and regulatory pressures.

Compounding this problem is the increasing dissatisfaction of employers regarding the Knowledge, Skills, and Abilities (KSA) of cybersecurity graduates' ability to fulfill the required tasks of the organization. Ross and Duke (2018) stated, "employers are expressing increasing concern about the relevance of certain cybersecurity-related education programs in meeting the real needs of their organization," in a report to the President of the United States. Additionally, an ISACA report (2023) identified that only 28% of employers surveyed believed that recent cybersecurity graduates were well prepared to meet the cybersecurity challenges of the organization citing lack of technical and soft skills.

One option for addressing these concerns and the cybersecurity workforce gap is to increase youth apprenticeship opportunities for potential cybersecurity professionals to develop the necessary knowledge, skills, and abilities to perform the required tasks. This paper reviews general cybersecurity learning paths, cybersecurity apprenticeship programs, and government initiatives to promote cybersecurity apprenticeship programs. Further, it will provide a case-study of a four-year U.S.-based cybersecurity youth apprenticeship program. Finally, this paper outlines future work and initiatives in expanding or duplicating this program.

2. LITERATURE REVIEW

Cybersecurity Learning Paths

Cybersecurity education requires a holistic approach integrating formal, non-formal, and informal learning to develop the KSAs required to complete required tasks. Formal learning is intentional, organized, and structured; usually arranged by institutions; and guided by curriculum or another formal program (Ainsworth, 2010). Non-formal learning may or may not be intentional or arranged by an institution but is usually organized somehow. There is no form of credit granted by this form of education (Ainsworth, 2010). Non-formal learning can include attending camps, industry certifications, and internships. Informal learning is never organized or guided by a rigid curriculum and is often considered experiential and spontaneous (Ainsworth, 2010). Examples of informal learning include participation in clubs, competitions, conducting self-study, and attending conferences and industry events.

Wagner (2023) proposed in their CyberEducation-by-Design Framework that non-formal and informal learning could be integrated into formal learning to provide enhanced learning for secondary education students to prepare them for future training and education, military service, or beginning their career in the workforce (Figure 1). Although Wagner's framework focuses on secondary education; Formal, Non-Formal, and Informal learning opportunities can be found at any level of education or at various stages in an individual's career.

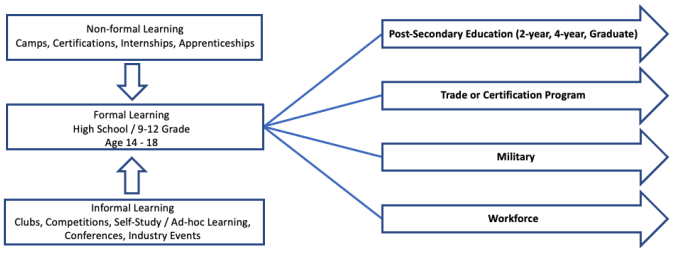


Figure 1 – CyberEducation-by-Design Framework (Wagner, 2023)

Apprenticeship Programs

This paper focuses on apprenticeship programs holistically before focusing on cybersecurity-

specific government initiatives and programs. Apprenticeship programs allow potential employees to gain, develop, and refine their cybersecurity skills while providing insight into the career field. They are considered a cost-effective approach to learning relevant academic, occupational, technical, and soft skills. Apprenticeships are unique in that they enhance the worker (supply) and employer (demand) side of the labor market (Lerman et al., 2020). Additionally, apprenticeship programs "improve the learning process (as students directly apply what they learn), encourage student engagement, increase incentives for students to perform well in academic courses, improve the match between workers' skills and labor market demands, encourage employers to upgrade their mix of jobs, and widen access to rewarding careers for workers who prefer learning by doing over traditional classroom and four-year college models." (Lerman et al., 2020) Further, 71% of individuals involved in apprenticeship programs felt that the programs led to better jobs due to increased salary, acquisition of skills, an expanded professional network, and more interesting work (Page et al., 2020).

The United States Department of Labor identifies six key characteristics of apprenticeships to differentiate this learning opportunity from internships. These are length, structure, mentorship, pay, credential, and college credit. Figure 2 outlines and describes these characteristics.

Apprenticeship
1. Length: 1-3 years
2. Structure: Structured training plan with focus mastering specific skills that an employ is typically looking to fill
3. Mentorship: Individualized training is provide overseen by an experienced mentor
4. Pay: Paid experience that can often lead to fu time employment
5. Credential: Often leads to an industry-recogniz credential
6. College Credit: Often granted; sometimes significant

Figure 2 – Apprenticeship Characteristics (Stoker, 2021)

Government Initiatives for Cybersecurity Apprenticeships

Cybersecurity apprenticeship programs are a subset of the overall apprenticeship programs previously discussed. Sponsors of these programs yield a significant return on investment in high employee productivity (highly skilled in unique roles), high employee retention (91% of apprentices retained employment nine months after program completion), and reduced recruiting costs (lower attrition) (CYAI, 2024). Apprenticeship programs have the potential to fill the increasing skills gaps in high-demand areas such as application development security, cloud security, risk management, threat intelligence, incident response, data privacy and security, compliance and controls, access management, health information security, and security strategy and governance. The projected five-year growth in these skill areas is outlined in Figure 3.

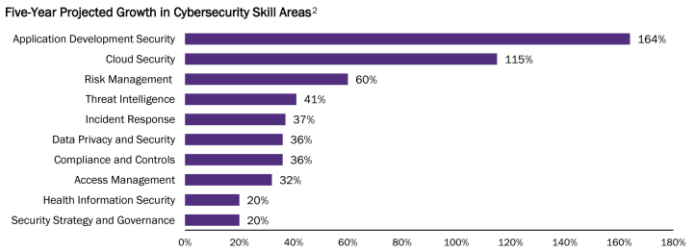


Figure 3 – Five-Year Projected Growth in Cybersecurity Skills Areas (CYAI, 2024)

Cybersecurity apprenticeships are becoming a growing initiative supported by the government. The National Institute of Science and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Apprenticeship Program Finder was a tool developed to support future cybersecurity professionals through paid work experience and work-based learning,
classroom instruction, mentoring, and a nationally- or state-recognized credential upon completion of the program (NIST NICE, 2022).

Reviewing the opportunities compiled on the NICE Cybersecurity Apprenticeship Program Finder identifies 159 unique apprenticeship opportunities; however, there are multiple listings from organizations like Apprenti, Boeing, and Camden Dream Center Technology Training School (NICE, 2024). Of these, nearly 50% (77 opportunities) provide virtual apprenticeship programs (NICE, 2024).

This effort aligns with the Cybersecurity Apprenticeship Sprint led by the Department of

Labor, the White House, the U.S. Department of Commerce, and other federal agencies. The results of this 120-day initiative included:

- 194 cybersecurity registered apprenticeship programs approved or under development,
- Program sponsors added 120 cybersecurity-related occupations to pre-existing and newly registered apprenticeship programs,
- 7,000 apprentices hired,
- Major organizations like IBM, CompTIA, and the Department of Defense (DoD) expanding their programs and Boeing, Cisco Systems, McDonald's, Department of Veterans Affairs, and more launched new programs, and
- Over 2,000 organizations and career seekers expressed interest in learning more about the registered apprenticeship program (The White House, 2022).

3. KUDELSKI APPRENTICESHIP PROGRAM

Kudelski Apprenticeship Program

The Kudelski Group is headquartered in Cheseaux-Sur-Lausanne, Switzerland and is a world leader in digital security. Kudelski selected Phoenix, AZ as its second headquarters in 2016 which serves as the home for its cybersecurity business, Kudelski Security. Kudelski Security provides intelligent cybersecurity that addresses challenges through Managed Security Services (MSS), advisory, customized innovation, and technology consulting (Kudelski Security, 2024). Swiss-based companies see it as their obligation to prepare people for productive and meaningful employment with 30 percent of companies hiring student apprentices (NCEE, 2024). Similarly, Kudelski has utilized three- and four-year apprenticeships for more than twenty years and wanted to demonstrate the viability of youth apprenticeship as a model to develop high-tech talent in the U.S., despite high-tech apprenticeship being a relatively new model in the U.S., and for U.S.-based Kudelski employees. The Kudelski Group is also a signatory to a Memorandum of Understanding between the Swiss Confederation and the U.S. Department of Labor to develop apprenticeship programs in the U.S. Kudelski's Switzerland based IT apprenticeship program includes classroom education and instruction, and On-the-Job-Training (OJT) that provides hands-on application of the conceptual and theoretical aspects taught in the classroom. Kudelski sought to develop an apprenticeship model compatible with the U.S.'s secondary and post-secondary school system and with as much fidelity to the Swiss model as possible. It was also thought that increased utilization of youth apprenticeship could help address the problem of increasing student debt for higher education since apprentices are paid for their work and may also have the benefit of their sponsor company paying for their post-secondary education for further development of skills and expertise.

Partnerships and Planning

Kudelski relocated their Swiss apprenticeship manager to the U.S. in 2018 to work with the U.S.-based staff and to create and implement their apprenticeship strategy. Outreach to the Maricopa Community College District provided Kudelski with an introduction to The Center for the Future of Arizona (CFA), a possible partner to assist in the development of this new endeavor.

CFA is a nonprofit, nonpartisan organization with deep and ongoing work in education, workforce, and civic health with partners at local, state, and national levels including nonprofits, K-12 and higher education, community-based organizations, government, philanthropic, business, and industry. Arizona Pathways to Prosperity (APTP), a CFA impact initiative, is part of the National Pathways to Prosperity movement in collaboration with Jobs of the Future (JFF), the Harvard Graduate School of Education, states, and geographic regions. The National Pathways to Prosperity movement was informed in large part by the Swiss Apprenticeship system, and APTP's implementation was aligned with the Kudelski apprenticeship program. APTP supports educational attainment, creates future opportunities, and leads to upward economic mobility for all young Arizonans while supporting state and regional talent needs. APTP works with educational partners and industry to identify the careers, knowledge, skills, and degrees/credentials businesses need to grow and thrive.

Kudelski and CFA reviewed information on current youth apprenticeships in the U.S. during the development stages of the apprenticeship. Of particular interest and value was the CareerWise youth apprenticeship program, which was founded in 2016, launched its first cohort in 2017, and has seen more than 1,400 apprentices hired by more than 120 employers (CareerWise, 2024). Kudelski and CFA met with CareerWise Colorado leaders to learn from their experiences of launching a successful program which was a hybrid of the Swiss system with adaptations for local education systems, businesses, and industry needs. CareerWise Colorado's three-year apprenticeship model starts during the junior

year of high school, consistent with the Kudelski model in Switzerland and the desired U.S. model.

Meetings held with the Arizona Office of Apprenticeship identified the 4-year competency-based Junior Cybersecurity Analyst apprenticeship role. This role was designed to include the key elements of expert mentorship across the different technical content areas of the apprenticeship, working on projects individually and in teams, and providing the flexibility for Kudelski to incorporate company-specific needs and requirements.

Based on the best information on implementing high-tech youth apprenticeships in the U.S, and the Kudelski apprenticeships in Switzerland, determinations were made about core elements for high school partner selection and the work-based learning structure and hours. The resulting OJT training model included an average of 12 hours per week during their junior year (year one), 16 hours during senior year (year two), 16-20 hours during year three, and 20-24 hours during year four. Year four was typically the second year of post-secondary education. Students are expected to work approximately four hours per day, three to four days per week, from 1-5 pm during years one and two. Schedules are more flexible in years three and four based on apprentices' post-secondary school schedules. Additional hours and flexibility of schedules are supported during summer and school break periods.

Key selection characteristics for the school consisted of:

1) Districts and schools are open to working as a partner with the company and to schedule flexibility. Large enough student body to support desired number of apprentices.
- Big Picture: Commitment to excellence, set students up for success in school and work-based learning.
- Logistics: Accommodate school and business schedule (Monday-Friday; 8 am to 5 pm), course release/seat time, reasonable distance to travel from school to Kudelski.

2) Relevant academic and curriculum infrastructure and teacher support.
- The school has preexisting course curriculum, IT, CS, or cybersecurity ideally; Dual enrollment options.
- A partner teacher who teaches IT/computer science and is committed to serving as the point person to ensure students receive the necessary skills and knowledge in course work.

3) School and parental support to ensure student (apprentice) success in both school and apprenticeship. Most important during the first two years of the apprenticeship.
- Parental support as a critical element for a new model for work experience and maintaining solid academic performance.
- Transportation: Students' ability, with support from caregivers and school, to get to and from the work site.

4) Communication is key: Constant, open channels of communication.
- Ongoing communication on student assignments and progress/performance and opportunities for lead teachers to stay abreast of apprenticeship goals and support them as appropriate with classroom learning.
- Maintaining open communications between partners to respond to changes, issues.

These salient elements for partner selection and building on the core alignment of work-based learning as part of the school's mission:
- Relevant Coursework: Offering coursework in Information Technology (IT), Networking, Computer Science, Cybersecurity, and preferably having dual enrollment course options for students in technical, Mathematics, and English classes.
- Scheduling Flexibility: Ability to commit to allocating some student release time during the school day, to support the minimum of 12 and 16 OJT hours during their junior and senior secondary education years.
- Student Population Size: A large enough student body to support a reasonable number of interested student candidates that would apply for the apprenticeships.
- Student Attributes/Abilities: Students were not expected to have significant technical skills before beginning the apprenticeship. Interest in the field, curiosity, communication skills, and general knowledge and awareness of the IT and cybersecurity field were expected.
- Parent support for students/youth apprentices: Apprenticeship was a new model and required a significant commitment on the part of the student and their families. Approval by a parent or guardian was required for application.

Initially, nine high schools were identified for exploratory discussions based on the school

selection characteristics. Phoenix Coding Academy (PCA) was determined to provide the best opportunity for partnering and mutual success. PCA is a learning community that engages students in computer science pathways and innovative academic experiences that empower them to make confident decisions about their life's journey (PCA, 2024). PCA is a specialty high school and part of the Phoenix Union High School District (PXU), which consists of 24 schools, tens of thousands of students, and over 3,500 employees (PXU, 2024). PCA students are predominately Hispanic (59%) with over 70% of students eligible for free or reduced lunch (NCES, 2023).

PCA focuses on computer coding and multiple technology pathways leveraging inquiry-based instructional design. Academic courses are integrated offering a dynamic, student-centered educational experience and PCA students receive a full high school curriculum consisting of core academic classes, electives, and Career and Technical Education (CTE) classes. CTE pathways include software development (game, application, and web development), computer networking, and cybersecurity which leads to select industry certification, college dual enrollment, and preparation of students for post-secondary success.

Program Roles

PCA would provide technical instruction in networking and security during the first two years of the apprenticeship and meet three to four times per year to ensure complementarity of instruction with planned OJT. Further, PCA and Kudelski would support the development of individualized plans for apprentices to pursue post-secondary education in years three and four of the apprenticeship, based on the apprentices' interests and Kudelski's plans. CFA would operate as an intermediary to facilitate the relationship between PCA and Kudelski while providing outreach, awareness, and the selection process. Kudelski Human Resource (HR) team members provided administrative support, including offer letters and onboarding paperwork, managing changes to wage schedules, and providing non-technical supervision.

Program Outline

Outreach, awareness sessions, and open houses were conducted by Kudelski and CFA during the spring semester of PCA students' sophomore year for students, caregivers, and teachers. Interested students are required to apply and participate in interviews to further explore their interest in technology, cybersecurity, and to discuss students' technology-related school or personal experience or projects. Differences between internships and apprenticeships and the four-year commitment are also explicitly discussed. Team exercises are used to make final selections.

Students take courses in software development (game design, application development, and web development) in additional to traditional courses in English, Math, Science, and Spanish. During students' junior and senior years courses in networking and cybersecurity are taken alongside traditional courses of English, Math, Science, and History. Table 1 outlines the coding academy course sequence. Additionally, Kudelski Security provides related OJT covering topics outlined in Table 2.

Coding Academy Course Sequence – 2023-2024		
Graduation Requirements	**Frosh 1**	**Frosh 2**
4.0 Electives	Software Development 1	Software Development 2
	Exploring Computer Science 1-2	
4.0 Math	Integrated Math 1-2	
4.0 English	Eng 1	Eng 2
3.0 Science		
3.0 Social Studies		
3.0 World Language	Spanish 1	Spanish 2
1.0 Fine Art	Art 1	Art 2
.5 Health (PXU)		
Graduation Requirements	**Soph 1**	**Soph 2**
4.0 Electives	Software Development 3	Software Development 4
4.0 Math	Integrated Math 3-4	
4.0 English	Eng 3	Eng 4
3.0 Science	Bio1/Chem1	Bio2/Chem2
3.0 Social Studies	World History 1-2	
3.0 World Language	Spanish 1	Spanish 2
1.0 Fine Art	Art 1	Art 2
.5 Health (PXU)		

Graduation Requirements	Junior 1	Junior 2
4.0 Electives	*Networking and Cybersecurity 1	*Networking and Cybersecurity 2
4.0 Math	Integrated Math 5-6	
4.0 English	Eng 5	Eng 6
3.0 Science	Environmental Science	
3.0 Social Studies	World History 1-2	
3.0 World Language	Spanish 3	Spanish 4
1.0 Fine Art		
.5 Health (PXU)		
Graduation Requirements	**Senior 1**	**Senior 2**
4.0 Electives	*Networking and Cybersecurity 3	*Networking and Cybersecurity 4
	Gifted Seminar (open to all students)	
4.0 Math	*College Algebra	
4.0 English	Eng 7	Eng 8
3.0 Science	*Physics 1-2 (optional)	
3.0 Social Studies	Govt/Econ	
3.0 World Language		
1.0 Fine Art	Art 3	Art 4
.5 Health (PXU)	Health	
* Dual Enrollment with Phoenix College		

Table 1 – Phoenix Coding Academy Course Sequence (PCA Course Sequence, 2024)

Kudelski OJT Outline	
Year 1	Systems, Networking, Firewall Management, Active Directory Infrastructure, IT Support
Year 2	Phishing Campaigns, Security Risk Management, Cloud Computing, Threat Intelligence
Year 3	Client Engagement, Vulnerability Management, Burp Suite, Penetration Testing
Year 4	Vendor Support, Security Frameworks, Information Security Tools, Security Analysis
Continuous	Business Writing, Communication Across Generations, Culture Competency, Embracing Change, Emotional Intelligence, Establishing Goals, Excel, Project Management, Professionalism in the Workplace

Table 2 – Kudelski Security OJT Outline

Apprentices are provided the opportunity to study and test for industry-recognized certifications. These include several CompTIA certifications (IT Fundamentals+, Network+, Security+), Juniper, F5, Security Journey, Amazon Web Services (AWS), Proof Point, and Open Source Intelligence (OSINT).

Program Costs

The primary cost of the program is the hourly rate paid to apprentices which is subject to increases based on participation in the company's formal annualized performance and salary review process. Apprentices are eligible for education and training-related funding consistent with the Kudelski's U.S. tuition assistance program. Additionally, apprentices are eligible for pro-rated benefits depending on the average number of hours worked. Other major costs include the portion of time technical leads allocate to apprentices away from their primary job role, and the cost of time provided by Kudelski HR personnel supporting the apprenticeship program. Additional costs include laptops provided to students for post-secondary courses, external training, equipment and/or materials for training and education, and certification associated costs deemed appropriate for the apprentices.

4. OUTCOMES AND LESSONS LEARNED

Outcomes

The Kudelski-PCA Youth Apprenticeship program launched in September 2019 with two apprentices. As of spring 2024, the two apprentices from Cohort 1 and one apprentice from Cohort 2, completed their fourth and final year of the apprenticeship and all were offered and accepted roles as Tier 1 Cybersecurity Analysts, demonstrating that apprentices became valuable members of the team during their apprenticeship and were positively perceived by colleagues. Additionally, there are currently four apprentices in each of the four years of the

apprenticeship program, and all apprentices are continuing from one year to the next. The apprenticeship program has demonstrated that individuals can develop the KSAs needed for a Cyber Security Analyst role without a four-year degree, although all three apprenticeship completers, and all of the high school graduates, are pursuing post-secondary education in Arizona, demonstrating apprenticeship as a model for college and career. Additionally, of the 16 current apprentices and three apprenticeship completers, eight are female, eleven are male, and 61% identify as Hispanic, demonstrating the ability to attract and retain diverse talent for cybersecurity apprenticeships.

Several other high level outcomes were identified:

- Kudelski increased program participants from two per year to accepting between four and five apprentices, indicating program success, organizational support, and improved and streamlined processes supporting the apprentices.
- The apprenticeship program continues to attract more students and applicants each year indicating positive perception of the program and status of the opportunity.

Challenges

As with all new programs, several challenges were identified. The first was scheduling. While Kudelski's Cyber Fusion Center operates 24/7, non-security operations center employees on the Kudelski team predominately work Monday through Friday, primarily from 8 am to 5 pm. This limited the days and hours students could complete their OJT hours, requiring students to be released from school during normal classroom time. Fortunately, PCA's principal and lead educator supported this based on the unique opportunity to provide directly related hands-on experience complementing or replacing missed classroom time during students' junior and senior years. Also, this provided a unique experience to learn extremely important professional skills in addition to the technical skills. Further, it was occasionally necessary for students to take online classes to balance their academic and apprenticeship schedules. Fortunately, due to COVID, PCA and students became adept at working with online courses.

The COVID pandemic was the second challenge which began during the first year of the apprenticeship program. COVID-related school and business restrictions required moving apprentices to a remote and virtual experience for the first two cohorts. Students were allowed to return to the workplace when PCA returned to in-person classes in March 2021. PCA, CFA, and Kudelski maintained frequent remote meetings to ensure sustained communication and progress in the apprenticeship and student success.

Transportation represented another challenge. Most students do not drive or have reliable transportation. A bus-line was located approximately 15 minutes from PCA and was one source of transportation to Kudelski, but alternative forms of transportation were required placing an additional burden on caregivers or others, especially for students to return home. Kudelski's sustained commitment to the apprenticeship program and increased volume in students provided the ability for PCA to secure a bus to assist with transportation, beginning in 2022. Third and fourth-year apprentices continue to rely on caregivers and public transportation as their primary source of transportation.

Finally, it became clear early in the apprenticeship program, that attention was needed to address the challenge of student apprentices who were required to transition from being teenage friends and classmates in the morning to peers and work professionals at Kudelski Security in the afternoon. This required time and adjustment for the apprentices as this was their first job experience. Additional HR-related training was developed to help apprentices better understand appropriate and inappropriate behavior in the workplace. Support was provided to help Kudelski staff mentor and guide young adults.

Lessons Learned

The success of the apprenticeship program to develop qualified talent for the security operations team was due first and foremost to the commitment of the Kudelski CEO and his executive team and the understanding across Kudelski Security of the importance of this initiative. The second core element was the opportunity for the apprentices to have on-going exposure to and use of state-of-the-art, high-tech tools, and work with and learn from experienced technical leads in a live environment. Additionally, apprentices observed and participated in meetings with customers which provided critical experience and context.

Kudelski's HR support, which coordinated work experiences, was a critical component of the apprenticeship program especially as the program reached maximum size across the four years. Exercising schedule flexibility for exams and projects, family priorities, and occasionally

allowing a student time to return to a solid level of academic performance, was often the purview of the HR team to manage internally. Additionally, HR team roles changed throughout the program. They facilitated updates to content and delivery models as the program grew and technical leads changed due to differing work assignments. They handled HR-related questions and issues with apprentices and caregivers. This work and flexibility was critical to the success of the program.

CFA provided the intermediary role. Facilitating the partnership and relationships between Kudelski and PCA and ensuring understanding of the business and education environment was a critical component to program sustainability. Kudelski's HR and technical leads changed during the third year of the apprenticeship. The consistent and ongoing engagement of both intermediary CFA and school partner PCA, along with the unwavering commitment of Kudelski CEO and his team ensured a successful transition.

Caregiver support cannot be overestimated. The 4-year commitment to the apprenticeship, support for missing class time in years one and two, and providing transportation are critical elements that make the apprentices and the program successful, as both caregivers and students navigate a new experience. Related, is the importance of organization, prioritization, and time management developed by apprentices and supported by caregivers.

Apprentices were required to share and report on research and projects they accomplished, resulting in the development of strong presentation, verbal and written communication skills. Additionally overlapping projects across apprenticeship years provide opportunities for more senior apprentices to lead assignments or projects with supervision from technical leads to develop leadership skills which proved to be a good model for apprentices' growth.

5. FUTURE WORK

The apprenticeship program will continue with the sixth cohort of four juniors in the fall 2024-2025 school year. Year six will focus on enhancing opportunities for the apprentices to explore additional career choices beyond direct security operations roles. Additionally, planning for the potential that upon completion of the apprenticeship some apprentices may not meet the needs of Kudelski or may want to pursue options outside of Kudelski, will also be part of future considerations.

Having successfully completed two full four-year cycles provides the opportunity for reflection and analysis. Documenting the OJT curriculum for use internally and externally, and presenting at technical and workforce conferences, as well as meeting with interested companies and school districts, will be pursued. Documentation of high school partner and intermediary roles will be evaluated and completed as part of process refinement. Successfully managing the apprenticeship program during COVID also provides the opportunity to consider alternative or virtual apprenticeship models. Identifying forms of financial support to offset program costs or replicate the program with other companies and school districts will also be explored.

6. CONCLUSIONS

The cybersecurity youth apprenticeship program described in this paper demonstrated a viable solution in addressing the cybersecurity workforce shortage by providing hands-on training and work experience to students. The program's longevity and growth can be attributed to the unwavering commitment of the administrators and teachers at Phoenix Coding Academy, Kudelski Security's executive and technical teams, and the caregivers and students involved in the program. The apprenticeship's focus on developing technical skills, professional attributes, and leadership abilities resulted in a pipeline of qualified talent for the security operations team. The program's adaptability to the challenges posed by COVID-19 demonstrates an ability to pivot and maintain momentum despite unforeseen circumstances. The importance of HR support, caregiver involvement, and organizational commitment ensured the success of this initiative.

This apprenticeship model offers valuable insights for organizations seeking to develop their own talent pipelines or address similar workforce shortages. Specifically, the program's emphasis on experiential learning, mentorship, and leadership development highlights the importance of investing in the next generation of cybersecurity professionals.

Future work is essential to refining the model for continuous improvement and expansion to other organizations or states. Additionally, exploring alternative or virtual apprenticeship options and identifying forms of financial support to offset costs or replicate the program with other companies and school districts is needed. The Kudelski Security Apprenticeship Program serves as a model for innovative workforce development

initiatives, demonstrating that by investing in the next generation, organizations can build a more skilled and diverse workforce and drive business success.

7. REFERENCES

Ainsworth, H. and Eaton, S. (2010, July 31). Formal, non-formal and informal learning in the sciences. Onate Press. https://files.eric.ed.gov/fulltext/ED511414.pdf.

CareerWise (2024). Making Youth Apprenticeship a Reality. https://www.careerwiseusa.org/our-story/.

"Cyberseek Supply and Demand Heat Map," (2024), Cyberseek.org, https://www.cyberseek.org/heatmap.html.

"How the Economy, Skills Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce," (2023), International Information System Security Certification Consortium (ISC2), https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e.

Kudelski Security (2024). About Us. https://kudelskisecurity.com/.

Lerman, R., Loprest, P., & Kuehn, D. (2020, October), "Training for Jobs of the Future: Improving Access, Certifying Skills, and Expanding Apprenticeship," IZA Policy Paper, No. 166, Institute of Labor Economics (IZA), Bonn, http://hdl.handle.net/10419/243452.

NCEE (2024). Global Perspectives: Expanding Youth Apprenticeships: Taking a Page from Switzerland. National Center on Education and the Economy (NCEE). https://ncee.org/quick-read/expanding-youth-apprenticeships-taking-a-page-from-switzerland/#:~:text=Swiss%20employers%20see%20it%20as,companies%20regularly%20hire%20student%20apprentices.

NCES (2023). Phoenix Coding Academy School Directory Information. National Center for Education Statistics (NCES). https://nces.ed.gov/ccd/schoolsearch/school_detail.asp?Search=1&DistrictID=0406330&ID=040633003509.

"NICE Apprenticeship Program Finder", (2024), National Institute of Science and Technology National Initative for Cybersecurity Education, https://www.nist.gov/nice/apprenticeship-finder.

NIST NICE (2022, January 10). NICE Cybersecurity Apprenticeship Program Finder. National Institute of Science and Technology (NIST). https://www.nist.gov/itl/applied-cybersecurity/nice/resources/apprenticeship-finder.

Page, L., Narel, R., & Beligio, E. (2020), "Skills Gap Challenge: How Apprenticeship Programs Address Skill Building and Educational Advancement," Journal of Organizational Psychology, Vol 20(6), https://articlearchives.co/index.php/JOP/article/view/4668/4630.

PCA Course Sequence (2024). Coding Academy program of study for 2023-2024 school year. https://www.pxu.org/domain/5481.

PCA (2024). Phoenix Coding Academy Welcome. https://www.pxu.org/coding.

"Protecting Digital Infrastructure: Securing Talent in Cybersecurity," (2024), Cybersecurity Youth Apprenticeship Initiative (CYAI), https://www.apprenticeship.gov/sites/default/files/CYAI_cybersecurity-skills-in-demand.pdf.

PXU (2024). Phoenix Unified School District (PXU). https://www.pxu.org/info.

Ross, W. and Duke, E. (2018). "Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Security Amerian Future," Secretary of Commerce and Secretary of Homeland Security, https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/supporting-growth-and-sustainment.

"State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources, and Cyberoperations," ISACA, https://www.isaca.org/state-of-cybersecurity-2023?utm_source=other&utm_medium=other&utm_campaign=pr_both_content_survey-report_state-of-cybersecurity-survey-2023_quarter-3-2023_state-of-cybersecurity-2023-press-release&utm_content=state-of-cybersecurity-survey-2023_state-of-cybersecurity-2023-press-release&cid=pr_3000043&Appeal=pr

Stoker, G., Clark, U., Vanajakumari, M., and Wetherill, W. (2021, April). Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned. Information Systems Education Journal (ISEDJ). https://files.eric.ed.gov/fulltext/EJ1297604.pdf.

Wagner, P. (2023, May 19). "CyberEducation-by-Design: Developing a Framework for Cybersecurity Education at Secondary Education Institutions in Arizona," https://scholar.dsu.edu/theses/430/.

White, A. and Bunce, J. (2023). Generative AI and cybersecurity: Bright future or business battleground? Sapio Research. https://info.deepinstinct.com/voice-of-secops-v4-2023?_ga=2.86841240.1038042311.1705606129-1595372854.1705443616.

White House (2022, November 15). FACT SHEET: Biden-Harris Administration Accomplishes Cybersecurity Apprenticeship Sprint. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/15/fact-sheet-biden-%E2%81%A0harris-administration-accomplishes-cybersecurity-apprenticeship-sprint/

Teaching Case:

Reshaping Cybersecurity Ethics Education: Evaluating a Posthumanist Pedagogy Using Human/AI Co-Generated Case Studies

Ryan Straight
ryanstraight@arizona.edu

Jonathon Lowery
jrl84623@arizona.edu

David Poehlman
dpoehlman@arizona.edu

Waamene Yowika
waamene@arizona.edu

Cyber, Intelligence, and Information Operations Department
University of Arizona
Tucson, AZ 85719

Hook

As the lines between human intuition and machine intelligence blur, AI-powered case studies push the boundaries of how we design and deliver instructional materials, offering a glimpse into the future of cyber praxis.

Abstract

This paper investigates the development, implementation, and pedagogical efficacy of AI-generated case studies and scenarios for cybersecurity ethics education. Employing a generative AI model, we developed learning materials for a cybersecurity ethics course, emphasizing a collaborative human-AI approach that resulted in a series of realistic and complex scenarios. These scenarios address core ethical concepts, foster critical thinking, and demonstrate adaptability to diverse learning preferences while maintaining relevance to contemporary cybersecurity challenges. While challenges such as advanced terminology use were identified through qualitative feedback, they were addressed through targeted interventions. This work situates itself within a posthumanist inquiry framework, exploring the evolving, co-constitutive relationship between human and non-human entities in educational contexts. Findings from a pilot implementation (n=23) indicate that the AI-generated scenarios significantly enhanced student engagement and perceived learning outcomes, with over 90% of participants reporting improved comprehension of core concepts and critical thinking proficiencies. This study contributes to the discourse on the intersection of AI, cybersecurity, and education, highlighting the potential of posthumanist pedagogical approaches.

Keywords: case studies, scenarios, artificial intelligence, posthumanism, ethics, teaching

Recommended Citation: Straight, R., Lowery, J., Poehlman, D., Yowika, W., (2025). Reshaping Cybersecurity Ethics Education: Evaluating a Posthumanist Pedagogy Using Human/AI Co-Generated Case Studies. *Cybersecurity Pedagogy and Practice Journal.* v4, n1, pp 24-34. DOI#: https://doi.org/10.62273/DTJD9647

Reshaping Cybersecurity Ethics Education: Evaluating a Posthumanist Pedagogy Using Human/AI Co-Generated Case Studies

Ryan Straight, Jonathan Lowery, David Poehlman and Waamene Yowika

1. INTRODUCTION

The integration of artificial intelligence (AI) into cybersecurity practices has propelled ethical considerations to the forefront, transforming them from mere discussion points into fundamental challenges to traditional notions of human agency, particularly within educational contexts. As cybersecurity professionals increasingly encounter complex ethical dilemmas with the potential to shape societal and cultural trajectories, the role of ethical principles in guiding the responsible development and implementation of AI systems becomes paramount (Blanken-Webb et al., 2018; González et al., 2024). This is particularly crucial given the significant global shortage of qualified cybersecurity professionals, estimated at 3.4 million in 2022 (Lake, 2022). This workforce deficit, coupled with the heightened demand for cybersecurity expertise, has intensified the focus on cybersecurity education (Matei & Bertino, 2023; P. Wang, 2022). The situation is further complicated by the fact that cybersecurity specialists often confront unpredictable ethical dilemmas that are not adequately addressed by existing legal frameworks or codified standards (Adaryukova et al., 2020). This lack of definitive guidelines, combined with the emerging potential of human-AI collaboration in educational content creation, underscores the imperative for innovative pedagogical approaches in cyber ethics education. These approaches must not only address the technical skills gap but also foster a nuanced understanding of the ethical complexities inherent in the cybersecurity domain.

A logical starting point for comprehending this evolving pedagogical landscape is to examine the established learning benchmarks and standards. The K-12 Cybersecurity Learning Standards, developed by CYBER.ORG (Cyber Innovation Center & CYBER.ORG, 2021), provide a comprehensive framework for introducing students to foundational cybersecurity concepts and equipping them with the requisite technical skills and knowledge to pursue careers in the field. Likewise, the National K12 Cybersecurity Education Roadmap (National Initiative for Cybersecurity Education (NICE), 2021) maintains a coordinated portfolio of national K12 cybersecurity education activities, designed to ensure the effective deployment of resources and optimize impact. At the post-secondary level, the National Security Agency's (NSA) Centers of Academic Excellence designations provide guidance aimed at establishing "standards for cybersecurity curriculum and academic excellence" (ibid.). Collectively, these initiatives, alongside the NSA's 2024 development of AI-focused standards, underscore the fundamental integration of AI across all cyber-related domains, particularly within education, signaling a shift towards even more technology-integrated learning environments.

However, translating theoretical AI ethics principles into practical pedagogical applications remains a significant challenge. The gap in formal ethical training and clearly defined ethical criteria for educating future cybersecurity experts (Jackson et al., 2023) has created an opening for the development of cognitive assemblages (Hayles, 1999)—synergistic interactions between human and artificial intelligence—in educational contexts. This paper posits that a posthumanist theoretical framework offers a valuable lens through which to examine this pedagogical innovation and the evolving, co-constitutive relationship between humans and AI in educational settings. One promising approach is the use of AI-generated case studies and scenarios, which can provide students with dynamic and engaging learning experiences while simultaneously instantiating intra-action (Barad, 2007) between human learners and technologically-mediated scenarios. This framework conceptualizes the learner and learning material not as pre-existing, independent entities, but rather as mutually constituted through their interaction, highlighting the dynamic interplay between human cognition and AI-generated content.

This paper investigates the development, implementation, and pedagogical efficacy of AI-generated case studies and scenarios for teaching cyber ethics, law, and policy, considering three crucial contexts: the current state of cybersecurity education, the imperative for diverse and inclusive approaches, and the

implications of AI for pedagogy. Grounded in both posthumanist theoretical frameworks and empirical evidence derived from a pilot implementation (n=23), we analyze how the collaborative interplay between human and artificial intelligence can yield effective learning materials while simultaneously challenging traditional notions of agency and expertise in educational contexts. This investigation contributes to the broader scholarly discourse on the intersection of AI, cybersecurity, and education, highlighting both the practical efficacy and theoretical implications of innovative posthuman pedagogical approaches, particularly the potential for AI-generated scenarios to foster deep engagement and enhance learning outcomes in cybersecurity ethics education.

2. LITERATURE REVIEW

A robust cybersecurity education should adopt a holistic approach, integrating both technical and non-technical content, and be grounded in rigorous research (Austin, 2020; Blair et al., 2020). The integration of ethics within the cyber domain is particularly crucial yet complex, requiring a nuanced balance between competing interests, such as security and civil rights. Moreover, accelerating technological advancement necessitates a continuous reevaluation of ethical considerations, which often serve as a catalyst for policy development (Navdeep, 2022). Existing pedagogical approaches in cyber education have increasingly incorporated ethics into cybersecurity curricula, aiming to cultivate students' ethical awareness and decision-making skills (Adaryukova et al., 2020; P. Wang, 2022). These initiatives underscore the growing recognition of the importance of such integration. However, mere memorization of laws and codes of ethics does not constitute a comprehensive ethics education for cybersecurity, a field that remains under-studied and insufficiently addressed in academic discourse (Blanken-Webb et al., 2018; Dexter et al., 2013). To tackle these limitations, innovative pedagogical approaches that actively engage students in realistic ethical decision-making scenarios are imperative.

Scenario- and case study-based pedagogical approaches have proven effective in introducing major domain concepts in technical cyber skills training, such as penetration testing (X. Wang & Bai, 2022). Furthermore, their efficacy has been demonstrated in the domain of cyber ethics education, providing students with practical experience in analyzing ethical dilemmas, immersing them in realistic scenarios, and fostering ethical reasoning skills (Adaryukova et al., 2020; Blanken-Webb et al., 2018). Similarly, interactive and game-based learning have been identified as effective methods for increasing awareness and interest in cybersecurity and related career paths (Triplett, 2023). However, curricular constraints, such as time limitations and a scarcity of readily available resources, can impede the implementation of these approaches (Kilhoffer et al., 2023). Moreover, early and structured ethical training related to AI applications in cybersecurity is necessary to bridge the gap between students' perceived and actual ethical preparedness (Matei & Bertino, 2023).

In addition to the pedagogical challenges, the field of cybersecurity education faces significant hurdles in terms of diversity and inclusion. Notably, women remain underrepresented in the cybersecurity workforce (Pinchot et al., 2020), necessitating the implementation of novel recruitment strategies targeting females across the K-20 educational spectrum (Rowland et al., 2018). Research indicates that girls often demonstrate improved learning outcomes when pedagogical approaches incorporate socialization and frequent interaction (Kim, 2016). Furthermore, peer mentorship has been identified as a critical factor in the success of cybersecurity programs for both women and men (Pinchot et al., 2020).

The integration of AI into educational practices raises fundamental questions about the nature of learning and the role of technology in shaping educational experiences. While much of the extant literature on AI in education conceptualizes AI as a tool subservient to teaching and learning (Veletsianos et al., 2024), this perspective may not fully encompass the complex relational interactions already underway between humans and AI (Woodward, 2023). As AI systems continue to advance, the potential for them to develop consciousness or sentience cannot be *entirely* dismissed, raising ethical considerations about the possibility of granting them certain protections and responsibilities typically associated with personhood (Osborne & Rose, 2024). However, it is crucial to acknowledge that current AI systems still–at time of publication–exhibit significant limitations when compared to human capabilities, and companies like Google strongly refute assertions that their advanced language models have attained any form of sentience (ibid.). The future role of AI as virtual and persistent, lifelong pedagogical agents remains uncertain yet plausible, thereby necessitating a continuous and consistent

reevaluation of educational approaches involving AI.

The successful integration of AI into educational practices is also contingent upon teachers' perceptions of educational technology and their willingness to adapt traditional pedagogical methods (Lin, 2022). Furthermore, students require adequate training and time to effectively utilize AI-assisted learning tools. AI-powered text analysis tools can be effectively integrated into innovative pedagogical approaches (O'Halloran, 2020), and story completion methods can be employed to elicit deeper insights from participants while fostering agency and creativity (Veletsianos et al., 2024).

As education confronts a period of rapidly accelerating change, it is imperative to consider novel approaches to thinking and teaching (Wallin, 2017). By affording students realistic and engaging learning experiences, AI-generated case studies and scenarios can contribute to the development of the ethical awareness and decision-making skills necessary for navigating the complex ethical dilemmas they are likely to encounter as future cybersecurity professionals (Adaryukova et al., 2020; Blanken-Webb et al., 2018).

3. METHODOLOGY

The study employed a developmental research approach within the context of a Cyber Ethics course. The course aligns with the National Security Agency's (NSA) required knowledge units for a Center of Academic Excellence in Cyber Operations (CAE-CO), and the learning objectives for each module are meticulously aligned with these requirements. To develop engaging and intellectually stimulating scenarios for the course's seven modules, an iterative, AI-assisted scenario development process was used. This process leveraged the capabilities of the Claude 3 Opus model, a generative AI developed by Anthropic PBC. The AI model was provided with comprehensive guidelines including the learning objectives, key concepts, readings, lecture notes, and desired complexity level for each module. A team of collaborators, consisting of one graduate student (JL) previously enrolled in the graduate version of the course and two undergraduate students (WY and DP), played an integral role in providing feedback and guidance throughout the development process. The AI model generated an initial set of scenarios based on the provided guidelines, which were subsequently reviewed and refined based on collaborator feedback. This feedback focused on assessing the relevance, clarity, level of engagement, and alignment of the scenarios with the specified learning objectives. This iterative process continued until a final set of scenarios was developed, representing a co-constitutive entanglement between human and artificial intelligence, as conceptualized within a posthumanist framework.
.

4. SCENARIO DEVELOPMENT

The AI-assisted scenario development process made possible the rapid and efficient creation of multiple scenarios tailored to the specific pedagogical needs of the course and informed by the perspectives of current and prospective students. This approach aimed to ensure that the scenarios were engaging, relevant, and effective in promoting critical thinking and fostering meaningful discussions surrounding the ethical, legal, and policy considerations inherent in the cyber domain. Scenarios were developed for each of the seven modules in the course. Each module addresses a distinct aspect of the subject matter, aligned with the NSA's CAE-CO knowledge unit requirements:

- **Module 1**: Examination of the evolution from classical Western ethical thought to cyber ethics, exploring how traditional moral frameworks adapt to digital environments, and establishing foundational concepts in information ethics.
- **Module 2**: Introduction to the fundamental concepts of cybersecurity ethics, including ethical frameworks and principles that guide decision-making processes in this domain and the contemporary philosophical underpinnings thereof.
- **Module 3**: Examination of the legal landscape governing cybersecurity, exploring relevant laws, regulations, and judicial precedents.
- **Module 4**: Focus on the policy dimensions of cybersecurity, discussing the roles and responsibilities of various stakeholders—including governments, organizations, and individuals—in shaping cybersecurity policies.
- **Module 5**: Addressing the ethical and legal implications of privacy and data protection within the context of cybersecurity, a particularly critical topic in the contemporary digital age.
- **Module 6**: Examination of the ethical and legal considerations surrounding cybercrime and cybersecurity incidents,

including issues such as attribution, jurisdiction, and response mechanisms.
- **Module 7**: Exploration of the future trajectory of cybersecurity ethics, law, and policy, considering the potential impact of emerging technologies and the evolving threat landscape.

The AI generated scenarios designed to be realistic and relevant to contemporary cybersecurity challenges. This was accomplished using the Quarto scientific publishing system to create interactive, rich documents, while using plain text markdown and CSS for styling. As such, they maintained readability and portability when engaging with the AI model. Module 5, for example, featured a scenario exploring the legal and ethical ramifications of a fictional smart home device company surreptitiously collecting and sharing user data. The final scenarios emulated a dossier-like format, incorporating an overview, diverse background information, "main characters" who served as individuals of interest, and a detailed timeline. To increase realism, each case included fabricated supplementary materials described above. This format not only provided students with a realistic perspective but also allowed for the integration of other relevant cyber-related skills, such as open-source intelligence gathering through detailed readings, while necessitating deep, critical engagement with the materials.

5. TEACHING GUIDE

Notwithstanding the relative ease and expediency afforded by contemporary generative AI, the effective integration of AI-generated scenarios into the curriculum necessitates meticulous planning and skilled facilitation to ensure that students engage in meaningful discussions and cultivate a profound understanding of the domain. In conjunction with the provided supplemental materials, the following teaching guide outlines the process for incorporating the scenarios into the course, encompassing suggested discussion questions, activities, and strategies for fostering productive conversations.

1. Introduction and Contextualization: begin by contextualizing each scenario within the framework of the corresponding module's learning objectives. This approach enables students to concretely identify the relevance of the scenario and discern the key concepts upon which they should focus. Subsequently, provide a succinct overview of the scenario, introducing its principal characters or stakeholders to establish a foundation for the ensuing discussion.
2. Engaging with the Scenario: encourage active engagement with the scenario through carefully crafted discussion questions and interactive activities.
    - Discussion Questions: discussion questions constitute a critical component of the teaching guide, as they prompt students to engage in critical thinking about the scenario and explore its multifaceted ethical, legal, and policy dimensions. For each scenario, develop a set of open-ended questions that encourage students to consider the perspectives of diverse stakeholders, analyze the potential ramifications of various courses of action, and evaluate the scenario through the lens of pertinent ethical frameworks and legal principles.
    - Interactive Activities: in addition to discussion questions, incorporate activities that enable students to actively engage with the scenario and apply their knowledge in a practical manner. For instance, students could be tasked with role-playing different stakeholders in the scenario, debating the merits of various courses of action, or presenting arguments for or against a particular decision. Alternatively, students could collaborate in small groups to formulate guidelines or recommendations for addressing the ethical, legal, or policy challenges presented in the scenario.
3. Facilitating Meaningful Discussions: when facilitating discussions, draw explicit connections between the scenarios and real-world events or current developments in the cybersecurity domain. This approach helps students apprehend the relevance and applicability of the concepts they are learning to authentic contexts. Encourage students to share their personal experiences or insights related to the scenario to further enrich the discussion and promote peer-to-peer learning. A posthumanist-informed pedagogy encourages explicit consideration of the AI's role in shaping the scenarios and the attendant ethical

complexities. This pedagogical approach invites students to critically examine the co-constitutive nature of human-AI interaction in the context of scenario development.

4. Cultivating a Safe and Inclusive Environment: to facilitate meaningful and productive discussions, it is imperative to cultivate a safe and inclusive learning environment where all students feel empowered to articulate their thoughts and perspectives. Establishing ground rules for respectful dialogue and encouraging active listening are essential to fostering a constructive exchange of ideas. As the instructor, guide the discussion, elucidate concepts when necessary, and ensure that all students have the opportunity to contribute.
5. Extending Learning Beyond the Classroom: conclude by providing students with resources for further learning and exploration, such as supplementary readings, case studies, or online resources that delve deeper into the ethical, legal, and policy aspects of cybersecurity. Encourage students to continue engaging with these topics beyond the classroom to foster a more comprehensive understanding of the field and better prepare them for future challenges in their professional endeavors.

The development and utilization of fictional—which is to say realistic but not verifiably real—case studies and scenarios has been demonstrated to be effective for fostering engagement and eliciting varied student responses (Orchard, 2019). To illustrate the potential impact and pedagogical affordances of such AI-generated scenarios, the student co-authors of this work—who also assisted in the development of scenarios—provide the following perspective in a later section.

6. STUDENT PERSPECTIVES

AI-generated scenarios offer numerous benefits for engaging students in the study of cyber ethics, law, and policy. By leveraging accurate information from pre-verified sources and real-life similarities, AI models can craft lifelike scenarios that captivate students' attention and provide them with realistic contexts to explore complex concepts. The depth and breadth of the content presented in these scenarios can keep students engaged and motivated to learn more about the subject matter, sparking interest in further self-study. One of the key advantages of AI-generated scenarios is their adaptability to different learning preferences in terms of modality, presentation, and interaction. These scenarios can be tailored to address contemporary issues related to cyber ethics and legislation, making the content more relevant and engaging for students.

In addition to the benefits mentioned above, AI-crafted scenarios can be created in a fraction of the time compared to traditional methods. AI models can utilize accurate information previously ingested by programmers and maintainers to craft scenarios, such as through the use of locally stored, pre-verified material or corroborated web-based content. Furthermore, these scenarios can be cross-referenced with other up-to-date models and real-life similarities using prompting techniques, thereby adding depth and value that can captivate students.

However, it is important to acknowledge the challenges associated with AI-generated scenarios. While models like ChatGPT can create compelling and easily digestible content, they may occasionally utilize terminology that is beyond the understanding of students new to the material. To mitigate this issue, providing a list of necessary terminology definitions can help ensure that students are well-informed and equipped to engage with the scenarios effectively.

The use of AI-generated scenarios in learning can be likened to the "Method, Opportunity, and Motive" model in cybersecurity. In this context, the AI-crafted scenarios serve as the method, providing students with the opportunity to explore and learn from realistic situations. While the initial motive may be to achieve a passing grade, the ultimate goal is to foster a genuine interest in the subject matter, encouraging students to pursue further learning independently.

Taken altogether, such AI-generated scenarios offer a powerful tool for engaging students in the study of cyber ethics, law, and policy. By providing realistic, adaptable, and thought-provoking content, these scenarios can captivate students' interest, promote practical application of complex concepts, and contribute to a more effective and engaging learning experience.

7. PILOT IMPLEMENTATION AND ANALYSIS

To evaluate the pedagogical efficacy of these AI-generated scenarios, a pilot implementation was conducted, followed by a comprehensive

quantitative and qualitative analysis, the findings of which are presented in the following section. The assessment protocol, theoretically grounded in posthumanist principles, used 5-point Likert-scale items and open-ended questionnaires to assess participant engagement, perceived learning gains, and the perceived efficacy of the scenarios in addressing topics within the domains of ethics, law, and policy. The protocol was specifically designed to capture traditional pedagogical metrics, identify indicators of intra-action between participants and the AI-generated content, and to acknowledged the "cognitive assemblage" (Hayles, 1999)–the synergistic interaction between human learners and AI-generated content–seeking to understand how this relationship manifests in educational outcomes. Data collection was conducted during the fall semester, engaging all enrolled students in the course. The response rate was 100% (n=25), with one response being incomplete, and one response being an outlier, and thus removed from quantitative analysis. The assessment instrument was designed to capture both traditional pedagogical metrics and indicators of intra-action between human learners and the technologically-mediated scenarios.

It is important to acknowledge the limitations of self-reported data, however. To mitigate, survey responses were unidentified, triangulated between quantitative (Likert) and qualitative (open-ended questions) data, allowing for cross-referenced validation, and participants were not provided any compensation or accolades. Despite these precautions, it's understood that self-reported perceptions may not perfectly correlate with improvements in domain mastery. This limitation presents opportunities for future research that is currently being designed.

8. RESULTS

Analysis of the survey data revealed compelling evidence for the effectiveness of AI-generated scenarios in fostering student engagement and facilitating deep learning in cyber ethics education. The quantitative data indicated consistently positive responses across three key dimensions: engagement with the AI-generated materials, perceived learning outcomes, and scenario effectiveness (see Table 1).

Table 1: Percentage of students who agreed or strongly agreed with statements about the AI-generated case studies.

Statement	M	SD	% Agree
The scenarios captured my interest.	4.65	0.49	100.0
The scenarios helped me understand key course concepts.	4.26	0.81	91.3
The scenarios were more engaging than traditional lectures.	4.35	0.71	95.7
The scenarios motivated me to think deeply about the issues.	4.30	0.70	95.7
The scenarios increased my confidence in applying course concepts.	4.17	0.78	91.3
The scenarios helped me grasp the complexities of the subject matter.	4.17	0.78	91.3

Note. Agreement reflects the percentage of students who selected "Agree" or "Strongly Agree" on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree).

.

The scenarios proved particularly effective in conveying complex ethical concepts. Students reported high levels of engagement with the material, with the majority indicating strong agreement that the scenarios motivated deeper thinking about cyber ethics, law, and policy issues. This engagement demonstrably translated into perceived learning outcomes, with students reporting an improved understanding of key concepts (M = 4.26, SD = 0.81) and increased confidence in applying course content to real-world situations (M = 4.17, SD = 0.78). This suggests the formation of *posthuman ethical assemblages* or learning environments where ethical understandings emerge not from solely directed interactions of humans *at* content, but rather a dynamic interaction between learners, the case studies, and the AI-based technical infrastructure that facilitates their interaction.

Thematic analysis of qualitative responses identified several recurring patterns that point to the posthuman dimensions of the AI-generated scenarios. Students consistently emphasized the value of multiple document types (news stories, social media posts, leaked emails, law enforcement reports, so on) and perspectives in enhancing their understanding of complex cybersecurity situations. As one participant articulated, "the integration of the AI Avatar into daily life was particularly fascinating and made the ethical implications feel more immediate and relevant." This finding aligns with "transversal connections" (Ferrando & Braidotti, 2019),

underscoring the participants' intuitive linking of the scenarios' technical dimensions to broader socio-ethical considerations.

Analysis of scenario effectiveness across specific learning objectives revealed consistently strong outcomes in ethics, policy, and legal domains (see Table 2). The qualitative data suggested that the scenarios' ability to capture student interest (M = 4.65, SD = 0.49) translated directly into improved perceived understanding, with students frequently citing the realistic nature of the scenarios and their relevance to contemporary issues as key factors in their engagement.

Table 2: Percentage of students who rated the case studies as 'Extremely effective,' 'Very effective,' or 'Moderately effective' in addressing each topic.

Topic	% Effective	*n*
Ethics	95.7	23
Policy	91.3	23
Law	91.3	23

Note. Effectiveness ratings reflect the percentage of students who selected "Extremely effective," "Very effective," or "Moderately effective" on a 5-point Likert scale.

Student feedback on the posthuman aspects of the scenarios emerged as a prominent theme in the qualitative analysis. Many students independently commented on the novel dynamics of learning through AI-generated materials, with a significant portion specifically noting how this approach challenged their preconceptions about human-AI interaction in educational contexts.

9. CONCLUSION AND FUTURE STUDY

The AI-assisted scenario development process and subsequent pilot implementation reveal more than merely the effectiveness of a novel pedagogical tool, demonstrating the emergence of cognitive assemblages between human and artificial intelligence in educational content creation and entanglement. Our findings suggest that this collaborative relationship transcends traditional notions of AI as a mere instrument, instead pointing toward transversal connections (Ferrando & Braidotti, 2019) across human and technological domains in the co-creation of knowledge. For instance, the observed high levels of participant engagement (see Table 1) lend empirical support to the concept of intra-action, wherein participants and the AI-generated content actively shape the resultant learning experience. Similarly, the enhanced comprehension of complex ethical concepts (M = 4.26, SD = 0.81) suggests the emergence of posthuman ethical assemblages, where ethical knowledge is collaboratively constructed through the interplay of human learners and AI.

The empirical evidence from our pilot implementation corroborates this theoretical framework. Students' consistently positive engagement with AI-generated scenarios (Table 1) demonstrates not just pedagogical effectiveness, but an intuitive grasp of intra-action: the mutual constitution of entities through their relationship rather than their pre-existence as separate elements. This was particularly evident in student responses that highlighted how the integration of AI-generated perspectives enhanced their understanding of complex cybersecurity situations, suggesting an emergent form of distributed cognition between human learners and technologically-mediated scenarios.

The scenarios' particular effectiveness in conveying complex ethical concepts merits special attention from a posthuman perspective. Rather than treating AI as a neutral tool for delivering pre-existing ethics education content, our findings suggest that the human-AI collaborative approach created what we might call posthuman ethical assemblages: learning environments where ethical understanding emerges through the dynamic interaction between human learners, AI-generated content, and the technological infrastructure that enables their interaction. The strong student engagement with these ethical scenarios (95.7% agreement, see Table 2) suggests that posthuman pedagogical approaches may be particularly well-suited for exploring the ethical dimensions of contemporary socio-technical systems.

Beyond traditional measures of effectiveness, our pilot implementation revealed how AI-generated scenarios challenge conventional boundaries between human and machine agency in educational contexts. Students' sophisticated engagement with the posthuman aspects of the scenarios—often unprompted—suggests an emerging awareness of how human cognition co-evolves with technological development (Adams & Thompson, 2016). This co-evolution was evident in how students navigated between human and AI-generated perspectives, developing posthuman literacy in their ability to critically engage with both human and machine-generated content.

However, the challenges uncovered during the implementation phase–specifically, instances of AI "hallucinations" and the injection of advanced

terminology outside the scope of the assignment–underscore key considerations regarding the inherent negotiations between human and non-human agency within a posthumanist pedagogy. These issues are not merely technical obstacles but rather manifestations of this ongoing negotiation between human and non-human agencies in educational contexts (Snaza et al., 2014). Addressing these challenges requires not just practical solutions but a theoretical framework that acknowledges the complex interplay between human cognition, artificial intelligence, and pedagogical practice.

Based on our findings, future research has opportunities across critical areas through a posthuman lens. For example, comparative analyses of learning outcomes derived from AI-generated versus traditional case studies should be prioritized, with a specific focus on the qualitative distinctions in participant engagement with human and AI-generated content. This should be done through a posthumanist analytical framework, emphasizing concepts of agency and distributed cognition. Second, longitudinal studies tracking student engagement and comprehension should investigate how prolonged exposure to posthuman pedagogical environments affects learning processes and outcomes. Finally, further inquiry into the discernible differences between authentic and fabricated scenarios is warranted to understand how the constructs of authenticity and simulation mediate participant learning and knowledge construction within posthuman learning environments. A postphenoemnological approach is especially well suited to this.

Though this study is small in scale and relies on self-reported data, it offers significant implications for cybersecurity education and the broader field. It points to the effectiveness of human/AI entanglement directed toward developing and teaching complex ethical concepts, suggesting a transformative approach to curricular development in cyber ethics in particular. Rather than treating AI as simply a tool to be studied, this approach positions it as an active participant with which one negotiates, supporting challenges to traditional notions of agency and expertise in cyber education context. This explicitly aligns with the evolving landscape of cybersecurity practice, wherein human/AI collaboration is increasingly present and characterizing of professional environments.

This posthuman approach to ethics education in cybersecurity also has a range of potential applications beyond academic settings. In industry training and professional development context, for example, human/AI generated content like this could provide timely, relevant learning opportunities that mirror the rapid pace of change in the domain, where practitioners must turn on a dime to deal with emerging ethical challenges. As such, these findings contribute to addressing the workforce development needs identified above. By enhancing student engagement and perceived learning outcomes, these case studies offer a promising approach to attracting and preparing the next generation of cyber professionals, especially in an incredibly complex atmosphere where technical expertise alone is increasingly insufficient.

These findings suggest the potential for fundamentally reconceptualizing how ethical reasoning is taught in technical fields. These case studies, the product of human and AI co-development, represent more than a novel teaching tool. In fact, they serve to exemplify a shift toward posthuman education in the cybersecurity realm, where the boundaries between human and machine, subject and object, become so fluid and negotiable to be almost negligible. This framework acknowledges this distributed and relational nature of ethical decision-making, rather than positioning it as an external constraint on technical practice. The evolution of cybersecurity as a domain stands to position this posthumanist approach in an increasingly vital and valuable role.

10. REFERENCES

Adams, C., & Thompson, T. L. (2016). *Researching a Posthuman World*. Palgrave Macmillan UK. https://doi.org/10.1057/978-1-137-57162-5

Adaryukova, L., Bychkov, O., & Skyrda, A. (2020). The Introduction of Ethics into Cybersecurity Curricula. *CEUR Workshop Proceedings*. https://ceur-ws.org/Vol-2740/20200013.pdf

Austin, G. (2020). Twelve dilemmas of reform in cyber security education. In *Cyber Security Education*. Routledge. https://doi.org/10.4324/9780367822576

Barad, K. (2007). *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*. Duke University Press. https://doi.org/10.2307/j.ctv12101zq

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2020). Holistic cyber education. In *Cyber Security Education*. Routledge. https://doi.org/10.4324/9780367822576

Blanken-Webb, J., Palmer, I., Burbules, N., Campbell, R., & Bashir, M. N. (2018). A Case Study-based Cybersecurity Ethics Curriculum. *ASE @ USENIX Security Symposium*. https://www.usenix.org/conference/ase18/presentation/blanken-webb

Cyber Innovation Center, & CYBER.ORG. (2021). *K-12 Cybersecurity Learning Standards*. https://cyber.org/standards

Dexter, S., Buchanan, E., Dins, K., Fleischmann, K. R., & Miller, K. (2013). Characterizing the need for graduate ethics education. *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, 153–158. https://doi.org/10.1145/2445196.2445245

Ferrando, F., & Braidotti, R. (2019). *Philosophical Posthumanism*. Bloomsbury Publishing Plc. https://www.bloomsbury.com/us/philosophical-posthumanism-9781350059481/

González, A. L., Moreno, M., Román, A. C. M., Fernández, Y. H., & Pérez, N. C. (2024). Ethics in Artificial Intelligence: An Approach to Cybersecurity. *Inteligencia Artificial*, *27*(73), 38–54. https://doi.org/10.4114/intartif.vol27iss73pp38-54

Hayles, N. K. (1999). *How we became posthuman: Virtual bodies in cybernetics, literature, and informatics*. The University of Chicago Press. https://hdl.handle.net/2027/heb05711.0001.001

Jackson, D., Matei, S. A., & Bertino, E. (2023). *Artificial Intelligence Ethics Education in Cybersecurity: Challenges and Opportunities: A focus group report* (arXiv:2311.00903). arXiv. https://doi.org/10.48550/arXiv.2311.00903

Kilhoffer, Z., Zhou, Z., Wang, F., Tamton, F., Huang, Y., Kim, P., Yeh, T., & Wang, Y. (2023). 'How technical do you get? I'm an english teacher': Teaching and learning cybersecurity and AI ethics in high school. *2023 IEEE Symposium on Security and Privacy (SP)*, 2032–2032. https://doi.org/10.1109/SP46215.2023.10179333

Kim, Y. (2016). The Role of Agent Age and Gender for Middle-Grade Girls. *Computers in the Schools*, *33*(2), 59–70. https://doi.org/10.1080/07380569.2016.1143753

Lake, S. (2022). The cybersecurity industry is short 3.4 million workers—that's good news for cyber wages. In *Fortune*. https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

Lin, H. (2022). Influences of Artificial Intelligence in Education on Teaching Effectiveness: The Mediating Effect of Teachers' Perceptions of Educational Technology. *International Journal of Emerging Technologies in Learning (iJET)*, *17*(24), 144–156. https://doi.org/10.3991/ijet.v17i24.36037

Matei, S. A., & Bertino, E. (2023). *Educating for AI Cybersecurity Work and Research: Ethics, Systems Thinking, and Communication Requirements* (arXiv:2311.04326). arXiv. https://doi.org/10.48550/arXiv.2311.04326

National Initiative for Cybersecurity Education (NICE). (2021). *National K12 Cybersecurity Education ROADMAP*. https://www.nist.gov/itl/applied-cybersecurity/nice

Navdeep, A. G. (2022). The Role of Ethics in Developing Secure Cyber-Security Policies. *Tuijin Jishu/Journal of Propulsion Technology*, *43*(4), 250–254. https://doi.org/10.52783/tjjpt.v43.i4.2346

O'Halloran, K. (2020). A posthumanist pedagogy using digital text analysis to enhance critical thinking in higher education. *Digital Scholarship in the Humanities*, *35*(4), 845–880. https://doi.org/10.1093/llc/fqz060

Orchard, R. K. (2019). Using Homemade, Short, Fictional Cases for Teaching the Theory of Constraints. *INFORMS Transactions on Education*, *19*(2), 81–88. https://doi.org/10.1287/ited.2017.0190

Osborne, T., & Rose, N. (2024). Against Posthumanism: Notes towards an Ethopolitics of Personhood. *Theory, Culture & Society*, *41*(1), 3–21. https://doi.org/10.1177/02632764231178472

Pinchot, J., Cellante, D., Mishra, S., & Paullet, K. (2020). Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap. *Information Systems Education Journal (ISEDJ)*, *18*(3), 44–53. https://files.eric.ed.gov/fulltext/EJ1258205.pdf

Rowland, P., Podhradsky, A., & Plucker, S. (2018). CybHER: A Method for Empowering,

Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 3727–3735. http://hdl.handle.net/10125/50358

Snaza, N., Appelbaum, P., Bayne, S., Carlson, D., Morris, M., Rotas, N., Sandlin, J., Wallin, J., & Weaver, J. A. (2014). Toward a Posthuman Education. *Journal of Curriculum Theorizing*, *30*(2), 39–55. https://journal.jctonline.org/index.php/jct/article/view/501

Triplett, W. J. (2023). Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability*, *3*(1), 47–67. https://doi.org/10.53889/ijses.v3i1.132

Veletsianos, G., Houlden, S., & Johnson, N. (2024). Is Artificial Intelligence in Education an Object or a Subject? Evidence from a Story Completion Exercise on Learner-AI Interactions. *TechTrends*. https://doi.org/10.1007/s11528-024-00942-5

Wallin, J. J. (2017). Pedagogy at the brink of the post-anthropocene. *Educational Philosophy and Theory*, *49*(11), 1099–1111. https://doi.org/10.1080/00131857.2016.1163246

Wang, P. (2022). Cybersecurity Ethics Education: A Curriculum Proposal. In S. Latifi (Ed.), *ITNG 2022 19th International Conference on Information Technology-New Generations* (pp. 155–159). Springer International Publishing. https://doi.org/10.1007/978-3-030-97652-1_19

Wang, X., & Bai, Y. (2022). Introducing Penetration Test with Case Study and Course Project in Cybersecurity Education. *Journal of The Colloquium for Information Systems Security Education*, *9*(1), 6–6. https://doi.org/10.53735/cisse.v9i1.148

Woodward, A. (2023). Postinformational Education. *International Journal of Philosophical Studies*, *31*(4), 501–521. https://doi.org/10.1080/09672559.2023.2290548

A Pivotal Progression of SEC's Cybersecurity Disclosure Requirements

Yining Chen
yining.chen@wku.edu

Divine Lokuku
lokukud@gmail.com

Tong Wu
tong.wu@wku.edu

Western Kentucky University
Bowling Green, KY 42101

Abstract

The U.S. Securities and Exchange Commission (SEC) introduced rigorous cybersecurity disclosure regulation mandating public companies to make prompt disclosure of material cybersecurity incidents and annual disclosure for cybersecurity risk management, strategy, and governance. The SEC's important progression of cybersecurity disclosure requirements signifies forward movement on ensuring transparency and maintaining investor confidence and market integrity. This study reviews the provisions of the new SEC cybersecurity disclosure rules and their implications for corporate governance, investor confidence, and the broader financial ecosystem. The information we present provides educators with pedagogical resources and teaching aids. To assist SEC registrants in adopting and complying with the new rules, we discuss implementation challenges and offer normative suggestions.

Keywords: cybersecurity disclosure, SEC rules, information asymmetry, materiality, transparency

Recommended Citation: Chen, Y., Lokuku, D., Wu, T., (2024). A Pivotal Progression of SEC's Cybersecurity Disclosure Requirements. *Cybersecurity Pedagogy and Practice Journal.* v4, n1, pp 35-44. DOI# https://doi.org/10.62273/MMYQ9950

A Pivotal Progression of SEC's Cybersecurity Disclosure Requirements

Yining Chen, Divine Lokuku and Tong Wu

1. INTRODUCTION

The digital age has ushered in unprecedented business opportunities, but it has also uncovered a new domain of challenges in the form of cyberattacks (Burt, 2023). The escalating frequency and severity of cyberattacks have necessitated a reevaluation of regulatory policies related to cybersecurity. The SEC's historical guidance on cybersecurity disclosures has been broad, affording companies significant discretion. However, the evolving threat landscape has prompted the SEC to adopt a more proactive stance, necessitating a reexamination and reinforcement of cybersecurity disclosure requirements (Vander & Rotman, 2024).

To address the evolving threat landscape posed by cyberattacks, the SEC implemented final rules, effective December 18, 2023, requiring public companies to disclose material cybersecurity incidents in their quarterly report on Form 8-K within four business days of the incident being determined material. Additionally, detailed information about cybersecurity risk management, strategy, and governance must be disclosed annually on Form 10-K.

In its press release, the SEC highlighted pivotal information regarding the recently adopted cybersecurity disclosure requirements. According to the press release, registrants are "to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance" (Securities and Exchange Commission, 2023a, para. 1). Notably, the new disclosure rules are applicable to not just malicious cyberattacks. Accidental occurrences not caused by a malicious attack, e.g., material internal systems failure, are also in the domain of the new rules. Besides, Form 8-K disclosure requirements are applicable when a company is materially affected by a series of related incidents, even if each individual incident is immaterial. What is more, the Commission has adopted rules requiring foreign private issuers to make comparable disclosures (Securities and Exchange Commission, 2023a).

Form 8-K Item 1.05 – Incident Disclosure

The new Item 1.05 of Form 8-K requires registrants to make timely disclosures of material cybersecurity incidents. Information disclosed, as illustrated in Figure 1, includes:

- Description — nature (e.g., unauthorized access, data breach, or system compromise), timing, and scope of the incident and its financial, operational, and reputational impact.
- Impact — material impact, reasonably likely material impact, and unknown but likely material impact of the incident on the registrant.
- Response — actions taken or undergoing to remediate the incident such as stringency containment measures or changes to policies and procedures.

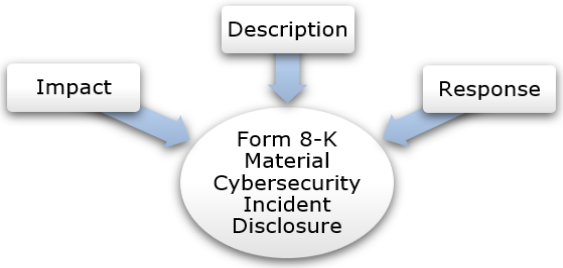


Figure 1: Form 8-K Incident Disclosure

Note: This figure shows the required Form 8-K disclosure for material cybersecurity incidents. The source of information for this figure is the Securities and Exchange Commission (2023a), SEC Press Release, 2023-139.

Form 10-K – Annual Disclosure

Form 10-K Item 106(b) requires registrants to make annual disclosures related to cybersecurity risk management, strategy, and governance. The annual cybersecurity disclosure must be included in the registrant's annual reports for fiscal years ending on or after December 15, 2023. Information disclosed, as illustrated in Figure 2, includes:

- Cybersecurity landscape, investments, and enhancement programs,

- Cybersecurity threats and previous incidents that have materially affected or are reasonably likely to materially affect the registrant, including their likelihood, severity, and impacts on business strategy, operations, or financial condition,
- Cybersecurity risk strategies and management, integrated into the registrant's risk management system or performed by third-party service providers, to identify, assess, and manage material cybersecurity threats, and
  Cybersecurity governance and oversight by board, management, and executives.

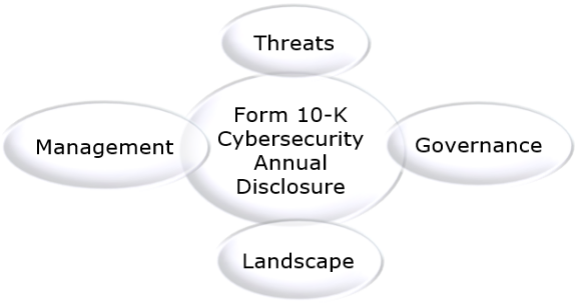


Figure 2: Form 10-K Annual Disclosure

Note: This figure shows the required information for the Form 10-K annual cybersecurity disclosures. The source of information for this figure is the Securities and Exchange Commission (2023a), SEC Press Release, 2023-139.

On Form 10-K Item 106(c)(2), registrant discloses how management assesses and responds to material cybersecurity threats, including, but not limited to (1) which management positions or committees are responsible for assessing and managing cybersecurity risks, and their relevant expertise (2) the processes by which such persons or committees monitor cybersecurity incidents, and (3) how management reports cybersecurity information to the board of directors and its cybersecurity committee. On Form 10-K Item 106(c)(1), registrant provides details for the governance and oversight of cybersecurity risk, including (1) the board's oversight of cyber risks and threats, (2) the board committee or subcommittee responsible for oversight, and (3) the processes by which the board or its committee is informed of cyber risks and attacks (Mazor et al., 2023).

2. KEY PROVISIONS

The new SEC cybersecurity disclosure requirements mark a notable departure from the previous laissez-faire approach, ushering in a more stringent and targeted set of guidelines for companies to adhere to. The provisions of these new requirements include the following.

Timely Disclosure
The SEC mandates companies to promptly disclose cybersecurity incidents, ensuring that investors receive timely and accurate information about potential risks. However, challenges arise from the stringency of the deadlines imposed and more so for specific industries and business styles. The new SEC regulations primarily require companies to disclose material cyberattacks within four days of becoming aware of the issue (Black et al., 2023). Notably, this four-day deadline is, as a rule, applicable across all businesses, though distinct and more stringent deadlines exist for specific industries. For instance, Critical Infrastructure Operators are obligated to report attacks within a tighter timeframe of 72 hours. Investment funds and advisors face an even more accelerated reporting requirement, needing to report incidents within 48 hours (Ciampa, 2023).

Materiality Assessment
The new cybersecurity disclosure requirements place significant emphasis on conducting a comprehensive materiality assessment to determine the significance of a cybersecurity incident. This assessment extends to evaluating the potential impact on the company's operations, financial condition, and reputation. However, it is crucial to note an exception to this rule: companies are not compelled to disclose "specific or technical information about their planned responses to the incident" (Black et al., 2023, para. 9).

Risk Factors
Companies are now obligated to furnish detailed information regarding the specific risks they encounter due to cybersecurity threats. This encompasses disclosing potential vulnerabilities, the likelihood of a cybersecurity incident occurring, and the potential magnitude of its impact. Importantly, this information is required to be reported annually on Form 10-K, as stipulated by the U.S. Securities and Exchange Commission.

Incident Response and Mitigation
The new cybersecurity disclosure requirements mandate companies to disclose their incident response and mitigation strategies comprehensively. This encompasses detailing the specific measures taken to address the incident, prevent future occurrences, and the potential costs associated with remediation efforts.

3. BACKGROUND AND LITERATURE

Cybersecurity Threats

A cyberattack is an intentional and malicious effort to breach the systems of another organization or individual (IBM, 2024). The attacker's motives may be information theft, financial gain, espionage, or sabotage. The SEC defines a cybersecurity incident as "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of the company's information systems or any information residing therein" (Black et al., 2023, para.6).

The increase in cyberattacks and cybersecurity risks is an undesirable outcome of modern business models and tech platforms such as e-commerce, remote work, digital payments, crypto assets, AI, and cloud computing, among others. While advanced technologies make business opportunities possible as never before, the unforeseen effects coming along are unprecedented cybersecurity threats and crises as well as skyrocketing cybercrime costs to companies and investors. Common cyber threats include ransomware, data breaches, stealth malware, underground trends, and AI fraud, while common attacking avenues include business email compromises, targeted cloud services, zero-day exploits, and link library abuse (Lavorgna, 2020).

Rising with the complexity and frequency of cyber threats is the ramping up of regulatory efforts. The SEC has undertaken several initiatives to issue guidance on cybersecurity risk and incident disclosures. Specifically, in 2011, the SEC staff issued guidance, and later in 2018, issued Commission Statement and Guidance on Public Company Cybersecurity Disclosures to help registrants prepare cybersecurity risk and incident disclosures (Gerding, 2023) and to promote clear and vigorous disclosures about cybersecurity, the risk factors, and incidents (Peng & Krivacek, 2020). Even with considerable effort, the Commission admitted that disclosure practices remain inconsistent.

Cereola & Dynowska (2019, "Abstract" section) denote that "although the SEC staff guidance warns public companies to make timely disclosure, recognizing the threat that cybercrime poses to investors in the public markets, it does not go far enough to institute direct measures that would compel companies to reveal the nature and scope of a cybersecurity breach." Their empirical findings indicate a sizable increase "in the number of firms referencing cybersecurity in the Risk Factor section of the 10-K." However, "there is a tendency not to disclose reported breaches in the narrative of the 10-K and that the cybersecurity risk factor disclosures do not include details on actual breaches."

The Commission's recent ruling represents its efforts "to provide investors with the more timely, consistent, comparable, and decision-useful information they need to make informed investment and voting decisions" (Gerding, 2023, para. 2).

Disclosure and Transparency

While disclosure regulations, in general, are expected to improve the quality of reporting and disclosure, the chief benefit reached is the mitigation of information asymmetry and the enhancement of corporate transparency (Bhattacharya et al., 2013). Brown & Martinsson (2018) find that the securities market disclosure reforms foster rich and transparent information environments.

From the existing literature, several empirical studies examine the market impact of mandatory disclosures. For instance, Wang & Fan (2014) explore the impact of R&D disclosure choices (capitalization and expensing) on firm value. Tang et al. (2013) study the capital market reaction to the mandatory disclosure of directors' opinions. Chen et al. (2018) investigate the effect of mandatory CSR disclosure on firm profitability. Xu et al. (2020) examine the effect of CSR disclosure on firm value.

Although high-quality disclosure is proven effective in reducing the information asymmetry between investors and management concerning company performance (Clinch et al., 2012), investors and other financial statement users are usually unable to discern its quality. Edwige & Levine (2020) model an information mosaic theory suggesting that voluntary public disclosures lead to higher *ex ante* information asymmetry by allowing the informed trader to refine his or her trading strategy and complete the information mosaic. Proponents of mandatory disclosure and policymakers argue from a social psychology perspective that disclosing value-relevant information makes firms' accountability more salient, thereby reducing agency costs. With the reduced information asymmetry and agency conflicts, users of financial information can make more informed decisions.

Healy & Palepu (2001, p. 406) argue that the "demand for financial reporting and disclosure arises from information asymmetry and agency conflicts between management and outside investors. The credibility of management disclosures is enhanced by regulators, standard setters, auditors, and other capital market intermediaries." While research finds broad support that disclosure regulation brings about new and relevant information to investors (Kothari, 2001), whether a particular disclosure regulation is effective in alleviating information asymmetry and agency problems remains a research question, especially when new disclosure regulations are enacted. Whether a particular disclosure regulation, such as a mandatory cybersecurity disclosure regulation, is effective in producing positive economic consequences is of greater interest to regulators, standard-setters, firms, and investors.

4. IMPLICATIONS OF THE SEC RULING

Although this study does not provide empirical evidence on the effectiveness of the new SEC cybersecurity disclosure rules, we deliberate on the provisions of the new rules and their implications for corporate governance, investor confidence, and the broader financial ecosystem.

Corporate Governance
The enhanced SEC cybersecurity disclosure requirements have profound implications for corporate governance. Companies are now compelled to elevate cybersecurity risk management to a strategic consideration for boards and executives, reflecting the interconnectedness between cybersecurity and overall corporate performance.

- Board Oversight: The growing recognition of the board's responsibility in ensuring the company's resilience against cyber threats. The board must exercise its oversight function by overseeing the management team's effort in managing cyber risks and responding to material incidents.
- Integration with Enterprise Risk Management: Companies are encouraged to integrate cybersecurity risk into their broader enterprise risk management framework, fostering a holistic approach to risk assessment and mitigation.
- Accountability and Transparency: Increased transparency promotes accountability among corporate leaders, holding executives responsible for ensuring effective cybersecurity measures are in place and transparently communicating the impacts of incidents.
- Evaluation and Control: Clearly defined reporting chain and materiality evaluation mechanism to ensure that cybersecurity risk evaluations and incidents are reported timely (Peng & Krivacek, 2020).

Investor Confidence and Market Integrity
Investor confidence is paramount to the functioning of capital markets. The new cybersecurity disclosure requirements aim to bolster investor confidence by providing more comprehensive and timely information about the risks companies face in the digital era.

- Informed Decision-Making: Investors armed with more detailed and timely information can make informed decisions, aligning with the SEC's mission of protecting investors and maintaining fair and efficient markets.
- Market Integrity: Reduced information asymmetry contributes to market integrity, allowing investors to more accurately assess the true value and risk associated with their investments, thereby enhancing market stability.
- Sector-Wide Impact: The SEC's cybersecurity disclosure requirements catalyze a collective improvement in cybersecurity resilience across industries, benefiting the entire financial ecosystem.

5. CHALLENGES AND CRITICISMS

The SEC's new cybersecurity disclosure requirements signify a positive stride toward ensuring reporting transparency and informed decision-making for both investors and companies. While these disclosure regulations are a commendable initiative, certain limitations, criticisms, and challenges merit consideration.

First, to comply with the new disclosure requirements, companies need to grapple with balancing the need for transparency and the protection of sensitive information. Also, critics argue that smaller companies with limited resources may bear an undue burden because of the cost of dealing with a potentially massive incident relative to company size (Securities and Exchange Commission, 2023b). Another notable concern is the existence of varied reporting deadlines. Last and foremost, the principal deadline, four business days from the date on which the incident is determined material, presents a substantial challenge.

An illustrative example is the cyberattack experienced by Clorox recently. The incident occurred after the implementation of the disclosure requirements, compelling the company to fully disclose the situation promptly. However, due to the pressing four-day reporting deadline, Clorox's initial 8-K report lacked substantial information as the company was still assessing the material impact of the attack. Clorox later filed multiple 8-K forms to update investors on the incident. This situation aligns with the sentiment expressed by an executive of Clorox, stating that "the fog of these incidents will make it hard to provide reliable information at the start" (Nash, 2023, para. 3). As exemplified, the new cybersecurity disclosure requirements are novel for companies, leading many to file Form 8-K without a thorough investigation into the incident's implications for their operations. This dilemma risks information overload and can adversely affect a company's stock value, as displayed in the case of Clorox.

Zukis (2024) examines cybersecurity disclosures that have been filed since the enactment of the SEC cybersecurity disclosure ruling and finds deficiency and noncompliance. Specifically, none of the first filers include quantitative disclosures of the material impacts or reasonably likely material impacts of the incident. The materiality disclosures are all based exclusively on the qualitative impacts of the incident, and none reference quantitative financial impacts due to the common reporting difficulty that "incident costs and financial implications typically lag as the incident plays out" (Zukis, 2024, para. 19).

Another noteworthy concern of implementation is the absence of specificity in determining materiality. The new SEC rules do not explicitly state who should decide materiality. Neither do they provide guidelines on evaluating if an incident should be deemed material. In fact, registrants may not be able to determine the materiality of an incident immediately after its discovery. While the SEC sets a stringent deadline (i.e., four days) to disclose an incident on Form 8-K from the date on which the incident is considered material, it does not set a specific deadline by which a registrant must determine whether an incident is material after its discovery. The only general rule is to make materiality determinations without unreasonable delay (Mazor et al., 2023).

6. MATERIALITY

The SEC defines a material incident as one that a reasonable shareholder would consider important in making an investment decision (Securities and Exchange Commission, 2023a). Specifically, an incident is considered material "if it significantly affects a company's operations, financial positions, reputation, or legal obligations" (Vander & Rotman, 2024, para. 2). This definition of materiality, however, lacks a clear objective threshold and therefore presents challenges for companies to assess cybersecurity incidents or to justify their disclosure decisions to regulatory authorities and interested parties.

The SEC cybersecurity disclosure rules are expected to be updated as more insights emerge. Also, better methodologies will be developed to guide companies in navigating this evolving landscape. But before any additional guidelines become available, it is important for companies to strive for best practices. With precise and timely disclosure of material incidents, companies can preserve trust from interested parties amidst cyber crises and attacks. To do so, companies should develop a clear process with proper mechanisms to determine materiality for cybersecurity incidents. The process should (1) require the IT function to play an integral role, (2) solicit support from legal counsels and financial advisors, (3) account for actual and expected impacts, and (4) consider both qualitative and quantitative factors (Vander & Rotman, 2024).

Quantitative factors that make an actual impact on the assessment of materiality include ransom payments, restoration costs, operational disruptions, earnings and stock price losses, and legal and litigation fees. Other quantitative factors with expected impacts may be costs to repair and strengthen system security and environment and future insurance and protection costs. Besides these actual and expected quantitative factors, qualitative factors to consider include reputation damage, goodwill impairment, supply chain and customer relationship destruction, motivation of malicious invader, and legal disputes and liabilities.

Vander & Rotman (2024) suggest that companies design or adopt a framework for their materiality assessment. The framework should suit the company's functions, leverage a combination of quantitative and qualitative factors, allow individual considerations for different incidents, offer a taxonomy of loss categories, and document the materiality assessment processes and decision points. The framework, like other frameworks used for business continuity and disaster recovery plans, data privacy and security policies, and enterprise risk management

programs, should be subject to continuous evaluation and improvement.

As a final point, when encountering cybersecurity incidents, companies need to assess whether the incident is material from the perspective of stakeholders rather than their own. They need to objectively evaluate whether investors and stakeholders would consider the incident material in making their investment decisions. To ensure the objective assessment of materiality, timely response and reporting of cybersecurity incidents, and proper adherence to the SEC disclosure requirements, companies can form a cross-functional disclosure team consisting of information security officers, risk management personnel, legal counsels, financial advisors, and board representatives (Vander & Rotman, 2024; Johnson, 2024).

7. COMPLIANCE PREPARATION

To implement the SEC cybersecurity disclosure requirements to achieve successful compliance, registrants should take preparation actions. They can build upon the lessons learned from prior compliance initiatives with the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the PCI security standards. Many of these regulations and standards have stricter requirements and their compliance solutions may have a synergistic effect in solving cybersecurity challenges. As cybersecurity challenges escalate and regulations multiply, it is increasingly important that companies develop not only sustainable programs to manage cybersecurity risks but also sensible strategies to comply with regulations and disclosure requirements. We show viable preparation actions in Figure 3, then explain them in the following sections.

Figure 3: Preparation Actions

Note: This figure suggests actions that SEC registrants can take to prepare for the new cybersecurity disclosure requirements. The source of information for this figure includes Mossburg et al. (2023) and Ehret (2023).

Conduct Readiness Assessment

First, registrants should assess their mindset acknowledging that cybersecurity is no longer bolt-on after cyberattacks, but rather baked-in as a core element of organizational culture (Rosone & Kleemann, 2023). Second, registrants should institute a foundation cultivating evolving capabilities in response to evolving threats. They should form a cybersecurity response and reporting team and ensure their mature understanding of the incident response and reporting processes. Third, registrants should prepare for the SEC's effect on the labor market, expecting a shortage of executives with cybersecurity experience and capabilities. They will need to reserve proper executives with talent aligning with the SEC requirements. Fourth, registrants need to assess their reliance on third-party service providers, and whether they have processes to oversee and identify cybersecurity threats associated with their use of third-party services.

Revise Incident Response Policies and Procedures

It's important that registrants revisit cybersecurity policies to ensure that they provide effective disclosure controls and procedures, including communication channels between the cybersecurity team, the investor relations advisor, and the legal counsel. These policies and channels of communication will be the core to the prompt assessment and response to detected cybersecurity incidents as well as the precise and timely compliance with the new disclosure requirements.

Cyber strategies, policies, and procedures must include response and recovery plans and periodic risk assessments. Registrants should test their adequacy and effectiveness and update them on a continuous basis to ensure compliance with applicable regulations and laws. In addition, cyber policies, procedures, and practices should be extended to third-party service providers.

Reinforce Governance and Oversight Structures

To prepare for compliance, registrants should adopt the mindset to provide shareholders and the public with confidence that cybersecurity is a top organizational priority. Their organizational security governance (OSG) practices should allow quick and reliable decision-making and adapt to the changing landscape of security management (Slonka et al., 2023). With the aim of doing this,

registrants should strengthen the cybersecurity governance structure by (1) educating the board and executives, (2) fostering a culture of responsibility and accountability, (3) delegating a specific board committee responsible for supervision, and (4) plotting operating models for cyber risk management and disclosure.

Expand Incident Response and Reporting Capabilities

It is essential that registrants invest in cyber-resilience and expand incident response capabilities. The incident response and reporting system should adopt a materiality framework, define materiality criteria, and form incident assessment processes. The materiality, e.g., complexity and severity, of the cybersecurity risk must be considered from each registrant's business risk, technology, reputation, and regulatory compliance perspective. There is no one-size-fits-all approach (Ehret, 2023). Besides, the system should have the capacity to meet disclosure obligations as incidents evolve and to learn from past incidents to improve resilience. Altogether, the cyber risk response system should promptly identify and address incidents in order to protect the organization against cyber risks and safeguard its reputation. It should facilitate timely and informative incident disclosures as well as consistent and transparent periodic disclosures.

Minimize Cyber Attack Risk and Threats

The best way to prepare for the stricter SEC disclosure rules is to minimize the possibility of data breach and system compromise. For registrants to boost up cyber risk defense, we make a few suggestions. First, invest in in-house or third-party security technologies, such as multi-layer and multi-factor access authentication, to strengthen identity and access controls. Second, secure cloud connection and remote access via enhanced network protection and intrusion detection systems. Third, perform penetration testing to identify weak spots in a system's defenses. Fourth, investigate emerging threat actors and their best defense. Fifth, train legal, infosec, and operational teams for breach prevention, response, mitigation, and reporting.

8. CONCLUSION

The SEC's enhanced cybersecurity disclosure requirements mark a pivotal progression in regulatory history, acknowledging cybersecurity as integral in maintaining investor confidence and market integrity. By mandating detailed and timely disclosures, the SEC aims to empower investors' decision-making and incentivize companies to prioritize cybersecurity within their corporate governance frameworks. As businesses navigate the complexities of the digital age, the new regulations offer a roadmap for building resilience and stability of corporate governance and ensuring the long-term sustainability of the financial ecosystem.

As the cybersecurity landscape continues to evolve, the SEC is likely to refine its disclosure requirements to address emerging challenges. Continued emphasis on transparency, accountability, and the integration of cybersecurity risk into corporate governance frameworks is anticipated. As companies move forward on the journey of compliance, disclosure examples will be set and penalties imposed, forcing all organizations into developing comprehensive materiality determination framework and structured reporting processes. (Zukis, 2024). At the other end, investors and stakeholders, with a regulatory baseline now in place, will persist in demanding more and better disclosures on material cybersecurity incidents and on how systems and data are secured, managed, and governed to support company values.

9. REFERENCES

Bhattacharya, N., Hemang, D., & Venkataraman, K. (2013). Does earnings quality affect information asymmetry? Evidence from trading costs, *Contemporary Accounting Research, 30*(2), 482-516. https://doi.org/10.1111/j.1911-3846.2012.01161.x

Black, E. W., Kent, E., & Halbhuber, H. (2023). New SEC cybersecurity disclosures. *The Harvard Law School Forum on Corporate Governance*, August 13. https://corpgov.law.harvard.edu/2023/08/13/new-sec-cybersecurity-disclosures/

Brown, J. R., & Martinsson, G. (2018). Does transparency stifle or facilitate innovation? *Management Science, 65*(4), 1600–1623. https://doi.org/10.1287/mnsc.2017.3002

Burt, A. (2023). The digital world is changing rapidly. Your cybersecurity needs to keep up. *Harvard Business Review*. Retrieved November 27, 2024 from https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up

Cereola, D. J., & Dynowska, J. (2019). Investigating the impact of publicly announced information security breaches on

corporate risk factor disclosure tendencies. *Journal of Cybersecurity Education*, *Research, and Practice, 2019*(2). https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss2/3/

Chen, Y. C., Hung, M., & Wang, Y. (2018). The effect of mandatory CSR disclosure on firm profitability and social externalities: Evidence from China. *Journal of Accounting and Economics, 65*(1), 169-190. https://doi.org/10.1016/j.jacceco.2017.11.009

Ciampa, M. (2023). Too much disclosure? Or not enough? Working Paper. Western Kentucky University.

Clinch, G., Stokes, D. J., & Zhu, T. (2012). Audit quality and information asymmetry between traders. *Accounting and Finance, 52*(3), 743-765. https://doi.org/10.1111/ j.1467-629X.2011.00411.xEdwige, C., & Levine, C. B. (2020). Public disclosures and information asymmetry: A theory of the mosaic. *The Accounting Review, 95*(1), 79–99. https://doi.org/ 10.2308/accr-52447

Ehret, T. (2023). Companies should prepare to comply with new SEC cybersecurity rules. Thomson Reuters. Retrieved November 28 from https://www. thomsonreuters.com/en-us/posts/ government/sec-cybersecurity-rules/

Gerding, E. (2023). Cybersecurity disclosure. SEC Statement, Dec. 14. https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics, 31*(1-3), 405-440. https://doi. org/10.1016/S0165-4101(01)00018-0

IBM (2024). What is a cyberattack? Retrieved November 20, 2024 from https://www.ibm.com/topics/cyber-attack#:~:text=A%20cyberattack%20is%20any%20intentional,theft%20to%20acts%20of%20war

Johnson, M. (2024). Why new SEC cybersecurity rules require an integrated approach, EY. https://www.ey.com/en_us/ cybersecurity/new-sec-cybersecurity-rules-require-integrated-approach

Kothari, S. P. (2001). Capital markets research in accounting. *Journal of Accounting and Economics 31*, 105-231. https://doi.org/10.1016/S0165-4101(01)00030-1

Lavorgna, A. (2020). *Cybercrimes: Critical issues in a global context*. Bloomsbury Publishing.

Mazor, C., Herrygers, S., & Danola, C. (2023). SEC issues new requirements for cybersecurity disclosures, *Deloitte Heads Up, 30*(13), July 30 (Updated Dec. 19). https://dart.deloitte.com/USDART/home/publications/deloitte/heads-up/2023/sec-rule-cyber-disclosures

Mossburg, E., Amjad, A., Kumar, G., Adib, N., Herrygers, S. & Mazor, C. (2023). Navigating the new SEC cybersecurity disclosure requirements, Deloitte, Retrieved November 28, 2024 from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-navigating-the-new-sec-cybersecurity.pdf

Nash, K. S. (2023). Clorox cyberattack brings early test of new SEC Cyber Rules. *The Wall Street Journal*, September 20. https://www.wsj.com/articles/clorox-cyberattack-brings-early-test-of-new-sec-cyber-rules-b320475

Peng, J., & Krivacek, G. (2020). The Growing Role of Cybersecurity Disclosures. *ISACA Journal*, *1*, February 26, 2020. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/the-growing-role-of-cybersecurity-disclosures

Rosone, B., & Kleemann, T. (2023). What new SEC cyber ruling requirements could mean for private companies. Deloitte Debriefs, November 1. 2023. https://www2.deloitte.com/us/en/events/private-companies-dbriefs-webcasts/2023/new-sec-cyber-ruling-requirements.html

Slonka, K., Mishra, S., Draus, P., & Bromall, N. (2023). Measurement, reporting, and monitoring in organizational security governance from the security professional's perspective. *Cybersecurity Pedagogy and Practice Journal, 2*(1), 38-49. https://cppj.info/2023-2/n1/CPPJv2n1p38.html

Tang, X., Du, J., & Hou, Q. (2013). The effectiveness of the mandatory disclosure of independent directors' opinions: Empirical evidence from China, *Journal of Accounting and Public Policy, 32*(3), 89-125. https://doi.org/10.1002/smj.2421

Securities and Exchange Commission (2023a). SEC adopts rules on cybersecurity risk

management, strategy, governance, and incident disclosure by public companies, SEC Press Release, 2023-139. https://www.sec.gov/news/press-release/2023-139

Securities and Exchange Commission (2023b). Cybersecurity risk management, strategy, governance, and incident disclosure. *Federal Register, 88*(149), August 4, 2023. https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

Vander, M., & Rotman, D. (2024). SEC cybersecurity disclosure rules: Cracking the code on materiality and reporting, KPMG Media News. February 27, 2024. https://kpmg.com/us/en/media/news/sec-cybersecurity-disclosure-rules-2024.html

Wang, Y., & Fan, W. (2014). R&D reporting methods and firm value: Evidence from China. *Chinese Management Studies, 8*(3), 375-396. https://doi.org/10.1108/CMS-01-2013-0019

Xu, S., Chen, X., Li, A., & Xia, X. (2020). Disclosure for whom? Government involvement, CSR disclosure and firm value. *Emerging Markets Review, 44*. https://doi.org/10.1016/j.ememar.2020.100717

Zukis, B. (2024). Companies are already not complying with the new SEC cybersecurity incident disclosure rules. *Forbes Leadership Strategy*, March 4, 2024. https://www.forbes.com/sites/bobzukis/2024/03/04/companies-are-already-not-complying-with-the-new-sec-cybersecurity-incident-disclosure-rules/?sh=258c7d8b5273