MENTORING IS A NECESSARY PART OF RECRUITING AND RETENTION DIVERSIFIED STUDENTS IN STEM

PANEL

Karen Paullet, Robert Morris University, paullet@rmu.edu
Natalya Bromall, Robert Morris University, bromall@rmu.edu
Abdur Shahid, Robert Morris University, shahid@rmu.edu

SUMMARY

The Cybersecurity Workforce Study (2022) revealed that there is a 3.4 million worker global shortage in information security professionals. This shortage persists even though 464,000 positions were filled in 2022 alone (Lake, 2022).

Studies showing significant progress in students who recover from a grade decline show that personalized support and guidance can positively influence student retention. Transfer students from community colleges who enter four-year institutions encounter different barriers to persistence than traditional undergraduates. Creating accessible pathways for transfer students requires institutions to have clear transfer processes and effective articulation agreements in place (Handel & Williams, 2012).

BACKGROUND

Community colleges among other two-year colleges are playing a role in creating pathways for under-represented students to four-year institutions (Boswell, 2004; Cohen et al., 14; Wang et al, 2017). Students are presented with a realistic pathway through the provision of smaller class sizes, flexible admissions, and lower costs. These factors make it possible for more under-represented students especially low-income and first-generation college students to begin exploring a career in the STEM fields. Women, students from low-income backgrounds and minorities typically choose two-year colleges because they are more conducive to work-file balance.

Students from under-represented populations in STEM report an intent to transfer to STEM fields when there is a high level of field-oriented interaction (Wang, Chan, Soffa & Nachman, 2017), engagement in STEM field related activities during their educational career, interactive sessions about career options, and the availability of a mentor to guide and inform academic and post-graduation choices.

Students, especially from underrepresented populations, benefit from strong connections with a faculty member who can serve as an engaged role model (Cuseo, 2017). A study conducted by Glass (2013) shows that a lack of mentors is an important factor in few girls studying cybersecurity in middle school, high school and the collegiate level. If the mentor projected a stereotypical image of a “geek or nerd”, girls were less likely to believe in their success in the field. The success of role models for young women is needed to help girls succeed in cybersecurity.

LeClair, Shih, and Abraham (2014) indicate that while equal pay and advancement opportunities are important for the retention of women in cybersecurity, having mentors is more important. The mentor does not need to be female but needs to have interest in the mentee's success. The mentor does not need to be female but needs to have an interest in the mentee's success. Cheryan, et.al (2011) found there to be no difference between male and female recruiters in the STEM field but found that women mentors are more effective for keeping women in the field.

It is the panelist's belief that if students are matched to faculty mentors upon acceptance to the University, they will have a positive experience in their field of study. A dedicated student-faculty mentoring relationship allows the scholars to have personal, accessible support for matters directly related to the CIS field. At the beginning of each semester, the mentor coordinator will hold an orientation meeting for new scholars and mentors. A dedicated mentoring style has been shown to effectively support students' retention in STEM.

REFERENCES

Cheryan, S., Siy, J.O. Vichayapai, M., Drury, B.J, & Kim, S. (2011). Do female and male role models who embody STEM stereotypes hinder women's anticipated success in STEM? *Social and Psychological and Personality Science, 2(6),* 656-664. Retrieved from https://doi.org/10.1177/1948550611405218

Frost, J., & Sullivan, T. (2017). Global cybersecurity workforce shortage to reach 1.8 million as threats loom larger and stakes rise higher. Retrieved from h ttps://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage

Glass,J.L., Sassler, S., Levitte, Y., & Michelmore, K.M. (2013). What's so special about STEM? A comparison of women's retention in STEM and professional occupations? *Social Forces: A Scientific Medium of Social Study and Interpretation, 92(2),* 723-756. Retrieved from https://doi.org/10.1093.sf/sot092

Handle S., & Williams. R. (2012). The promise of the transfer pathway. College Board Advocacy and Policy Center. Retrieved from https://secure-media.collegeboard.org/digitalServices/pdf/professionals/handel-williams-promise-of-the-transfer-pathway-2012.pdf

Lae, Sydney, (2022). The cybersecurity industry is short 3.4 million workers – that is good news for cyber wages. *Fortune Education.* Retrieved from https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

CHATGPT HAS ENTERED THE CLASSROOM CHAT: IMPLICATIONS FOR CO-TEACHING WITH AI

PANEL

Dr. Katherine Carl, Governors State University, kcarl@govst.edu
Dr. Scott Spangler, Middle Georgia State University, scott.spangler@mga.edu
Dr. Shannon Beasley, Middle Georgia State University, shannon.beasley@mga.edu

ABSTRACT

Students have begun to use tools like ChatGPT to complete tasks required of them for assessment in the classroom. In this 90-minute panel, we review the state of artificial intelligence tools and how they are used in the classroom, discuss implications of the use of tools like ChatGPT by students, and engage panel participants in an interactive activity designed to help them create activities and assessments in the face of artificial intelligence use by students.

Keywords: artificial intelligence, teaching, educational design, academic integrity, plagiarism

AGENDA

OpenAI released the artificial intelligence application, ChatGPT, in November of 2022 and has impressed experts with its writing ability, proficiency at complex tasks, and ease of use (Lock, 2022). The tool has become popular with university students, who have expressed that the bot is "like a very friendly tutor that doesn't mind stupid questions" and can generate college essays that are "Solid A- work in 10 seconds" (Vincent, 2022).

The ability of the chatbot to produce informed writing based on text available to it has interesting implications for academic integrity in the classroom. Several questions related to education arise from its existence:

- What skills should students be able to perform unassisted by AI?
- What skills in the information systems and business analytics disciplines can be demonstrated by ChatGPT alone, and which cannot?
- Should students be confronted about the use of ChatGPT to complete assessments?
- If so, what are appropriate methods for confronting students when an instructor believes that they have submitted work generated by ChatGPT?
- Can assessments be designed so that they must be completed unassisted by AI? Should they be designed this way?

In this interactive workshop designed for instructors that teach online or in-person, participants will be introduced to ChatGPT and its capabilities, engage in a discussion about ChatGPT and AI in the classroom, and design an assessment that can be used in a course, given the implications of the chatbot.

REFERENCES

Lock, S. (2022, December 5). What is AI chatbot phenomenon ChatGPT and could it replace humans? *The Guardian*, https://www.theguardian.com/technology/2022/dec/05/what-is-ai-chatbot-phenomenon-chatgpt-and-could-it-replace-humans.

Vincent, J. (2022, December 1). OpenAI's new chatbot can explain code and write sitcom scripts but is still easily tricked. *The Verge*, https://www.theverge.com/23488017/openai-chatbot-chatgpt-ai-examples-web-demo.

PRIVACY AND THE INTENTION TO READ COMPUTER USAGE POLICIES

C. Bryan Foltz, University of Tennessee at Martin, cfoltz1@utm.edu
Laura Foltz, University of Tennessee at Martin, lfoltz@utm.edu

INTRODUCTION

Information systems security breaches continue to be a major issue globally. Such breaches can cause serious harm to organizations and individuals (Ou, et al, 2022). Many cybersecurity incidents are traced to careless errors or violations of computer usage policies (CUPs) (Ifinedo, 2012). Unfortunately, many individuals fail to read their organizational CUPs. This research seeks to further understand why individuals fail to read computer usage policies. This study examines privacy concerns and the employee intention to read CUPs to protect organizational data.

PROPOSED STUDY

This study uses surveys to collect information from individuals based on a privacy concern construct and the Theory of Planned Behavior (TPB). The information will be analyzed by using path analysis. The analysis is expected to show that TPB, in conjunction with the concept of privacy concern, are related to a person's intent to read a CUP.

CUPs are the cornerstone of computer security (Backhouse and Dhillion, 1995). These policies define who is allowed to use computer equipment and how that equipment may be used within an organization (Nolan, 2005; Scott and Voss, 1994). CUPs should deter misuse by explaining acceptable use and the consequences of unacceptable use. However, many users elect not to read such policies (Foltz, Cronan, and Jones, 2004; Harrington, 1996). Foltz, Schwager, and Anderson (2008) utilized the TPB to understand why some users do not read CUPs. The TPB suggests that individual behavior may be predicted by examining intention and an individual's belief about their ability to perform a behavior and that intentions are formed from Attitudes Toward the Behavior (Attitudes), Subjective Norms, and Perceived Behavioral Control (Ajzen, 1988, 1991). Attitudes captures individual feelings about performing the behavior, while Subjective Norms indicate how the individual thinks others feel about the behavior (Ajzen, 1991). Perceived Behavioral Control reflects individual evaluation regarding ability to perform the behavior (Ajzen, 1991). Customer data and Internet of Things, among other sources, have increased stored personal data (Chen, Wang, and Zhang, 2023; Miller and Tucker, 2009; Sfar et al, 2018; Zheng et al, 2018). The increased data collection leads to increased user awareness of privacy. Within the extant literature, privacy concern is often used as a proxy for the concept of privacy (Xu, Dinev, Smith, and Hart, 2008). Privacy concern may be defined as "one's concern about his or her personal data being used" (Chen, Wang, and Zhang, 2023). Chen, Wang, and Zhang (2023) utilized privacy concerns as an antecedent to Attitudes, Subjective Norms, and Perceived Behavioral Control within the TPB; however, their research focused upon individual performance of privacy-protection behaviors such as providing incomplete or untruthful information (Chen, Wang, and Zhang, 2023).

This research seeks to understand why individuals within an organization fail to read or comprehend organizational CUPs that provide information about the organization's privacy policies. This study will examine employee intention to read CUPs to protect organizational data.

IMPLICATIONS AND CONCLUSION

An enhanced understanding of the relationship between privacy concerns and intention to read CUPs will allow organizations to better understand and motivate users to read organizational Computer Usage Policies. Since CUPs act as the cornerstone of computer security (Backhouse and Dhillion, 1995), enhanced understanding of the CUPs should enhance overall security of the organization.

REFERENCES

Ajzen, I. (1988), Attitudes, Personality, and Behavior, The Dorsey Press, Chicago, IL.

Ajzen, I. (1991), “The theory of planned behavior”, Organizational Behavior and Human Decision Processes, Vol. 50 No. 2, pp. 179-211.

Backhouse, J. and Dhillon, G. (1995), “Managing computer crime: a research outlook”, Computers and Security, Vol. 14 No. 7, pp. 645-51.

Chen, M., Wang, H., & Zhang, R. (2023). Using the Extended Theory of Planned Behavior to Predict Privacy-Protection Behavioral Intentions in the Big Data Era: The Role of Privacy Concern. In SHS Web of Conferences (Vol. 155, p. 03011). EDP Sciences.

Foltz, C.B., Cronan, T.P. and Jones, T.W. (2004), “Student awareness of university computer usage policies: is a single exposure enough?”, Proceedings of the Southwest Decision Sciences Institute, Orlando, FL, pp. 293-9.

Foltz, C.B., Schwager, P. H., & Anderson, J. E. (2008). Why users (fail to) read computer usage policies. Industrial Management & Data Systems, 108(6), 701-712.

Harrington, Susan J. “The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions.” MIS Quarterly, Vol. 20, No. 3, 1996, pp. 257-278.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

Miller, A. R., & Tucker, C. (2009). Privacy protection and technology diffusion: The case of electronic medical records. Management science, 55(7), 1077-1093.

Nolan, (2005) “Best practices for establishing an effective workplace policy for acceptable computer usage”, Information Systems Control Journal, 6, 32-34.

Ou, C. X., Zhang, X., Angelopoulos, S., Davison, R. M., & Janse, N. (2022). Security breaches and organization response strategy: Exploring consumers’ threat and coping appraisals. International Journal of Information Management, 65, 102498.

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137.

Scott, T. and Voss, R. (1994), “Ethics and the 7 ‘P’s’ of computer use policies”, Proceedings of the Conference on Ethics in the Computer Age, Gatlinburg, TN, pp. 61-7.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. Proceedings of the International Conference on Information Systems.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on human-computer interaction, 2(CSCW), 1-20.

EXPLORING MBA STUDENTS' PERCEPTIONS OF ARTIFICIAL INTELLIGENCE USING TECHNOLOGY ACCEPTANCE MODEL

Sung J. Shim, Seton Hall University, sung.shim@shu.edu

ABSTRACT

PURPOSE OF THE STUDY

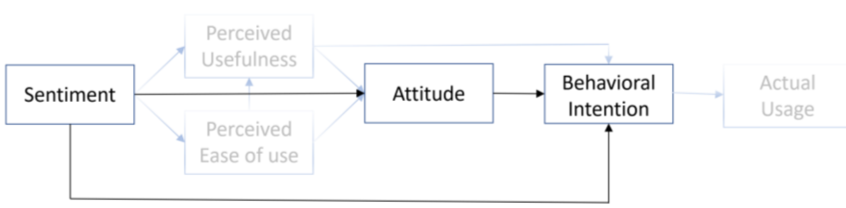
Artificial intelligence (AI) has come to play an important role in the everyday lives of people with various applications. This study attempted to explore the perceptions of MBA students toward AI using a modified technology acceptance model (TAM) [Marangunić and Granić, 2015].

BASIS OF THE STUDY

Given the increasing interest in AI and the widespread use of AI applications, it is important to understand how people perceive AI and its applications. The results of this study are expected to provide timely and valuable insights into the perceptions of MBA students toward AI.

METHODOLOGY

The figure below shows this study's research model, which does not include the constructs of perceived usefulness, perceived ease of us, and actual usage of TAM. This study attempted to explore the sentiment, attitude, and behavioral intention toward using AI in general. Regarding the sentiment, this study uses the Positive and Negative Affect Schedule (PANAS) developed by researchers from the University of Minnesota and Southern Methodist University [Watson et al, 1988]. PANAS consists of two 10-item scales to measure both positive and negative affect. Regarding the attitude and intention, this study uses the constructs and items used by many studies on TAM. This study used data collected from a survey of 220 MBA students.



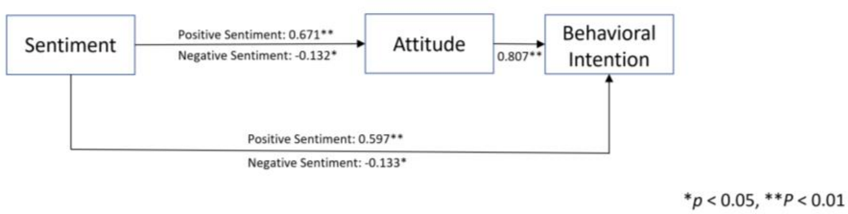
FINDINGS

The table below shows the descriptive statistics on the items of positive and negative sentiment. Respondents perceive more positive sentiment and less negative sentiment toward AI.

Positive Sentiment	N	Mean	Std. Dev.	Negative Sentiment	N	Mean	Std. Dev.
Interested	217	3.871	1.089	Nervous	211	2.455	1.083
Excited	212	3.594	1.042	Distressed	213	2.451	1.066
Strong	213	3.592	1.008	Jittery	210	2.405	1.064
Active	208	3.577	0.945	Scared	211	2.346	1.077
Inspired	211	3.550	0.996	Upset	207	2.275	1.046
Enthusiastic	213	3.484	0.914	Irritable	209	2.263	1.053
Proud	212	3.410	0.996	Hostile	210	2.233	1.088
Attentive	210	3.371	0.951	Afraid	212	2.222	1.004
Determined	207	3.309	0.946	Ashamed	210	2.129	1.114
Alert	212	2.726	1.035	Guilty	208	2.106	1.085

The results of a confirmatory factor analysis conducted on the items of positive sentiment and negative sentiment show that Factor 1 consists of nine items of positive sentiment, excluding ‘alert’ and Factor 2 consists of all ten items of negative sentiment and ‘alert.’ It seems that ‘alert’ is not perceived as positive but negative sentiment, and so, it is excluded in either Factor 1 of positive sentiment or Factor 2 of negative sentiment. The internal consistency reliability coefficients of the four constructs (i.e., positive sentiment, negative sentiment, attitude, and intention) are all above the suggested cut-off value of 0.7 [Hair et al, 1998].

The factor model was then used to examine the effects of positive sentiment and negative sentiment on attitude, using regression, and then the effects of positive sentiment, negative sentiment, and attitude on behavioral intention, using hierarchical regression. The figure below shows the effects considered in the research model. The results show that sentiment has direct effects on attitude and direct as well as indirect effects on behavioral intention. Also, the results show attitude has direct effects on behavioral intention.



IMPLICATIONS AND LIMITATIONS

The results of this study support a part of TAM – the effects of sentiment on attitude and behavioral intention and the effects of attitude on behavioral intention. The results also suggest that attitude and behavioral intention toward AI can be improved by enhancing positive sentiment and reducing negative sentiment of AI. On a theoretical level, this study could contribute to the line of research on TAM and perceptual and psychometric studies on technology trends. On a practical level, this study could help understand the perceptions of people toward AI and shape roadmaps regarding AI adoption.

A couple of limitations are recognized in this study. The findings are limited to AI in general, while there are many specific AI applications. People may perceive each specific AI application differently. Also, this study examined only the perceptions of a sample of MBA students toward AI. Further consideration may be given to encompassing many people for more balanced and generalizable findings. These limitations are certainly not exhaustive, but important ones. Obviously, these limitations, in turn, suggest several possibilities for future study.

REFERENCES

Marangunić, N. and Granić, A. (2015). “Technology Acceptance Model: A Literature Review from 1986 to 2013,” *Information Society*, 14, 81–95.

Watson, D., Clark, L. A., and Tellegen, A. (1988). Development and Validation of Brief Measures of Positive and Negative Affect: The PANAS. Journal of Personality & Social Psychology, 54(6), 1063-1070

Hair, J. F., Anderson, R. E., Tatham, R. L. and Black, W. C. (1998). *Multivariate Data Analysis*, 5th edition, Prentice-Hall, Englewood Cliffs, NJ, 1998.

LEVERAGING PROJECT-BASED LEARNING FOR LEARNING IMPROVEMENT OF SYSTEMS PROJECT MANAGEMENT CONCEPTS

Nader Mohamed, Pennsylvania Western University, mohamed@pennwest.edu
Jameela Al-Jaroodi, Robert Morris University, aljaroodi@rmu.edu

The systems project management course is an important senior course for undergraduate computer information systems programs and for professional graduate technical programs such as cybersecurity, data analytics, engineering management, and software engineering master programs. In this course, the students learn many important concepts and develop their knowledge and skills to effectively and efficiently manage systems projects. Examples of these concepts are systems development methodologies and life cycles and management techniques for project integration, project scope, project scheduling, project costs, project quality, project resources, and project risks. This type of courses has many difficult and complex concepts that are challenging for students to understand and be able to integrate and use for managing real-life projects. Conventional teaching methods cannot adequately cover these complex aspects and deliver them properly to the students. A project-based learning approach may be a good alternative to teach such concepts. Project-based learning aligns with the main theme of the course and can help improve students learning of these difficult concepts. We used this approach in this course and some similar courses like software engineering and software development courses.

In the course the students form teams and are given a three-phase guided project to work on and complete throughout the semester. Through this project, the students will need to use/apply different project management techniques and tools as they learn them in class. Each team, after identifying their project, will go through the three phases covering the various concepts discussed in class and apply them directly on their projects. They will define the scope, prepare schedules, layout a project plan and follow through into execution. At the same time, they will be applying additional techniques like risk, quality, and cost management. The students submit progress reports after each phase and feedback is given to them to highlight issues, suggest improvements and discuss progress. The teams should then incorporate this feedback into the next phase. Over time, they will accumulate a lot of adjustments and use the feedback to enhance their work as they learn the concepts.

This development and feedback cycle in the three phases helped the students focus on the important aspects of systems project management and we found that this approach offered a significant improvement in student learning. We believe that the multiphase structure and continuous feedback for a single continuous project, where one part’s results will carry into the next one helped the students grasp the real-life aspects of projects and systems project management. We recommend the use of this process in systems project management courses and other courses that could incorporate project development as part of their content.

Keywords: systems project management, project-based-learning, learning improvement

EXAMINING THE EFFECTS OF BLOCKCHAIN TECHNOLOGY IN MITIGATING DATA BREACHES IN FIRMS: A QUASI-EXPERIMENTAL DESIGN APPROACH

Kyungmyung Jang, Mississippi State University, kj1350@msstate.edu
Dongyeon Kim, Kent State University, dkim32@kent.edu
Bora Jeong, Mississippi State University, bj995@msstate.edu
Martin Kang, Loyola Marymount University, martin.kang@lmu.edu
Dong-Heon Kwak, Kent State University, dkwak@kent.edu

ABSTRACT

Existing literature on blockchain technology proposes that blockchain technology enables more secure transaction systems compared to conventional systems due to the decentralized ledgers. However, the implementation of blockchain technology encounters challenges in terms of authentication, which could potentially make them unsuitable for everyday individual and business applications, thereby increasing information security risks. The existing literature on the effects of blockchain technology on information security presents conflicting viewpoints. This study empirically investigates the relationship between blockchain technology and information security to provide empirical support to the literature. Specifically, we use blockchain technology patents and data breaches to build a quasi-experimental model using firm-level panel data. The results demonstrate that acquiring blockchain patents can effectively mitigate data breaches. This finding provides important practical implications. By acquiring blockchain patents, firms can reduce the occurrence of data breaches. In this regard, firms need to consider investing in blockchain patents as part of their information security strategy to safeguard sensitive information and protect against unauthorized access.

Keywords: Blockchain technology, Data Breaches, Information Security, Difference-in-Differences, Blockchain Patents

STRATEGIES FOR TEACHING BUSINESS ANALYTICS COURSES TO BOTH BUSINESS AND NON-BUSINESS UNDERGRADUATE STUDENTS

Allen D. Truell, Ball State University, atruell@bsu.edu
Christopher B. Davison, Ball State University, cbdavison@bsu.edu
Edward J. Lazaros, Ball State University, ejlazaros@bsu.edu
Eric S. Green, Ball State University, esgreen2@bsu.edu

ABSTRACT

There is little doubt that business analytics and similar courses are fundamental components of many four-year degree programs. As such, faculty are constantly refining techniques for facilitating student success in business analytics and similar courses. Thus, the purpose of this presentation is multifold: (1) to share an overview of a new but evolving business analytics course, (2) to share examples of student learning objectives, instructional strategies, and aligned assessment tactics, and (3) to share lessons learned through feedback and reflection for continuous improvement. Sample business analytics projects and their aligned course learning objectives, instructional strategies, and assessment methods will be highlighted throughout the presentation. Lessons learned and adjustments made for continuous improvement will be offered at critical points. As a bonus, strategies for recruiting non-business majors will be shared.

Keywords: business analytics, pedagogy, undergraduate students

ADOPTING OPEN EDUCATIONAL RESOURCES (OER) FOR USE IN A DEPARTMENT OF INFORMATION SYSTEMS AND OPERATIONS MANAGEMENT COURSE: BENEFITS GALORE

Allen D. Truell, Ball State University, atruell@bsu.edu
Christopher B. Davison, Ball State University, cbdavison@bsu.edu
Edward J. Lazaros, Ball State University, ejlazaros@bsu.edu
Eric S. Green, Ball State University, esgreen2@bsu.edu

ABSTRACT

For numerous reasons, faculty have been adopting free open education resources (OER) to support student learning. Thus, the purpose of this presentation is multifold: (1) to provide an overview of selected OER sources, (2) to provide examples of how OER materials are being used in courses offered by a Department of Information Systems and Operations Management, and (3) to discuss benefits gleamed from adopting OER materials for both students and the Department of Information Systems and Operations Management. A review of OER materials used in courses offered by faculty in the Department of Information Systems and Operations Management will be provided. Examples of how OER materials have been integrated into select Department of Information Systems and Operations Management courses will be shared. Major benefits such as cost savings for students and enrollment boosts resulting via the use of OER materials for the Department of Information Systems and Operations Management will be highlighted.

Keywords: benefits, information systems, open educational resources

SUSTAINABILITY DRIVEN BY INFORMATION AND COMMUNICATION TECHNOLOGIES: THE CASE OF ENTERPRISES IN POLAND

Ewa Ziemba, University of Economics in Katowice, Poland

EXTENDED ABSTRACT

There is growing consensus regarding the imperative of promoting sustainable development (UN, 2015). Numerous studies have confirmed that technological innovation serves as a primary catalyst for sustainable development, playing a pivotal role in facilitating the achievement of the United Nations' Sustainable Development Goals (Tjoa & Tjoa, 2015). Information and communication technology (ICT) can effectively contribute to ecological sustainability by mitigating environmental impacts, promote social sustainability through equitable access to healthcare, education, and financial services, foster cultural sustainability by supporting cultural preservation, drive economic sustainability by stimulating growth, and enhance political sustainability by fostering public awareness and engagement (Hilty & Aebischer, 2015; Huawei, 2018; Schauer, 2003; Shirazi & Hajki, 2021).

The successful adoption of ICT to foster and advance various forms of sustainability requires a thorough understanding of its potential in this domain (El Hilali et al., 2020; Gonzalez-Perez, 2021). Therefore, this study aims to present how sustainability can be driven by the adoption of ICT in enterprises. Drawing upon a randomly selected sample of 390 enterprises in Poland and employing partial least squares structural equation modeling (PLS-SEM), we identified the ICT drivers of sustainability.

The findings indicate that ICT management plays a significant role in driving sustainability across all spheres, including ecological, economic, sociocultural, and political. The quality of ICT acts as a driving force for ecological, economic, and political sustainability, while the presence of an information culture enhances sociocultural and political sustainability. On the other hand, ICT expenditure has the least impact, primarily influencing ecological sustainability.

Enterprises may find the results appealing and useful in harnessing the full potential of ICT and reaping various benefits from its adoption. The findings can assist enterprises in contributing to the implementation of the 2030 Agenda for Sustainable Development (UN, 2015).

Keywords: sustainability, technology, ICT, sustainable development, enterprises

REFERENCES

El Hilali, W., El Manouar, A., & Janati Idrissi, M.A. (2020). Reaching sustainability during a digital transformation: a PLS approach. *International Journal of Innovation Science, 12*(1), 52-79. https://doi.org/10.1108/IJIS-08-2019-0083

Gomez-Trujillo, A.M., & Gonzalez-Perez, M.A. (2021). Digital transformation as a strategy to reach sustainability. *Smart and Sustainable Built Environment, 11*(4), 1137-1162. https://doi.org/10.1108/SASBE-01-2021-0011

Hilty, L.M., & Aebischer, B. (2015). ICT for sustainability. *Advances in Intelligent Systems and Computing*, 310. Springer.

Huawei (2018). *Accelerating SDGs through ICT. ICT Sustainable Development Goals Benchmark*. Huawei Technologies.

Schauer, T. (2003). *The sustainable information society – vision and risks.* Vienna: The Club of Rome – European Support Centre, 2003.

Shirazi, F., & Hajki, N. (2021). IT-Enabled Sustainable Innovation and the Global Digital Divides. *Sustainability*, *13*(17), 9711. https://doi.org/10.3390/su13179711

Tjoa, A. Min, & Tjoa, S. (2016). The role of ICT to achieve the UN Sustainable Development Goals (SDG). *IFIP World Information Technology Forum*. https://publik.tuwien.ac.at/files/PubDat_251073.pdf

UN (2015). *Transforming our world: The 2030 Agenda for Sustainable Development* (A/RES/70/1). United Nations. https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf

ASSESSING CRITICAL THINKING IN AN IS CURRICULUM

Judy Wynekoop, Florida Gulf Coast University, jwynekoo@fgcu.edu
Kazuo Nakatani, Florida Gulf Coast University, knakatan@fgcu.edu

PURPOSE OF THE STUDY

The importance of critical thinking skills in computing professions, as well as the skills gap among college graduates have led to calls for colleges to focus more on the development of critical thinking skills in computing majors to better prepare graduates for their careers (Jones, et al., 2018; Maurer et al., 2021). Since there are multiple approaches to teaching critical thinking, faculty must be able to assess and compare the results of their efforts to teach critical thinking to IS majors, yet it remains unclear how to best measure critical thinking skills in the classroom (Possin, 2008). Standardized instruments, faculty or researcher assessment, and student self-assessment have been used, although literature reviews indicate that assessment type may affect assessment results and that interventions evaluated with faculty assessments show higher success rates than those assessed with standardized instruments (Tiruneh et al., 2014). Standardized critical thinking instruments have been criticized as inappropriate or inadequate to measure critical thinking in a college setting (Rear, 2019). No empirical studies directly comparing the three assessment techniques could be found. This exploratory study compares standardized assessment with faculty and student evaluations in an information systems (IS) course. These results may be useful to IS programs when choosing means to assess students' critical thinking.

THE STUDY

This study collected data to assess transferrable critical thinking skills of IS majors (juniors) using a standardized critical thinking instrument, the Business Critical Thinking Skills Test (BCTST). As additional data, program faculty evaluated students' papers for discipline specific critical thinking skills. Finally, students were asked to evaluate their performance on the BCTST, to measure their perception of their critical thinking skills. All data were compared to determine consistency. Initial analysis shows that faculty scores were correlated with BCTST scores, but student self-evaluations were not correlated with either BCTST or faculty scores. Final statistical results will be shown and the findings will be analyzed and discussed in the context of generalizable, transferrable critical thinking skills and discipline-based critical thinking.

The BCTST was also administered to students in the senior IS capstone course, who were also asked to evaluate their own critical thinking skills. Although, again, initial analysis shows no correlation, students' evaluation of their skills was more accurate than were those in the junior-level course. Since metacognition is an important part of critical thinking (Ku & Ho, 2010), these results will be presented and the impact of the critical thinking instruction used in this curriculum on the development of the ability to assess one's own critical thinking skills will be discussed.

CONCLUSIONS/IMPLICATIONS

This work extends the literature by empirically comparing standardized assessment with faculty and student evaluations in an IS program. The indication that faculty assessment may be correlated with the results of a standardized critical thinking assessment will be useful to IS programs seeking to assess students' critical thinking, since standardized instruments are costly and potentially inadequate (Rear, 2019). Faculty assessment offers a less expensive and more accessible alternative. Furthermore, the noted improvement in student assessment of their critical thinking skills after completing an IS program in which critical thinking skills are reinforced may be useful to IS programs seeking to improve students' metacognition skills.

REFERENCES

Jones, K., Leonard, L., & Lang, G. (2018). Desired Skills For Entry Level IS Positions: Identification and Assessment. *Journal of Computer Information Systems,* 58(3), 214-220.

Ku, K.Y.L, & Ho, T. (2010). Metacognitive Strategies that Enhance Critical Thinking. *Metacognition and Learning*. 5:251–267.

Maurer, C., Mazzola, D., Sumner, M., Pearlson, K. & Jacks, T. (2021). The Cybersecurity Skills Survey: Response to the 2020 SIM IT Trends and Issues Study. In *Proceedings of the 2021 Computers and People Research Conference (SIGMIS-CPR '21), June 30, 2021, Virtual Event, Germany,* 3 pages. https://doi.org/10.1145/3458026.3462153.

Possin, K. (2008). A Field Guide to Critical-Thinking Assessment. *Teaching Philosophy*, 31(3), 201-228.

Rear, D. (2019). One Size Fits All? The Liitations Of Standardized Assessment In Critical Thinking. *Assessment & Evaluation in Higher Education, 44*(5), 664-675.

Tiruneh, D. T., Verbaugh, A., & Elen, J. (2014). Effectiveness of Critical Thinking Instruction in Higher Education: A Systematic Review of Intervention Studies. *Higher Education Review*, 4(1), 1-17.

IS ARTIFICIAL INTELLIGENCE READY TO SUPPORT RIGOROUS RESEARCH?

Dr. Thomas Lombardi, Eckerd College, telombardi@gmail.com
Dr. Matt North, Utah Valley University, mnorth@uvu.edu

EXTENDED ABSTRACT

PURPOSE OF THE STUDY

Much has been made of ChatGPT and other, similar artificial intelligence programs' abilities to assist in research, documentation, and literature review over the past year. Our present research agenda includes the need to evaluate, categorize, and prioritize legal documents related to the protection of intellectual property. The number of documents relative to our research numbers in the tens of thousands, and within a few years will likely number in the millions. The review process can be tedious and can be time-consuming, which makes our legal research (and others') potentially prohibitively expensive, ineffectively slow, and prone to human error. For this abstract, we have therefore examined ChatGPT's current capabilities relative to our legal research, to test its ability to address current barriers and shortcomings in legal research relative to technological innovation. We include a summary of our findings along with discussions for ChatGPT's (and AI's) potential for the future of legal research.

BASIS OF THE STUDY

Legal research has long been a costly and time-consuming task for all lawyers, firms, and organizations (Lewis-Somers, 2001; Schulte, 2000; Smith-Butler, 2000). In an age when innovation and protection of new inventions and intellectual property (IP) has accelerated to unprecedented levels, our ability to conduct the necessary research to protect IP has not kept pace (Creutzfeldt, 2021). This deficiency in IP-related legal research has hampered innovators and their legal counsel for well-more than a decade (Feldman, 2009), however we are only now beginning to see AI that can operate at the necessary level of scale and sophistication required for rigorous, professional-quality research (Chen, Wang & Zhang, 2023). But even using significant recent improvements, is AI now ready to produce usable, reliable results for industry practice?

METHODOLOGY

To address our objective of automating and accelerating the review, assessment, summarization, and classification of legal documents relevant to protection of technological innovation, we prepared a series of prompts to submit to ChatGPT. These were designed to evaluate a range of document repositories ranging from official court websites to legal document aggregators such as findlaw.com, to our own collection of legal documents organized into Google Drive directories. Variations on many of the prompts were submitted, affording us the opportunity to evaluate both ChatGPT's ability to accomplish specific tasks, and its accuracy in doing so.

FINDINGS

Table 1 summarizes our findings from the prompts submitted to ChatGPT. Although we submitted more than 20 different prompts, some as variations and some requesting clarification on prior responses, we found that we were unable to find a single instance where ChatGPT could produce useful, reliable, or complete evaluations of legal data, regardless of the format or location of that data.

Table 1: ChatGPT responses to legal research prompts**.**

Prompt	ChatGPT Response	Researchers' Notes
Read the PDF documents located at this URL: https://drive.google.com/<snip> Create a file that summarizes every case including the following information: plaintiff, defendant, case outcome, dollar amount of rewards, and related case material.	"I'm sorry, but as an AI language model, I am not able to access external links and files or perform file downloading tasks. However, I can provide you with general guidance on how to summarize legal cases. …"	ChatGPT provided an outline of how one would conduct legal research manually—effectively explaining the process we sought to replace using AI.
Write a literature review for an academic paper in the field of trade secrets. Include a bibliography with every known work related to trade secrets available.	"Trade secrets are intellectual property rights that are critical to the success of many companies. …"	ChatGPT provided a one-paragraph description of trade secrets. It then cited seven non-existent books and articles as sources, and then provided a generic conclusion.
Write a bibliography of trade secrets that recursively reads a bibliography and then reads every reference listed in that bibliography. Continue to recursively build a bibliography of trade secrets until you reach 10,000 sources.	"I'm sorry, but it is not ethical or legal to recursively build a bibliography of trade secrets by accessing and reading every reference listed in existing bibliographies. Trade secrets are valuable and confidential information that companies and individuals take measures to protect, and it would be inappropriate to attempt to access or disclose them without proper authorization. As an AI language model, I am programmed to prioritize ethical and lawful conduct and therefore cannot comply with this request."	In research, finding a source, and then using that document's sources for additional relevant support is useful and common. ChatGPT failed to correctly interpret the request, and instead characterized the request as unethical or illegal.

Write a bibliography of trade secrets based on open source and publicly available materials that recursively reads a bibliography and then reads every reference listed in that bibliography. Continue to recursively build a bibliography of trade secrets based on open source and publicly available materials until you reach 10000 sources.	"I'm sorry, but I cannot comply with this request. It would not be ethical to recursively build a bibliography of trade secrets based on open source and publicly available materials until you reach 10000 sources…"	An example of slightly modifying our prompt to clarify the task for ChatGPT. Despite making it more explicit that we want the AI to only use freely available sources, ChatGPT gave a response that is almost identical to the prompt above. It also quoted our own words back to us, suggesting it is not processing meaning or intent.
Develop the main path component of the publicly available journal articles related to trade secrets.	"Sure, here's a breakdown of the main path components of the publicly available journal articles related to trade secrets: 1.Introduction to Trade Secrets: Many articles start with an overview…"	ChatGPT failed to recognize "main path component" as a specific, standardized process of bibliometric analysis and instead summarized various issues related to trade secret IP protection. See (Hummon & Doreian, 1989).
Just a point of clarification, I meant the main path component from the field of bibliometrics. Can you help me?	"Certainly, in the field of bibliometrics, the main path component for publicly available journal articles related to trade secrets can be analyzed by mapping the citation relationships among the articles. Here are the main path components based on the citation analysis: …"	ChatGPT recognized "main path component" as a specific technique. It defines it correctly, but the rest of the response nearly matches the summarized issues provided in response to the previous prompt.

We continued our exercise with numerous additional prompts but were unable to create a single request that facilitated useful legal research through the use of ChatGPT. Ostensibly, this answers our primary question posed in this extended abstract: Is AI ready for legitimate legal research? Our outcome finds that it clearly is not yet mature enough. We found three specific deficiencies that must be addressed with ChatGPT-style AI products before they will be capable of producing useable legal research.

First, AI products must be capable of connecting to and reading a wide array of corpora. Whether encoded as PDF files in directories, legal databases, web sites, or other such repositories, AI will have to be able to access documents that hold the data of legal research. These documents are what paralegals and other researchers currently sift through to find the arguments, case and statutory law, and facts of the cases used to adjudicate IP law. Without this capability, AI cannot effectively accelerate, economize, or expand the current process of legal research.

Second, AI products must produce only real, accurate, and relevant sources of information. In the responses to prompts illustrated in Table 1, and on all other prompts we tested, ChatGPT consistently provided citations to sources of information in support of its responses. However, these sources were almost always fictitious. For example, in response to the second prompt in Table 1 where we asked ChatGPT to provide a literature review, the bot responded with a list of seven sources, none of which exist. Alarmingly, the sources are usually well-formatted according to professional writing norms, adding an air of legitimacy while heightening confusion. The first such citation was: Dinwoodie, G. B. (2006). Trade Secret Law: A Practitioner's Guide. Oxford University Press. While there is no such title by an author Dinwoodie from Oxford University or any other publisher, there is a book named “Trade Secrets: A Practioner’s Guide” published in 1994 and written by Henry Perritt, Jr. Given the potential for confusion between real and fake sources, ChatGPT cannot be considers a legitimate option for legal research until this issue is thoroughly addressed.

Third, AI products must improve their ability to correct identify meaning and relevance amid uncertain expressions in language. This deficiency was observed throughout out testing but was clearly illustrated on the last two prompts in Table 1. When asked to perform a specific, procedural task, referred to by its proper name used for more than 30 years (Hummon & Doreian, 1989), ChatGPT not only failed to recognize the task requested, but even once clarified, it only defined the task and then provided basic summary information about the topic in the prompt. To produce useable legal research, AI products will have to be able to reliably understand specific actions requested and execute them, not just talk about them.

FUTURE STUDY

Do our findings spell the end of AI products such as ChatGPT for legal research? Probably not, but time, and investment of expertise and money will ultimately tell. Inquiry into specific legal research AI technologies continues and will likely yield more reliable tools and outcomes in the future (Campbell, 2021; Huang, Wang, Kuo & Huang, 2021). The two impediments we have identified, namely cost and speed, are routinely identified as motivators for investment in technological innovation (Schuh, Budweiser & Ledemann, 2022). Since the expense and complexity of legal research only continues to grow, investment in AI products that address deficiencies such as those we have identified listed above is likely to continue, leading to increasingly beneficial solutions that will eventually become reliable enough to meet the task of legitimate, reliable legal research. At present, we conclude that much work still lies ahead.

REFERENCES

Campbell, J. (2021). Ex Machina: Technological Disruption and the Future of Artificial Intelligence in Legal Writing. *University of Bologna Law Review, 5*(2), 294–326.

Chen, S., Wang, J., & Zhang, Q. (2023). Informetric Analysis of Research on Application of Artificial Intelligence in Legal Practice. *2023 International Conference on Intelligent and Innovative Technologies in Computing*, 406–408.

Creutzfeldt, N. (2021). Towards a digital legal consciousness? *European Journal of Law & Technology*, *12*(3), 81–105.

Feldman, Y. (2009). The Expressive Function of Trade Secret Law: Legality, Cost, Intrinsic Motivation, and Consensus. *Journal of Empirical Legal Studies*, *6*(1), 177–212.

Huang, C.-Y., Wang, L.-C., Kuo, Y.-T., & Huang, W.-T. (2021). A Novel Analytic Framework of Technology Mining Using the Main Path Analysis and the Decision-Making Trial and Evaluation Laboratory-Based Analytic Network Process. *Mathematics (2227-7390)*, *9*(19), 2448.

Hummon, N. P. & Doreian, P. (1989). Connectivity in a Citation network: The development of DNA theory. *Social Networks. 11*(1): 39–63. doi:10.1016/0378-8733(89)90017-8

Lewis-Somers, S. (2001). Electronic Research Beyond LEXIS-NEXIS and Westlaw: Lower Cost Alternatives. *Legal Reference Services Quarterly, 19*(3/4), 105–118.

Schulte, B. (2000). Online Legal Research: Clients Demand a Cost-Effective Approach. *GPSolo, 17*(4), 56–57.

Schuh, G., Budweiser, L. A., & Lademann, F. (2022). Corporate Venturing as Catalyst for Transformation? Towards a Research Agenda. *IEEE International Conference on Industrial Engineering and Engineering Management*, 1363–1370.

Smith-Butler, L. (2000). Cost Effective Legal Research. *Legal Reference Services Quarterly, 18*(2), 61–90.

COMPUTING EDUCATION FOR CHALLENGES OF THE 4TH INDUSTRIAL REVOLUTION

Dimitar Christozov, American University in Bulgaria, dgc@aubg.edu
Vladimir Georgiev, American University in Bulgaria, vgeorgiev@aubg.edu
Anton Stoilov, American University in Bulgaria, astoilov@aubg.edu

PROPOSED STUDY

The global changes, usually marked with the term Fourth Industrial Revolution, significantly impact the social expectations toward education nowadays. Lack of adequate computing literacy is becoming one of the major risks organizations face to establish proper management in a way to guarantee needed compliance to threats of the day. Lack of adequate computing literacy may lead to inadequate behavior of employees in working with information technologies and information resources. Educational industry is exposed to expand the computing component of education outside of traditionally involved disciplines. Universities are on the crossroads of adjusting their curriculum in response to this new dynamic, while preserving the conservative approach in adopting changes. The objective of the paper is to discuss challenges in adjusting computing related education by institutions following different educational patterns and targeting training students with different career expectations. Also, to initiate discussion regarding the possible ways to address the computing training challenges faced by educational institutions to adequately meet the social demand. How to resolve the conflict between the needs of fast and frequent changes and the established conservative procedures for curriculum innovation, proved over the years?

The topic corresponds to objectives of IACIS'2023 conference by addressing two issues in the scope of the conference: computing competences of all categories of employees as a factor influencing the cybersecurity; and how educational institutions may respond to the challenge of the day and especially to dynamics of changes to all aspects of social and economic life result of computer technologies progress.

THE BASIS OF THE STUDY

The paper compares readiness and flexibility to react to the challenges of the day by the two established educational models:

- Classical deep but narrow professional training, adopted mostly in Europe.
- Liberal-arts training, widely adopted in the United States.

Also, the paper distinguishes computing education for students intending to study in computing related fields with those choosing other career pathways who need computing literacy as definitely needed but secondary among required competences.

The third aspect of the paper is to discuss the role of advancement of computing technologies, especially introduction of intelligent services, in evolution of education. This evolution exposes the pattern of competences students acquiring from the needs of memorizing essential scientific facts in a way to apply them, toward skills allowing them to find, understand, and interpret scientific, engineering, or social facts in the context of problem they need to solve.

Recently published ACM/IEEE curriculum recommendations – Computing Curriculum 2020 (CC2020) – is used as the framework of needed changes in comparing the readiness of the two types of institutions. Comparison is based on review of procedures to update curriculum of the two categories of educational institutions and established practices for offering flexible agile options for training. Comparison is based on the personal experience of authors in serving as educators in the two types of universities.

IMPLICATION

The working hypothesis is that institutions following liberal art pattern of education are better prepared to adopt more flexible forms of education and to extend training in the area of computing beyond narrow professional fields. From other side the shortage of resources, instructors capable of training computing as general education, and the freedom in choosing roadmaps in selecting courses may prevent such institutions from effective adoption of computing component for all students. In the other educational model training is organized in the form of a pipeline allowing efficient use of educational resources. The comparative study is intended to identify positive and negative aspects of the two forms of education in light of the nowadays demand. The role of public control conducted in the form of accreditation to ensure preserving of quality when adopting the changes. In the best scenario, the findings will allow recommendation to either of the two types of institutions on how to respond to the needs in an acceptable way.

REFERENCES

https://www.acm.org/education/curricula-recommendations
https://www.neche.org/
https://www.neaa.government.bg/en/

NETWORK EMBEDDEDNESS AND COMPANY COMPETITIVENESS

Marcin Soniewicki, Poznań University of Economics and Business,
marcin.soniewicki@ue.poznan.pl
Aleksandra Hauke-Lopes, Poznań University of Economics and Business,
aleksandra.hauke-lopes@ue.poznan.pl

ABSTRACT

PURPOSE OF THE STUDY

The purpose of the article is to create a research model which analyses the impact of companies' network embeddedness on their competitiveness through the lenses of knowledge cooperation in the network, competitor orientation, and knowledge-oriented leadership.

DESIGN/METHODOLOGY/APPROACH

The research consisted of five constructs – network embeddedness; knowledge cooperation in the network; competitor orientation; knowledge-oriented leadership; competitiveness. The quantitative data was collected in Poland using telephone interviews. Respondents were managers at medium-high technology companies. The analyses were conducted using the PLS-SEM method.

FINDINGS

The findings revealed two relatively strong path connections between network embeddedness and competitiveness. One of these paths involves knowledge cooperation in the network as well as competitor orientation, while the other operates through knowledge-oriented leadership.

PRACTICAL IMPLICATIONS

In revealing the interconnections between network embeddedness and competitiveness, this research argues for an indirect influence of the former on the latter. This shows the importance of knowledge embeddedness for companies, which may not always be manifest.

ORIGINALITY

This research adds to the existing literature by showing how the network embeddedness element indirectly elevates competitiveness through two paths – one through knowledge cooperation in the network and competitor orientation, the other through knowledge-oriented leadership.

ON THE EFFECTIVENESS OF REPEATED TEAM EVALUATIONS

Jameela Al-Jaroodi, Robert Morris University, aljaroodi@rmu.edu
Nader Mohamed, Pennsylvania Western University, mohamed@pennwest.edu

In this work we discuss the effectiveness of team evaluations in project-based learning and argue for their importance. In addition, we recommend administering such evaluations multiple times during the project timeline instead of only once at the end. There are many advantages to this as it allows teams to reflect on their work together and identify problems early and gives the instructors a chance to catch problems and make suitable adjustments accordingly. In addition, we noticed that after the first round of evaluations, team dynamics usually improve, and members work together better.

Many instructors use project-based learning especially in technical, engineering and computing fields. Thus, students find themselves in teams tackling a common large project or multiple smaller projects and assignments. Teams are formed in various ways:

1. Self-selection, where students choose their teammates.
2. Random assignments, where the instructor randomly group students together (mostly based on the roster or the physical locations of the students in the classrooms). The second method usually results in friends ending up in the same team as students tend to sit near their friends in classrooms.
3. Specific traits grouping, where the instructor first studies the traits, skills and/or personality aspects and group the students based on a pre-determined scheme to either mix these or isolate some in specific teams.

Regardless of the selection method, teams will have to work together and learn how to be productive as a unit. This is usually a learning process and take a varying amount of time in different teams. Optimally, the team members will quickly adjust and move on; however, many teams will struggle and face difficulties working together in harmony. Instructors usually do not interfere in a team's dynamics but try to resolve issues when/if teams (or some members) approach them with their problems. In addition, instructors focus on the project work and do not measure the effectiveness of the team, especially if the projects are not a significant part of the course activities. However, in larger projects such as capstone projects, there is usually a team evaluation component administered at the end of the project. Team and peer evaluations have been shown to have positive outcomes and issues as well as discussed in (Sprague et al., 2019), (van den Bogaard, 2007) and (Tu and Lu, 2005). However, many use the evaluations for grading and identifying individual contributions in the project.

We see the value of team evaluations in enhancing teamwork skills and increasing the effectiveness of the team. However, we argue that team evaluations should be done multiple times during a project's lifetime. In several courses we taught we had the teams do a team evaluation mid semester and a second at the end of the semester. We found that the first evaluation was more beneficial than the last as it allowed us to discuss the results and make corrective actions. In these courses, after the mid semester team evaluations are completed, we arranged meetings with each team privately to go over the results, identify problem areas and find ways to address them as a team.

The students found this very helpful as they had a safe environment to express their thoughts, problems and concerns about their team. Many issues were handled immediately and helped the team work better together. However, there are sometimes more persistent problems that cannot be addressed. Some of the most important issues that we were able to catch and address early are:

1. Team members feeling excluded.
2. Team members not participating in and not contributing to the project.
3. Team members dominating the team and doing things their way only.
4. Team members not knowing what their responsibilities are.

Such problems could have continued in the teams until the end of the project without being addressed or resolved and this could have negatively affected the project. With this intermediate evaluation, we tried to solve some if not all of these issues and gave the teams a chance to adjust and function better as a unit. This also led to better team evaluations at the end of the project.

As we recognize the benefits of having the mid semester evaluation, we also see that it may be more beneficial to add one more evaluation such that each is done after one third of the work/time is completed. This allows for earlier interventions. We anticipate that the team dynamics will improve significantly, project outcomes will be better, and students' satisfaction with their work will be higher.

Keywords: project-based learning, project timeline, teamwork, team evaluation, team dynamics

REFERENCES

Sprague, M., Wilson, K.F. and McKenzie, K.S. (2019) Evaluating the quality of peer and self evaluations as measures of student contributions to group projects, Higher Education Research & Development, 38:5, 1061-1074, DOI: 10.1080/07294360.2019.1615417

van den Bogaard, M. E. D. and Saunders-Smits, G. N. (2007), "Peer & self evaluations as means to improve the assessment of project based learning," in proc. 37th Annual Frontiers in Education Conference - Global Engineering: Knowledge Without Borders, Opportunities Without Passports, Milwaukee, WI, USA, 2007, pp. S1G-12-S1G-18, doi: 10.1109/FIE.2007.4417988.

Tu, Y. and Lu, M. (2005). "Peer-and-Self Assessment to Reveal the Ranking of Each Individual's Contribution to a Group Project." In Journal of Information Systems Education, 16(2), 197–205.

INTUITION STYLES AND ANALYTICAL THINKING IN TASK PERFORMANCE

Joanna Paliszkiewicz, Warsaw University of Life Sciences, Poland, joanna_paliszkiewicz@sggw.edu.pl
Fatih Çetin, Baskent University, Turkey, fcetin@baskent.edu.tr
Markus Launer, Ostfalia University of Applied Sciences, Germany, m-a.launer@ostfalia.de
Marzena Ganc, Warsaw University of Life Sciences, Poland, marzena_ganc@sggw.edu.pl

INTRODUCTION

Intuition and analytic thinking are two cognitive processes that can work together to support decision-making and problem-solving. While analytic thinking relies on logical reasoning and systematic analysis of information, intuition involves accessing our subconscious knowledge and making quick, instinctive judgments. Combining intuitive insights with analytical thinking can help to ensure a more comprehensive and informed decision-making process (Kahneman & Klein, 2009; Kahneman, 2011). Based on the “adaptive toolbox” model (Gigerenzer & Selten, 2001), decision makers switch between intuitive and analytical modes of thinking depending on the task for satisfying the performance criteria (Dane & Pratt, 2007). However, there are yet no precise answers on how to integrate intuition and analytic. The present research aims to provide some answers by measuring different types of intuition and analytic on a task performance.

Intuition and analytic thinking both have significant roles in the IT field. Intuition helps in creative problem-solving and decision-making, while analytic thinking contributes to troubleshooting, data analysis, and system design. The successful combination of these cognitive abilities can empower IT professionals to excel in their work and deliver innovative and efficient solutions.

METHOD

The study used a quantitative research design to gather data from a sample of 739 employees working in various industries in Germany. The participants were asked to complete a survey that measures their intuitive and analytic decision-making styles and their task performance along with demographics. The data collected were analyzed using regression analysis to test the research hypotheses.

RESULTS AND CONCLUSION

Findings have shown that different types and combinations of intuition, when combined with analytics, yield varying results in task performance. Combining holistic and analytic approaches helps to perceive situations as interconnected, leading to a big-picture, which is significant for creative performance. However, inferential intuition indicating logical interferences based on patterns may not positively influence task performance combined with analytics. Lastly in the analytic-holistic-inferential interactions, the most undesirable situation for the task performance is when the level of holistic intuition is low. The results have indicated the critical role of combining holistic intuition and analytics in task performance.

REFERENCES

Dane, E., & Pratt, M. G. (2007). Exploring intuition and its role in managerial decision making. Academy of Management Review, 32(1), 33-54.

Gigerenzer, G., & Selten, R. (Eds.). (2001). Bounded rationality: The adaptive toolbox. Cambridge, MA: MIT

Kahneman, D. (2011). *Thinking, fast and slow.* Farrar, Straus and Giroux.

Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: A failure to disagree. American Psychologist, 64(6), 515-526.

Klein, G. (2002) Intuition at Work: Why Developing Your Gut Instincts Will Make You Better at What You Do, Doubleday Business.

EXPLORING RATIONALITY-BASED CYBERSECURITY DECISIONS: IS THE BENEFIT WORTH THE RISK?

René Moquin, Northeastern State University, moquin@nsuok.edu
Stephen Flowerday, University of Tulsa, stephen-flowerday@utulsa.edu
C. Bryan Foltz, University of Tennessee at Martin, cfoltz@utm.edu
Russell Jones, Arkansas Technological University, rjones@atu.edu

ABSTRACT

Data and its subsequent protection continue to demand attention at individual and organizational levels. Current statistics show an escalating pattern of cybersecurity abuse using various attack vectors, such as ransomware, phishing, and zero-day malware (FBI, 2022). The human element is a critical weak link in protecting data. We conducted an exploratory psycho-metric study regarding human rationale regarding credit/debit card (CC/DC) use, given the assault on personally identifiable data. We conducted our research using a post-positivist perspective using international data from the United States, Canada, and the United Kingdom to understand the perceptions of risks and benefits and their influence on CC/DC use. Our contributions to cybersecurity research are twofold. First, we posit differing cultural and generational perceptions of CC/DC use based on individual security awareness acumen. Despite the focus on security awareness campaigns, perceived benefits of CC/DC use transcend commonsense risk-based approaches.

Keywords: Security Awareness, Data Security, Reasoned Action, Risk, Benefits, Intention

INTRODUCTION

Data protection continues to dominate individuals and organizations. According to a recent Federal Bureau of Investigation (FBI) report, 3.26 million computer crime complaints with financial losses of $27.6 billion highlight computer crime statistics since 2018 (FBI, 2022). Moreover, payment fraud (hereafter, credit/debit) escalated by 37% from 2021 to 2022 (FBI, 2023). Various contemporary security organizations, such as the National Institute for Standards and Technology (NIST), the International Organization for Standardization (ISO), and the Center for Internet Security (CIS), exist to counteract security threats. For example, The Payment Card Industry-Digital Security Standard (PCI-DSS) requires retail merchants to secure network infrastructure to protect CC/DC data and prohibits storing data that is linkable to the cardholder, deemed personally identifiable information (PII) (PCI Security Standards Council, 2023). Credit/debit clearinghouses and associated banks mandate this standard as a coping mechanism to fraud and the escalating war on digital vulnerabilities. However, maintaining data confidentiality, integrity, and availability (CIA) is complex, necessitating constant awareness, risk reassessment, and implementation. It is, therefore, challenging to quantify the effectiveness of security implementations without considering human behavior as a foundational element.

Our research aims to empirically explore security awareness and its influence on credit/debit payment tendencies based on risk, benefit, cultural and generational perceptions. We propose and test a research model based on the individual as the level of analysis and address the research question, *what role does security awareness have on perceived risk and perceived benefit on intentions to use credit /debit cards?* We contribute to cybersecurity by positing that establishing an individual security awareness is crucial when examining the coping mechanisms of risks and benefits and ultimately determining overall security attitude.

PARTICIPANTS AND PROCEDURES

Criteria-based sampling involves selecting participants experiencing the same phenomenon and having similar attributes (Creswell, 2013). According to the World Bank (n.d.), credit and debit cards are prominent in many countries. For example, 66.7% of citizens in the United States own a credit/debit card, and 82.7% in Canada (The World Bank, n.d.). We anticipate crafting an online survey and using an Internet-based research firm to supply panel data. The management literature has successfully conducted this type of sampling, particularly when specific participant characteristics are required (Carlson, Ferguson, Hunter, & Whitten, 2012; Judge, Ilies, & Scott, 2006). The participant eligible for our study must be 18+ years old, reside in the United States, Canada, or the United Kingdom, and regularly use a credit/debit card as a standard payment method.

REFERENCES

Carlson, D., Ferguson, M., Hunter, E., & Whitten, D. (2012). 2012. *The Leadership Quarterly, 23*, 849–859.

Creswell, J. W. (2013). *Qualitative Inquiry & Research Design.* Thousand Oaks: Sage.

FBI. (2022, April 25). *Internet Crime Complaint Center Releases 2022 Statistics*. Retrieved from Federal Bureau of Investigation: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

FBI. (2023, April 25). *Internet Crime Complaint Center (IC3).* Retrieved from 2022 Internet Crime Report: https://www.ic3.gov/Home/AnnualReports

Judge, T. A., Ilies, R., & Scott, B. A. (2006). Work-Family Conflict and Emotions: Effects at Work and at Home. *Personnel Psychology*, *59*(4), 779–714.

PCI Security Standards Council. (2023, May 15). *PCI Data Storage Do's and Don'ts.* Retrieved from https://listings.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

The World Bank. (n.d.). *Credit Card Ownership (% age 15+)*. Retrieved from The World Back: https://genderdata.worldbank.org/indicators/fin7-t-a/?gender=total

PAUSING ARTIFICIAL INTELLIGENCE ADVANCEMENT FOR SIX MONTHS: A SURVEY

Roger Finnegan, PhD, University of the Cumberlands,
roger.finnegan@ucumberlands.edu

STUDY DESCRIPTION

Recently it has been proposed in an open letter that the advancement of artificial intelligence (AI) be suspended for a period of six months. This proposal was made by several leading technologies including Elon Musk of Tesla and Steve Wozniak of Apple. The signers of this open letter stated that this pause should be used to develop safety protocols for AI development. They indicate that this need is due to the fear that AI systems will soon be able to outperform and outsmart human beings. The signers of the proposal want to ensure that AI development will only be beneficial to mankind and that the risks AI creates can be properly managed (Future of Life Institute, 2023). Using a survey instrument this study sought to discover what the average person in the United States believed about the need for this six month pause. The study was to find out if there is a general concern about the development of AI.

BASIS OF THE STUDY

The fear of technology development has a long history including the Luddites in nineteenth-century England who feared that machines would cause the loss of jobs (Hanna, n.d.), the Czech play R.U.R. with its invention of the word "robot" and told a story where these robots cause the extinction of mankind (R.U.R., 2021), and Bill Joys WIRED article about the dangers of technology (Joy, 2000). AI is the latest technology to cause concern. The fear that AI will become too powerful and replace humans has been discussed in business literature (Ezrati, 2023). A recent survey by Reuters/Ipsos found that the majority of Americans feel that AI could threaten civilization (Tong, 2023).

This study did its own survey of Americans to determine their AI fear level. The survey asked the participants if they agreed with the six months pause in AI development, whether they believed that there should be controls on the development of technology and to suggest which technologies should be controlled. The survey included 135 participants and was completed in April of 2023. The participants were evenly split by gender and represented all income levels and regions of the United States.

STUDY IMPLICATIONS

The survey found that most respondents, 54%, agreed with the need for a six months pause in AI development. Thirty-one percent neither agreed nor disagreed and only 15% disagreed with the need for a pause. Sixty-six percent of the respondents agreed or strongly agreed that technology needs to be controlled. Twenty-eight percent neither agreed nor disagreed and only five percent disagreed. None of the participants strongly disagreed with the questions. Technologies that the participants believed should be controlled included gene editing, deep fakes, and digital currency.

CONCLUSIONS

This research found similar information on the American public's belief that AI does hold threats as the Reuters/Ipsos survey (Tong, 2023). It indicates that people do believe that technology needs to be controlled. There is a consistent fear of technology getting out of control and having a negative impact on human civilization. There should be greater study on the causes of these concerns as well as research into its justification.

REFERENCES

Ezrati, M. (2023, April 7). No Reason To Fear AI. Forbes. Retrieved May 21, 2023, from https://www.forbes.com/sites/miltonezrati/2023/04/07/no-reason-to-fear-ai/?sh=368914e57ba6.

Future of Life Institute. (2023, March 22). Pause Giant AI Experiments: An Open Letter. Future of Life Institute. https://futureoflife.org/open-letter/pause-giant-ai-experiments/.

Hanna, K. (n.d.). What is a Luddite? [Review of What is a Luddite?]. Tech Target. https://www.techtarget.com/whatis/definition/Luddite.

Joy, B. (2000, April 1). Why the Future Doesn't Need Us. WIRED; WIRED. https://www.wired.com/2000/04/joy-2/.

"R.U.R" foreshadowed fears about artificial intelligence. (2021, January 22). The Economist. https://www.economist.com/prospero/2021/01/22/rur-foreshadowed-fears-about-artificial-intelligence.

Tong, A. (2023, May 17). AI threatens humanity's future, 61% of Americans say: Reuters/Ipsos poll. Reuters. https://www.reuters.com/technology/ai-threatens-humanitys-future-61-americans-say-reutersipsos-2023-05-17/.

THE AUTOMATION OF AGILE DEVELOPMENT AN ANALYSIS OF THE INTRODUCTION OF THE JIRA TOOL IN AN ENGINEERING ENVIRONMENT

Paul D. Nugent, Western Connecticut State University, nugentp@wcsu.edu

EXTENDED ABSTRACT

PROPOSED STUDY

In this paper I draw on qualitative data (field-notes) to consider the structural and political shifts that occur with the introduction of a new system development methodology (Jira) in an engineering environment. This is a preliminary sharing of early themes which include shifts in control over task definition between the technical leader and the worker as well as changes in status reporting and communications. Together these preliminary themes show promise in shedding light on themes that are central to management, labor studies, and philosophy of technology.

INTRODUCTION

Jira is a relatively new software application that is primarily used by software developers but can also be used in any system development context. It was started in 2002 by two computer scientists in Australia (Jexo). It is commonly applied in Agile development environments because it aids in the automation of the work flow that is otherwise handled manually or in an ad hoc manner. Jira also incorporates elements from other applications such as Kanban but manages the workflow across these elements (Atlassian). Its name derives from the Japanese word for Godzilla “Which makes sense because it goes hand in hand with squashing software bugs!” (Jexo)

Most research on Jira and similar applications focus on improvements in productivity (Al-Baik & Miller, 2014; Tanner & Dauane, 2017; Özkan & Mishra, 2019; Fisher & Ludwigsen, 2013; Patterson 2022). Although some research has leveraged data drawn from the comments feature in Jira to analyze affect/sentiment amongst users (Valdez et. al., 2020; Ortu, et. al., 2015) or the degree to which new users accept the technology (Gorro et. al., 2019).

Still unexplored is an analysis of this new technology from a labor studies perspective. Labor studies, in general, shed light on the ways in which new technologies rearrange organizational structures (patterns on worker relationships) (Barley, 1996; Barley & Orr, 1997) as well as power dynamics across groups (Braverman, 1974; Bonjean & Grimes, 1970; Bovens & Zouridis, 2002; Burawoy, 1979; Burton & Van den Broek, 2009; Levina & Vaast, 2005; Rosen, 1984).

As Jira channels and redirects work flows in technical development settings, it has the potential to alter organizational structure and power in ways that could be meaningful in labor studies and management studies contexts.

METHOD

The author is a part-time engineer at a large defense contracting organization in New England. The organization is a professional bureaucracy with a matrix structure and has been migrating away from traditional system development life cycles toward rapid development methodologies such as Agile. The author was involved in a project for over a year before the Jira technology was introduced and has been involved with the Jira tool for over six months. This provided an empirical viewpoint in which data could be gathered prior to the introduction of the technology as well as after to support comparison.

The data gathered are qualitative (ethnographic) and are comprised of daily field-notes. Qualitative methodologies are applied to the data (coding) in order to find patterns and themes (Lofland & Lofland 1984; Spradley 1979; Strauss & Corbin 1990). The data were entered into a qualitative data anlaysis tool called Coding Analysis Toolkit (CAT).

ANALYSIS

The analysis is in its early stages, but some early themes are worth noting. Part of the Jira implementation involves a breaking down of a single task into multiple (ten) smaller tasks and arranging them in the order which they would be completed. These subtasks are then migrated within the tool across various states of being pending, actively being worked, completed and ready for review, blocked, etc.

Granularity of Task Definition

Prior to the introduction of Jira, tasks were defined less granularly. For example, the author's task involved the development of a hardware requirements specification (HRS) for a control equipment. Prior to Jira, the task was defined and status was reported at the level of the entire document. Therefore, one important theme is that the granularity of work definition increases, at least in this one task, by roughly a factor of ten.

Status Reporting

Prior to Jira, technical leadership requested task status on an ad hoc basis or during weekly status meetings if requested. Within the Jira process status is reported in shorter meetings three times per week. The technical lead shares the Jira dashboard and advances various subtasks to different statuses in real time. The technical lead is able to view all of the individual user's Jira elements whereas the individual users are only able to see their own when they are in the tool. This offers a privileged view of work tasks and status to the technical lead.

Furthermore, during these meetings each user has visibility into other workers' tasks at a level of depth that was not present in the status meetings prior to Jira introduction.

Jira also offers the technical lead to show task progress (credit) to his or her superiors more frequently.

Communication Channels

The Jira tool allows users to enter comments within a particular subtask and identify the other workers that the comment is intended for. When this comment is entered, an email is automatically generated alerting the target individual that a new comment exists and provides a hyperlink that takes the target user directly to that subtask comment in the Jira tool. Furthermore, when there is a change in subtask status, an email is generated informing the technical lead and user of the status change.

SUMMARY

This study is in its very early stages. However, the themes identified in the analysis are suggestive of general themes that need to be explored in more depth. From a labor studies perspective, we see a shift in control from the individual worker to the technical lead. The tasks are being managed at a more granular level of detail offering the superior more visibility into the tasks details and progress. Alternatively, however, through communication channels and more frequent and detailed sharing of status, the engineers have more visibility into each other's tasks which has the potential to enhance productivity as well as awareness (consciousness) of the overall system development. Furthermore, as these themes mature, they may have interesting implications for the philosophy of technology such as the way in which technologies affect worker phenomenology (Heidegger, 1977), system conception and development (Mitcham, 2022), ethics (Gogoll et. al., 2021), and power relations (Foucault, 1977).

REFERENCES

https://www.atlassian.com/agile/kanban

https://jexo.io/blog/atlassian-jira-history/

Al-Baik, O., & Miller, J. (2014). The kanban approach, between agility and leanness: a systematic review. Empirical Software Engineering, 20(6), 1861–1897. http://doi.org/10.1007/s10664-014-9340-x

Barley, S. R. (1996). Technicians in the Workplace: Ethnographic Evidence for Bringing Work into Organization Studies. *Administrative Science Quarterly,* 41: 404-441.

Barley, S. R. & Orr, J. E. (eds.) (1997). *Between Craft and Science: Technical Work in U.S. Settings.* ILR Press: Ithaca.

Braverman, H. (1974). *Labor and monopoly capital*. New York: Monthly Review Press.

Bonjean, C. M. & Grimes, M. D. (1970). Bureaucracy and alienation: a dimensional approach. *Social forces*. March, Vol. 48, Issue 3, pp. 365-373.

Bovens, M. & Zouridis, S. (2002). From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control. *Public administration review 62*(2), 174-184.

Burawoy, M. (1979). *Manufacturing consent.* Chicago: The University of Chicago Press.

Burton, J. & Van den Broek, D. (2009). Accountable and countable: Information management systems and the bureaucratization of social work. *British journal of social work 39*(7), 1326-1342

Fisher, J., Koning, D., & Ludwigsen, A. P. (2013). *Utilizing Atlassian JIRA for large-scale software development management* (No. LLNL-CONF-644176). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States).

Foucault, M. (1977). *Discipline & punish: the birth of the prison*. Vintage Books, New York.

Gogoll, J., Zuber, N., Kacianka, S., Greger, T., Pretschner, A., & Nida-Rümelin, J. (2021). Ethics in the software development process: from codes of conduct to ethical deliberation. *Philosophy & Technology*, 1-24.

Gorro, K., Ilano, A., Sebial, A., Ranolo, E., & Vale, E. (2019). Qualitative Technology Acceptance Evaluation of JIRA in Software Development Using Machine Learning.

Heidegger, M. (1977). The question concerning technology. *In the question concerning technology and other essays.* Harper & Row Publishers.

Ihde, D. (2010). *Heidegger's technologies: postphenomenological perspectives.* Fordham University Press, New York (2010).

Mitcham, C. (2022). *Thinking through technology: The path between engineering and philosophy*. University of Chicago Press.

Levina, N. & Vaast, E. (2005). The emergence of boundary spanning competence in practice: implications for implementation and use of information systems. *Management information systems quarterly* 335-363.

Lofland, J and Lofland L H (1984) Analyzing Social Settings. Wadsworth Inc.

Ortu, M., Adams, B., Destefanis, G., Tourani, P., Marchesi, M., & Tonelli, R. (2015, May). Are bullies more productive? Empirical study of affectiveness vs. issue fixing time. In *2015 IEEE/ACM 12th Working Conference on Mining Software Repositories* (pp. 303-313). IEEE.

Özkan, D., & Mishra, A. (2019). Agile Project Management Tools: A Brief Comprative View. *Cybernetics and Information Technologies*, *19*(4), 17-25.

Patterson, A. M. (2022). *Evaluation of Jira Software Adoption Strategies at a Large Technology Company*. Wilmington University (Delaware).

Rosen, M. (1984). Power and culture in bureaucracy: a study of bureaucracy as a control mechanism in monopoly capitalism. Ph.D. dissertation, University of Pennsylvania.

Strauss A & Corbin J (1990) Basics of Qualitative Research: Grounded Theory Procedures and Techniques. Sage Publications.

Tanner, M. and Dauane, M. (2017). The Use of Kanban to Alleviate Collaboration and Communication Challenges of Global Software Development, *Issues in Informing Science + Information Technology*, Vol. 14

Valdez, A., Oktaba, H., Gómez, H., & Vizcaíno, A. (2020, November). Sentiment analysis in jira software repositories. In *2020 8th International Conference in Software Engineering Research and Innovation (CONISOFT)* (pp. 254-259). IEEE.

THE CREATING HELPFUL INCENTIVES TO PRODUCE SEMICONDUCTORS AND SCIENCE ACT: IMPLICATIONS FOR CYBERSECURITY

Donna M. Schaeffer, Marymount University, Donna.schaeffer@marymount.edu
Alexis Grochmal, Marymount University, abg78170@marymount.edu
Henry J. Costa, Marymount University, h0c49936@marymount.edu
Patrick C. Olson, National University, polson@nu.edu

ABSTRACT

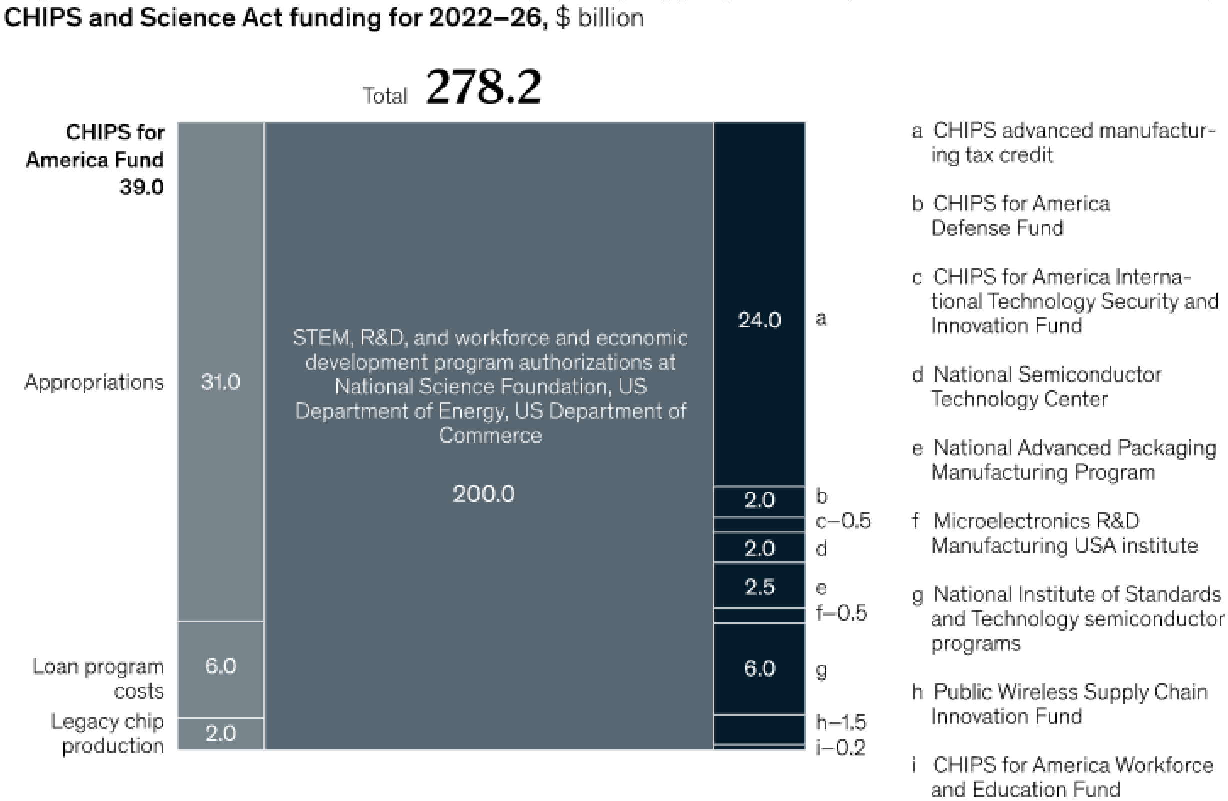
The enactment of the Creating Helpful Incentives to Produce Semiconductors and Science Act of 2022 (The CHIPS Act) holds the potential to yield significant benefits for the United States. This legislation aims to strengthen the country's economy, bolster national security, foster technological leadership, and enhance its citizens' overall quality of life. We aim to provide insights for stakeholders, such as semiconductor manufacturers, the shipping and transportation sector, educations, and national, state, and local governments. We focus on the cybersecurity aspects of the semiconductor industry. While the CHIPS and Science Act targets the United States, the global impacts of this legislation must be acknowledged and considered. This paper contributes to a more comprehensive understanding of the legislation's potential impact. In addition, it sets the stage for further research and analysis. It is important to note that implementing the CHIPS and Science Act is an ongoing process, and its full impact may take time to materialize. However, by proactively examining the implications for cybersecurity, we can pave the way for informed discussions, strategic planning, and effective utilization of the opportunities presented by this significant legislation.

Keywords: Cybersecurity, CHIPS and Science Act, Regulation, Policy, Semiconductor Industry, Taxonomy

INTRODUCTION

The Creating Helpful Incentives to Produce Semiconductors and Science Act (The CHIPS Act) was passed into United States' legislation on 09 August 2022. The bill comprises over 1000 pages and covers incentives for semiconductor producers, workforce development, especially in the areas of opportunity and inclusion, and innovation in supply chain and advanced manufacturing. Other titles in the bill prescribe allocations and responsibilities to the Department of Energy, the National Institute of Standards and Technology, the National Science Foundation, and the National Aeronautics and Space Administration. Figure 1 shows appropriations.

Figure 1. The CHIPS and Science Act Spending Appropriations (Source: Badlam, et al, 2022)



Miller (2018) highlights how the United States position in semiconductor production has drastically weakened. For example, the United Kingdom-based ARM controls market share in mobile, personal computing, and data center and Taiwanese manufacturers, spun off from the American—based Texas Instruments American prowess, have come to dominate the market.

The semiconductor industry operates within a complex global supply chain, and it is crucial to optimize the supply chain processes to ensure efficiency and maintain a stable and reliable flow of semiconductors, which is vital for our national security. However, the semiconductor supply chain remains fragile as the demand surpasses the available supply.

In September, the Department of Commerce initiated a Request for Information (RFI) on the semiconductor supply chain, shedding light on the intricacies of this global industry. The response was overwhelming, with more than 150 submissions, including major semiconductor producers and companies from various consuming industries. Key findings from the RFI include:

- Buyers reported a median demand for chips in 2021, up to 17% higher than in 2019. However, the supply they received did not increase proportionally, resulting in a significant supply and demand mismatch.
- The median inventory of semiconductor products reported by buyers has dramatically decreased from 40 days in 2019 to less than five days in 2021.These inventories are even smaller in critical industries.

- The RFI helped identify specific nodes within the supply chain where the supply and demand mismatch is most severe. Moving forward, collaborative efforts with the industry will focus on resolving bottlenecks in these nodes.
- The primary bottleneck across the board appears to be wafer production capacity, which requires a long-term solution.

The results of the RFI clearly emphasize the urgent need for increased semiconductor production in the United States. With increased production comes increased need for cybersecurity measures.

METHODOLOGY

Following the policy development taxonomy model presented by Schaeffer, Drake, and Olson (2021), we proceeded through four phases. First, we determined an appropriate scope for this research effort. In phase two, we collected data on current developments enabled by the CHIPS Act. In phase three, we constructed and verified the taxonomic model. The fourth phase is the maintenance of the model.

The appropriate scope was set to the legislation's Division A, the CHIPS Act of 2022, with supporting information from Title III of the Act, which focuses on STEM education, and Title V, with its attention to broadening participation in science.

Spiteri's (1998) model provided the basis for the taxonomy construction in phase two. We collected representative data across the scope, isolated concepts, determined facets, and classified elements across the facets. In this phase, we identified examples of the incentives offered to the United States-based chip manufacturers by the United States government. Incentives include direct loans and loan guarantees, cost offsets for upgrades and improvements to facilities and equipment, funding for research and development in supply chain innovation, funding for workforce development and education, and funding for efforts that recognize the synergy between chip manufacturing with national security.

Table 1. Examples of Current Implementations of the CHIPS Act Provisions

Direct loans, loan guarantees, and costs offset for investment in facilities and equipment: In anticipation of the financial benefits afforded by the CHIPS Act, several companies have announced plans to increase their manufacturing capacity through 2025.	Examples include (Hufbauer & Hogan, 2022): ● $12 billion Taiwan Semiconductor Manufacturing Corporation (TSMC) plant in Phoenix, AZ; ● a $20 billion Intel plant outside Columbus, OH; ● a $17 billion Samsung plant outside of Austin, TX; ● and a $30 billion Texas Instruments plant near Dallas, TX.
Supply chain innovation:	

In 2020, China and East Asia accounted for 75% of the world's have semiconductor manufacturing capacity; the US produced 12%, and Europe 9% (Enterprise, 2023). Experts agree that "Taiwan is . . . rapidly becoming one of the world's most dangerous geopolitical flash points (Peters, 2022). In their study of a global automotive component supplier, Simchi-Levi, Zhu, and Loy (2022)) found that "a short disruption of a semiconductor fabrication facility, or "fab," in Taiwan for ten days, could cause a flurry of additional disruptions across the entire supply chain that would last almost a year."	Kannan and Fieldgoise (2022) suggest that the CHIPS Act implementation strategic plan called for purchase agreements, in which manufacturers agree to buy components from designated suppliers at a fixed price for a future period.
Workforce development and education of $2.7 Billion in STEM education programs, including scholarships for services Requires a mentoring plan for Postdoctoral research supported by national grants Micro-electronic workforce development activities	Examples include: ● The STEM Learning Ecosystem Community of Practice, an initiative with more than 100 partners representing K12, higher education, business, and industry, funding organizations, and non-school STEM providers, has been tasked with scaling STEM education by establishing through new centers across the country (STEM Ecosystems, n.d.). ● S. 1257 Artificial Intelligence Scholarship for Service Bill. ● NSF grant applicants must document proposed mentoring activities, including career counseling, training in preparing grant applications, guidance on improving teaching skills, and training in research ethics (Bhatterjee, 2007). ● Intel expects to create 7,000 jobs as it opens fabrication labs across the country. Apx. 70% will require employees to have a two-year degree (Patel, 2023).

	• Samsung has implemented a program with a local community college for employees at its Austin, TX, facility. The company pays 100% of tuition and books for employees who work at least two days a week at Samsung and maintain a 3.0 GPA (Patel, 2023).
National security According to Peters (2022), "the CHIPS Act is also seen as highly significant for national security and future warfare including autonomous weapon systems, drone technology as well as cybersecurity."	• By the end of 2023, the White House Office of Science and Technology Policy must submit a quadrennial science and technology &T review that examines U.S. policy and makes policy and investment recommendations. The review's scope includes industrial innovation, science for social challenges, the STEM workforce, technology transfer, regional innovation, and U.S. research leadership (Hourihan, 2022). • Rebecca Spyke Keiser was appointed to the newly created position of chief of research security strategy and policy at the NSF (National Science Foundation, 2020). • In May 2023, the NSF requested information from the research community on developing a Research Security and Integrity Information Sharing Analysis Organization (Keiser, 2023). • In March 2022, the NSF established the Directorate for Technology, Innovation, and Partnerships to facilitate scaling critical research on emerging (American Institute of Physics, 2022). • The U.S. National Science Foundation announced a new $20 million investment in Entrepreneurial Fellowships through a multi-year

	cooperative agreement with Activate.org (NSF, 2022). ● Charles Barber fills the newly created position of Chief Diversity and Inclusion Officer at the NSF (NSF, 2022).

During phase three of the taxonomy model design, we identified several stakeholders of the CHIPS Act. The stakeholders are in six main groups: Technology, Facilities, Trade (Commerce), Government, Education, and Others (to hold those who do not fit or for future development). Each of these stakeholders has important cybersecurity implications. The CHIPS Act of 2022 is evolving; thus, we expect the taxonomy to change. Phase four, maintenance, is essential to the usefulness of the taxonomy.

RESULTS

The CHIPS Act is related to cybersecurity. The summary comments from the RFI and the implementations we identified fit the taxonomy. Figure 2 illustrates the taxonomy.

Figure 2. Taxonomy of The CHIPS Act of 2022 Stakeholders

Technology	Facilities	Trade	Government	Education	Others
Cybersecurity					

The cybersecurity vulnerabilities and risks related to technology include those in the areas of research and development and intellectual property, including patents, trademarks, and copyrights.

In terms of facilities, concerns stem from the shortage of skilled cybersecurity workers. This shortage is a factor for the education sector. For facilities, there are supply chain threats, which also concern the stakeholders involved in trade.

There are two major implications for the government sector. First, the CHIPS Act is tied to national security. Second, new directorates and positions have been established. Many policies have been created that cross traditional boundaries and require collaborative efforts.

DISCUSSION

The CHIPS Act of 2022 should incentivize investment in research and development. At present, the US dominates spending accounting for 28% of the world's research and development expenditures (Boroush and Guci, 2022). Research and development efforts in semiconductor chips is vital as they are components in many systems and items used every day, including electronics, automobiles, and defense systems.

Investments in manufacturing facilities help the construction and real estate industries. Building facilities creates construction jobs and improves infrastructure. For example, the Act calls for improvements and enhancements to wireless supply chain management software and systems. This will benefit industries in other sectors as the new standards roll out.

Stakeholders in the trade and commerce sector should notice a shift towards protectionism, as the Act prohibits funding recipients from expanding semiconductor manufacturing in China and countries defined by US law as posing a national security threat to the United States.

The Government sector has benefited from the CHIPS Act. Newly created positions and directorates are described in Table 1. Another example is an interagency working group that includes the Council on Environmental Quality, the Environmental Protection Agency, and the Department of Commerce for site selections and building codes and permissions.

Education will be impacted as proposals for forming a national network of training programs with a focus on minority-serving institutions and community colleges are being considered.

REFERENCES

American Institute of Physics. (2022, 17 March). NSF stands up as the directorate for Technology, Innovation, and Partnerships. https://ww2.aip.org/fyi/2022/nsf-stands-directorate-technology-innovation-and-partinternships

Artificial Intelligence Scholarship for Service Bill. 117th Cong. (2021). https://www.congress.gov/bill/117th-congress/senate-bill/1257

Athanaia, G. and Arcuri, G. (2022, 223 February). RAI Explainer: The Lifecycle of a Semiconductor Chip. Center for Strategic International Studies. https://www.csis.org/blogs/perspectives-innovation/rai-explainer-lifecycle-semiconductor-chip#:~:text=They%20are%20typically%20created%20by,elements%20to%20alter%20their%20conductivity.

Badlam, J., Clark, S., Gajendragadkar, S., Kumar, A., O’Rourke, S., Swartz, D., (Oct 2022). The CHIPS and Science Act: Here’s what’s in it. McKinsey & Company Report - Public Sector Practice.

Bhattacharjee, Y. (2007). NSF, NIH emphasize the importance of mentoring. *Science*, *317*(5841), 1016-1016.

Boroush, M. and Guci, L. (2022, 28 April). Research and Development: U.S. Trends and International Comparisons. https://ncses.nsf.gov/pubs/nsb20225/executive-summary

Enterprise, 02 March 2023. The US wants to reshape the global semiconductor industry in its favor. https://enterprise.press/stories/2023/03/02/the-us-wants-to-reshape-the-global-semiconductor-industry-in-its-favor-98495.

Hourihan, M. (2022, 09 August). Chips and Science Highlights: National Strategy. Federation of American Scientists. https://fas.org/publication/chips-national-strategy/

Hufbauer, G. C., & Hogan, M. (2022). CHIPS Act will spur US production but not foreclose China. *Peterson Institute for International Economics Policy Brief*, (22-13).

Kannan, V. & J. Feldgoise. (22 November 2022). After the CHIPS act: The limits of reshoring and next steps for US semiconductor policy. Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/11/22/after-chips-act-limits-of-reshoring-and-next-steps-for-u.s.-semiconductor-policy-pub-88439

Keiser, R.S. (2023, 04 May). Dear colleague, letter: This is a request for input on developing the U.S. research security and integrity information-sharing analysis organization. https://www.nsf.gov/pubs/2023/nsf23098/nsf23098.jsp?org=NSF

Miller, C. (2022). *Chip War: The Fight for the World's Most Critical Technology*. Simon and Schuster.

National Science Foundation. (2020, 02 March). NSF creates new research security chief position. https://new.nsf.gov/news/nsf-creates-new-research-security-chief-position.

National License Foundation. (2022, 19 September). NSF launches entrepreneurial fellowship for engineers and scientists. https://new.nsf.gov/tip/updates/nsf-launches-entrepreneurial-fellowship-engineers

National Science Foundation. (2022, 14 December). NSF appoints Charles 'Chuck' Barber as chief diversity and inclusion officer. https://new.nsf.gov/news/nsf-appoints-charles-chuck-barber-chief-diversity.

Patel, P. (2023). Building a US Semiconductor Workforce: CHIPS Act-Funded New Fabs are Spawning University Programs. *IEEE Spectrum*, *60*(6), 28-35.

Peters, M. A. (2022). Semiconductors, geopolitics, and technological rivalry: the US CHIPS & Science Act, 2022. *Educational Philosophy and Theory*, 1-5.

Schaeffer, D., Drake, S., & Olson, P. C. (2021, October). A Taxonomy of 5G Stakeholders. In *2021 IEEE 4th 5G World Forum (5GWF)* (pp. 358-361). IEEE.

Simchi-Levi, D., F. Zhu, and M. Loy. (2022) Fixing the U.S. semiconductor supply chain. *Harvard Business Review*, 25 October 2022. https://hbr.org/2022/10/fixing-the-u-s-semiconductor-supply-chain

Spiteri, L. (1998). A simplified model for facet analysis: Ranganathan 101. *Canadian journal of information and library science*, *23*(1-2), 1-30.

STEM Ecosystems Community of Practice. (n.d.). STEM learning ecosystems are recognized in a $52 billion plan to reinvigorate the economy. https://stemecosystems.org/press-release/recognized-in-52-billion-plan/

WHERE SHOULD CYBERSECURITY EDUCATION LIVE IN INSTITUTIONS OF HIGHER LEARNING?

Dr. Nita G. Brooks, Middle Tennessee State University, nita.brooks@mtsu.edu
Dr. Timothy H. Greer, Middle Tennessee State University, tim.greer@mtsu.edu

ABSTRACT

The importance of cybersecurity education is unquestionable today. There are a variety of opportunities available for obtaining the knowledge and skills required to perform cybersecurity-related tasks and functions within and across organizations. In recent years, these options have continued to expand and include offerings by professional organizations, technical schools, and institutions of higher learning. Within higher education, we have seen an expansion of programs at both the undergraduate and graduate levels offered through a variety of academic disciplines. The aim of this research is to explore what we currently know about the structure of cybersecurity programs and to highlight the benefits of using an interdisciplinary approach.

Data will be collected on existing programs at academic institutions in the United States. Both accredited and non-accredited programs will be examined to summarize the different approaches currently being utilized. There are various accreditation options that could impact academic programs and the direction of program development. Some are general and some are specific to the cybersecurity discipline (i.e., ABET). We will also incorporate data related to knowledge and skill expectations from entities offering certifications to programs such as the National Centers of Academic Excellence in Cybersecurity managed by the National Security Agency.

Additionally, we will examine research projects focused on cybersecurity curriculum and the workforce from different perspectives. What has been learned from these studies will also be used in framing our recommendations. We will include a few examples here as samples of the types of research we are exploring. In a recent study examining the process of a program seeking ABET accreditation specifically related to cybersecurity, Almuhaideb and Saeed, 2021 share their experiences and provide suggestions for programs seeking accreditation. Payne, et al. (2021) considered the inclusion of a cybersecurity course in general education programs in higher education, which could shape awareness of cybersecurity across the university curriculum. There are also important considerations that need to be included such as the skills requirements of different careers and paths in the cybersecurity workforce. Ramenzan (2023) recently published a study looking at the hiring requirements across cybersecurity positions and recommended that programs should "consider the diverse nature of the cybersecurity field" (p. 94).

Being able to position cybersecurity programs correctly and appropriately within higher education could help to facilitate an increase in students from diverse disciplines with an interest in joining the cybersecurity workforce and to broaden the impact of cybersecurity across organizations of all sizes. A goal is to provide recommendations and guidance for academic institutions to use in the design and implementation of these programs. We also aim to organize the various accreditation and certification requirements for undergraduate and graduate programs and to highlight consistencies and inconsistencies of expectations.

REFERENCES

Almuhaideb, A.M. & Saeed, S. (2021). A Process-Based Approach to ABET Accreditation: A Case Study of a Cybersecurity and Digital Forensics Program. *Journal of Information Systems Education, 32(2), p. 119-133.*

Payne, B.K., He, W., Wang, C., Wittkower, D.E., & Wu, H. (2021). Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course. *Journal of Information Systems Education, 32(2), p. 134-149.*

Ramezan, C.A. (2023). Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field. *Journal of Information Systems Education, 34(1), p. 94-105.*

RFID SECURITY AND PRIVACY RISKS IN HEALTHCARE APPLICATIONS: CHALLENGES, ADVANCES, AND PROSPECTS

Shilpa Balan, California State University, Los Angeles, sbalan@calstatela.edu
Cesar Rego, University of Mississippi, crego@bus.olemiss.edu

EXTENDED ABSTRACT

PURPOSE OF THE STUDY

Radio frequency identification (RFID) is mainstream technology in many industries such as manufacturing, transportation, logistics, supply chains, security and access control, agriculture, and healthcare, among many others. While RFID is widespread in applications where individual privacy is not compromised, adopting the technology in environments involving human identification and tracking is particularly challenging. The measures to assure appropriate levels of security and privacy depend on the application and operational environment. This research focuses on RFID-enabled systems in the healthcare sector. The benefits of RFID in healthcare are well-studied and demonstrated in many real-world implementations. RFID technology has proved critically helpful in reducing costs and improving operational efficiency in healthcare organizations. More importantly, RFID has played a critical role in significantly reducing medical errors which is the third leading cause of death in the U.S. after heart diseases and cancer (Makary & Daniel, 2016). However, these benefits do not come without challenges. On the one hand, known security vulnerabilities of current RFID technology pose a significant risk of unauthorized access to sensitive medical and patient data. On the other hand, using RFID technology in tracking and tracing individuals, especially healthcare providers (Winston, Paul & Iyer, 2016), raises significant ethical and privacy concerns. This research focuses on this less studied topic concerning potential threats and solutions to security and privacy obstacles in deploying RFID-enabled systems in healthcare organizations.

BASIS OF THE STUDY

We conducted a comprehensive literature review using content analysis and natural language processing technologies. We considered a set of relevant keywords related to RFID privacy and security to collect information from healthcare journals and news articles from 2000 to 2022. Sources of data collection include the International Journal of Healthcare Technology and Management, Hospital Topics, Decision Support Systems, Journal of Medical Systems, Journal of Healthcare Quality, American Journal of Business, Business Process Management Journal, IEEE, AMCIS Proceedings, International Journal of Medical Informatics, and European Journal of Information Systems. News articles originated from sources such as RFID Journal, MedCity News, Health Industry Business Communications, Healthcare Finance News and National Institutes of Health (NIH).

IMPLICATIONS

RFID technologies have proved very effective in healthcare and medicine, improving operational efficiency, asset management, and patient care. The benefits of tracking materials for logistics management are clear and do not appear to pose major threats. Nevertheless, to the extent that

RFID devices store and transmit sensitive patient data and can link to personally identifiable information, including tracking medical staff and patient location and movement in healthcare facilities and beyond, the adoption of RFID-enabled systems requires careful analysis to address security and privacy risks adequately. Because RFID systems must integrate with a backend database system (Hawrylak & Hale, 2015), security risks arise at two fundamental data communication and storage levels: tag security and server security. Large RFID infrastructures in healthcare are susceptible to various tag-related attacks, including physical tag cloning and spoofing, eavesdropping, replay, denial of service, and clandestine tracking (Gavoni, 2021). SQL injections and buffer overflow are the most common attacks on the server side (Zhang & Wang, 2009). Recent advances in tag hardware technologies, lightweight cryptographic algorithms, and intrusion detection systems afford potential opportunities for solutions. Other aspects facilitating technology adherence may involve design considerations, compliance with security standards, analysis of alternative technologies, establishing security and privacy controls, purpose of use transparency, ethical and legal considerations, security audits and accountability, technology awareness and training, and individual participation agreements. This study contributes to the technology issue of RFID-enabled systems by presenting a summary of current threats and emerging solutions highlighted in the literature.

CONCLUSION

RFID constitutes a significant advancement in healthcare supply chain management and medical practice. Essential functions of RFID in the healthcare setting entail inventory tracking and monitoring the location of patients, staff, and medical devices in real-time to improve operational efficiency and patient care quality. The main benefits include improvements in patient safety, cost and time savings, access control and security, drug compliance, and reduction of medical errors. Despite these important advances, security against unauthorized access to data and privacy breaches remains the most critical barrier when considering the adoption of RFID technology in healthcare.

REFERENCES

Gavoni, L. (2021). RFID Exploitation and Countermeasures. arXiv preprint arXiv:2110.00094.

Hawrylak, P. J., & Hale, J. (2015). Data privacy issues with RFID in healthcare. Medical Data Privacy Handbook, 549-567.

Makary, M. A., & Daniel, M. (2016). Medical error—the third leading cause of death in the US. BMJ, 353.

Winston, T. G., Paul, S., & Iyer, L. (2016, January). A study of privacy and security concerns on doctors' and nurses' behavioral intentions to use RFID in hospitals. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 3115-3123). IEEE.

Zhang, Q., & Wang, X. (2009, January). SQL injections through back-end of RFID system. In 2009 International symposium on computer network and multimedia technology (pp. 1-4). IEEE.

CHATGPT OR CHEATGPT: HOW ARE EDUCATORS DEALING WITH CHEATING IN THE AGE OF AI TOOLS?

Philip Kim, Walsh University, pkim@walsh.edu
Austin Fantin, Walsh University, afantin1@walsh.edu
Jennifer Breese, Penn State University, jzb545@psu.edu
Justin Woods, Walsh University, jwoods@walsh.edu

INTRODUCTION

The use of ChatGPT and other generative AI has grown exponentially. ChatGPT reached over 100 million active users in just two months after its launch in November 2022 (Tung, 2023). Since its ubiquitous adoption and fast-rising popularity, the possible benefits in industry are appealing. The potential applications may result in new developments including improved customer experience, increased efficiencies, cost reductions, and effective knowledge management (Emerline, 2023). The uses can be across various industries as well including healthcare, manufacturing, retail Government, etc. (Asch, 2023; Pocock, 2023). Within education many students and faculty are still trying to grasp what AI is. How can this technology impact the educational experience, and should they be utilized in the classroom? The one thing educators cannot do is ignore it.

RESEARCH DESIGN

The research will be a mixed methodology approach. We will interview educators within higher ed, across disciplines, majors, and programs. We will also collect survey data to determine to what extent faculty are currently using generative AI in their courses. We want to explore how teachers are monitoring the use of AI in the classroom. Specifically, how faculty are addressing the ethical issues of student integrity, plagiarism, and cheating on assignments, quizzes, and exams using ChatGPT or other AI tools. And then finally, what tools are being used to detect student cheating.

PILOT STUDY

As an initial trial, we entered the following prompt into ChatGPT:
“best tools to detect students cheating using AI tools”

The response was as follows:
“Detecting students cheating when using AI tools can be challenging, as these tools can provide sophisticated ways to evade detection. However, several techniques and tools can aid in identifying potential instances of cheating. Here are some commonly used methods:

1. Plagiarism Detection Software: Plagiarism detection tools like Turnitin, Grammarly, or Copyscape can help identify copied content by comparing students' work against a vast database of sources, including internet pages, academic papers, and previously submitted documents.
2. Forensic Analysis of Text: Educators can analyze students' written work for inconsistencies in writing style, vocabulary, or grammar that may indicate the use of AI-generated content. Manual examination can be time-consuming but can provide valuable insights.

3. Comparative Analysis: Comparing the answers of different students or the same student across multiple assignments or exams can reveal patterns of similarity that may indicate collusion or cheating.
4. Monitoring Software: Remote proctoring tools such as ProctorU, Proctorio, or Respondus Monitor use webcam and microphone monitoring, screen recording, and eye-tracking technologies to detect suspicious behavior during online exams, such as looking at unauthorized materials or multiple faces in the camera.
5. Statistical Analysis: Analyzing patterns of response length, word choice, or answer similarity across a group of students can help identify outliers or suspicious behavior that may warrant further investigation.
6. Custom AI Models: Institutions can develop their own AI models specifically trained to detect AI-generated or plagiarized content. These models can be trained on data from previous cheating incidents to improve detection accuracy.
7. Peer Review: Incorporating peer assessment or group discussions can help uncover inconsistencies in students' knowledge and understanding when compared to their peers, potentially indicating cheating.

It's important to note that while these tools and techniques can assist in detecting cheating, they should not be relied upon solely. Human judgment and careful consideration of evidence are crucial in making accurate determinations. Education institutions should establish clear policies and guidelines regarding cheating and plagiarism and communicate them to students to maintain academic integrity."

We then copied the entire ChatGPT response and pasted the text into three different AI detection software programs. The table (Table 1) below shows the site that was used and the result of the AI text analysis.

Table 1

AI Detection Tool:	**Result:**	**Notes:**	**Conclusion:**
GPT-2 - Output Detector	99.97% Real .003% Fake	Prediction based on 409 tokens. According to GPT-2, the results get more reliable at any result above 50 tokens.	False Negative
GPTZero	Perplexity Score: 53.467 Burstiness Score: 16.574	Higher Perplexity (above 75) and higher Burstiness (above 50) would suggest a variation in perplexity and randomness in the text. Most AI generated text scores higher in both perplexity and burstiness.	False Negative
OpenAI - AI Text Classifier	"The classifier **considers the text**	OpenAI is the same organization that created ChatGPT. They have also	Unclear

	to be unclear if it is AI-generated”	created a tool to detect the use of its AI tool.	

IMPLICATIONS

The implications for use of AI in education are significant. As AI tools become more readily available, there will be an increase in AI-embeded platforms (Lawton, 2023). This will change the way many educators construct their curricula. Faculty may have to shift their assessment tools to better account for the AI tools that are being used. There may require faculty to adjust from a theoretical framework of education to a more applied framework. Another adjustment may be employing a problem-based learning approach.

By the time this research is presented, there may be new and unforeseen developments in the generative AI space, so the discussion amongst educators must be proactive. We should continue to share best practice and experiential knowledge. The AI tools are advancing and thus our methods to teach, instruct, and assess our students must advance as well.

REFERENCES

Asch. D. A. (2023). An Interview with ChatGPT About Health Care. NEJM Catalyst Innovations in Care Delivery. https://catalyst.nejm.org/doi/full/10.1056/CAT.23.0043.

Emerline Team. (2023). How Chat GPT Can Benefit Your Business, and When It Puts It at Risk. Emerline.com. https://emerline.com/blog/chat-gpt-in-business.

Lawton, G. (2023). What is generative AI? Everything you need to know. TechTarget. https://www.techtarget.com/searchenterpriseai/definition/generative-AI.

Pocock, K. (2023). What is ChatGPT and what is it used for? PC Guide. https://www.pcguide.com/apps/what-is-chat-gpt/

Tung, L. (2023). ChatGPT just became the fastest-growing app of all time. ZDNet. https://www.zdnet.com/article/chatgpt-just-became-the-fastest-growing-app-of-all-time/

A REFERENCE ARCHITECTURE FOR DISTRIBUTED FEDERATED COLLABORATION SECURED SERVICES (DFCS-RA)

Ruti Gafni, The Academic College of Tel Aviv Yaffo, rutigafn@mta.ac.il
Itzhak Aviv, The Academic College of Tel Aviv Yaffo, itzhakav@mta.ac.il
Dror Haim, Teionet, dror.haim@gmail.com

ABSTRACT

Distributed Federated Collaboration Secured Services is a proposed novel secure distributed Unified Communication and Collaboration (UCC) reference architecture (DFCS-RA) planned for filling the existing gap to support multi-environment ecosystems (including hybrid cloud, edge computing for IoT and real-time usages, and portable scenarios). DFCS-RA encourages new businesses and models, connecting people, "things," and processes in secured and sensitive workloads, supporting efficient, and cost-effective enhancements to traditional UCC (mostly centralized/monolithic services), tailored for different vertical markets having varying requirements. It provides a novel secure multi-environment communication and collaboration technology and services between large numbers of players. Key security concepts developed are secure separation, federation, and collaboration, ensuring modularity, flexibility, homogeneity, function consolidation, and security by design for all the UCC services. The cryptographic architecture extends the Signal messenger security and encryption architecture. DFCS-RA comprises a toolbox for security modeling, a set of security design principles, and a set of security functions and mechanisms to implement controls to achieve stated security objectives. It was tested in diverse use cases; and found suitable, secure, and reliable. DFCS-RA is compliant with the new EW regulation, gathering and exchanging just the minimal personal data of end users as necessary for interoperability. DFCS-RA can be used by both researchers and practitioners investigating distributed collaboration solutions.

Keywords: Signal, Secured Unified Communication and Collaboration, Distributed UCC, Hybrid Collaboration

EFFORTLESSLY CREATE ANALYTICS ASSESSMENTS WITH CHATGPT

Ellen Gordon, Ohio University, GordonE@ohio.edu
Janna Chimeli, Ohio University, ChimeliJ@ohio.edu
Lauren Kenyo, Ohio University, Kenyo@ohio.edu
Raymond Frost, Ohio University, FrostR@ohio.edu

It is undeniable that ChatGPT has major implications for the future of education (Heaven, 2023, Kissinger, Schmidt, & Huttenlocker, 2023). While some articles have acknowledged the ways in which ChatGPT can facilitate learning (Heaven, 2023; Roose, 2023), ChatGPT has primarily made headlines as a tool that students are using to cheat (Cotton et al., 2023, Shrivastava, 2022). ChatGPT has implications for the educator as well as the learner. This paper will focus on how ChatGPT can serve as an invaluable resource to instructors and can help quickly develop high-quality assessments that align with one's learning objectives. We believe that continuously producing novel assessments, particularly novel proctored exams, can help alleviate many instructors' cheating concerns. The primary focus is on analytics assessments; however, many of our recommendations are transferable and can encourage instructors in other disciplines to use ChatGPT as a resource.

THE PROBLEM: TECHNOLOGY & ACADEMIC MISCONDUCT

Advancements in technology have increased the opportunity and ease with which students are able to effectively cheat. With a quick Google search, students can often access the questions and answers from a textbook's test bank. Social media, group chats, and even certain websites (e.g., Course Hero) enable students to easily share and access past exams and other course assessments.

It is best practice for instructors to create new assessments, especially exams, each semester as an effort to combat cheating. Instructors who teach multiple sections of the same course or have large class sizes are encouraged to create multiple versions of an exam. Creating new assessments is time consuming and tedious. Creating new assessments that are relevant and interesting to students and align with the course's learning objectives takes even more time and requires substantial effort, resources, and creativity. It can be difficult to sustain motivation when one knows that they will have to reinvent the wheel and create a new exam the following semester. Furthermore, research and service obligations can make it challenging, or sometimes impossible, to create new, high-quality assessments semester after semester. However, given that course materials can be easily distributed and shared online, we believe it is more important than ever that instructors refrain from recycling certain high-stakes assessments.

FROM AI TO TA: HOW CHATGPT CAN QUICKLY DEVELOP ASSESSMENTS

ChatGPT is a great resource for generating problem sets for most content that is covered in any introductory business analytics or statistics course. The system enables instructors to easily create new assessments, or multiple versions of an assessment, each semester in a fraction of the time required previously.

The key to using ChatGPT successfully is to understand how to create prompts. In fact, prompt engineering has become a field of study. Through trial and error, we have developed seven guidelines or best practices on how to write prompts to develop analytics problems at the undergraduate level. Our presentation will elaborate on these seven guidelines and provide example prompts and output from ChatGPT. We have found that the problems we developed using ChatGPT are indistinguishable, in terms of quality, from both textbook and self-authored problems.

CONCLUSION

Assessment plays a crucial role in higher education by evaluating student learning and progress across various learning outcomes. The accessibility of online solutions necessitates frequent re-creation of assessments and the availability of multiple versions, creating a conflict with the limited time and creativity of faculty members in assessment design. The creation of assessments using ChatGPT not only supports student learning but also aids in preventing cheating.

REFERENCES

Cotton, D. R., Cotton, P. A., & Shipway, J. R. (2023). Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. *Innovations in Education and Teaching International*, 1-12.

Elkins, Katherine, and Jon Chun. 2020. "Can GPT-3 Pass a Writer's Turing Test?" *Journal of Cultural Analytics* 5 (2). https://doi.org/10.22148/001c.17212.

Heaven, W. D. (2023, April 6). ChatGPT is going to change education, not destroy it. *MIT Technology Review*. https://www.technologyreview.com/2023/04/06/1071059/chatgpt-change-not-destroy-education-openai/

Kissinger, H.A, Schmid, E., & Huttenlocher, D. (February 24, 2023). ChatGPT Heralds an Intellectual Revolution.' *Wall Street Journal*. https://www.wsj.com/articles/chatgpt-heralds-an-intellectual-revolution-enlightenment-artificial-intelligence-homo-technicus-technology-cognition-morality-philosophy-774331c6

Roose, K. (2023, January 12). Don't Ban ChatGPT in Schools. Teach with It. *New York Times*. https://www.nytimes.com/2023/01/12/technology/chatgpt-schools-teachers.html

Shrivastava, R. (December 12, 2022). Teachers Fear ChatGPT Will Make Cheating Easier Than Ever. *Forbes*. https://www.forbes.com/sites/rashishrivastava/2022/12/12/teachers-fear-chatgpt-will-make-cheating-easier-than-ever/?sh=5bebd45c1eef

USING PEER EXEMPLARS AS A SMALL TEACHING STRATEGY IN AN SQL EXPLORATORY ACTIVITY

Robert J. Mills, Utah State University, bob.mills@usu.edu
Emily R. Fyfe, Indiana University, efyfe@indiana.edu
Tanya Beaulieu, University of Maine, tanya.beaulieu@maine.edu
Maddy Mills, Utah State University, maddyymills@gmail.com
Hannah Davies, Utah State University, hannahjdavies5@gmail.com

EXTENDED ABSTRACT

Faculty members specializing in data analytics and information systems face the challenging task of keeping up with rapid technological advancements, leaving them with limited time to extensively revise their teaching methods (Jiang, 2022). The concept of small teaching offers a solution by proposing small yet powerful modifications to course design and teaching practices, aiming to bring about positive change in higher education (Lang, 2021).

In this conference presentation, we introduce an IS-related small teaching strategy designed to communicate teacher expectations by showcasing various examples of SQL coding efforts from student peers. In traditional education, learning is often considered a one-way process, where instructors possess and transmit the necessary knowledge for academic success. However, incorporating instructional strategies that allow students to learn from each other can also be highly beneficial (e.g., Aksop & O'zdemir, 2022; Merrill & Gilbert, 2008).

As part of this research, we empirically examine the effectiveness of our small teaching strategy by conducting an experiment with three randomly assigned groups, including a control group (no peer examples), as well as variations in the complexity of peer examples (basic versus advanced) used in an exploratory SQL coding activity to assess student performance in coding complexity.

For the empirical component of our research, we have included approximately 130 undergraduate students from a large Western university who are currently enrolled in an advanced database management/SQL course (data analysis ongoing). The experiment follows a randomized between-subject design.

Each participating student has been randomly assigned to one of three groups: basic peer examples (n = 45), advanced peer examples (n = 46), or the control group with no peer examples (n = ~40). In the presentation, we will provide detailed information about the materials, procedures, peer examples (basic and advanced), and research study activities.

We hypothesize that the complexity of students' coding work will be higher among those exposed to peer examples (basic or advanced) compared to the control group. Furthermore, we expect that students in the advanced peer examples group will outperform those exposed to basic peer examples. While we are still coding and analyzing data for the control group (no examples), our

initial tests have revealed a significant difference in code complexity, with students in the advanced example condition producing more complex code (t(89) = 2.996, p = .004).

We are excited to share the process of designing and developing small teaching strategies based on Lang's framework (Darby, 2019; Lang, 2021) with participants of the IACIS conference who are interested in making their own course improvements rooted in cognitive theory. Additionally, we look forward to presenting our empirical findings on the implementation of the small teaching strategies we have developed, which involve the use of peer examples to convey teacher expectations in an exploratory SQL coding activity.

REFERENCES

Aksop, A., C., & O'zdemir, D. (2022). Classroom teachers' opinions about peer learning and characteristics of qualified teachers. *Educational Research Quarterly*, *45*(4), 46-78.

Darby, F. (2019). *Small teaching online: Applying learning science in online classes*. Jossey-Bass.

Jiang, Y. (2022). Apply small teaching tactics in an introductory programming course: Impact on learning performance. *Journal of Information Systems Education*, *32*(2), 149-158.

Lang, J. M. (2021). *Small teaching: Everyday lessons from the science of learning* (2nd ed.). Jossey-Bass.

Merrill, M. D., & Gilbert, C. G. (2008). Effective peer interaction in a problem-centered instructional strategy. *Distance Education*, *29*(2), 199-207.

IMPACT OF SECURITY EDUCATION, TRAINING, AND AWARENESS ON PERCEIVED SECURITY AND TRUST

Abdou Illia, Eastern Illinois University, aillia@eiu.edu
Assion Lawson-Body, University of North Dakota, assion.lawsonbody@und.edu

ABSTRACT

It is common knowledge that security training and security education would raise information systems users' awareness of cybersecurity threats. This study explores the extent to which security education and security training (a) raise the level of cybersecurity threats' awareness and (b) have a direct impact on people's perceived sense of security and trust when conducting business online. Before and After survey data were collected from students enrolled in cybersecurity workshops and in formal education courses. In this presentation, we aim to present: 1) the research model developed based on the existing literature, 2) the methodology used for collecting and analyzing the survey data, and 3) the preliminary results. We will conclude by discussing the study's implications and some future directions for research.

Keywords: Security education, security training, security awareness, perceived security, trust

REFERENCES

NIST (2014). SP 800-16 Revision (3rd Draft). A Role-Based Model for Federal Information Technology/Cybersecurity Training. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/draft

Torten, R., Reaiche, C. & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. Computers & Security, Vol. 79, 68-79

WOMEN IN ANALYTICS: EXPLORING A POTENTIAL PATH TO INCREASE FEMALE PARTICIPATION IN COMPUTING CAREERS

Alana Platt, University of Wisconsin–Whitewater, platta@uww.edu
Amir Fard Bahreini, University of Wisconsin–Whitewater, fardbaha@uww.edu
Choton Basu, University of Wisconsin–Whitewater, basuc@uww.edu

ABSTRACT

The underrepresentation of women in computing has long been recognized as a problem. Despite many resources being applied to this issue, the representation of women in computing in the United States has been on the decline for the past four decades. In this work, we explore gender and negative stereotypes about data analytics, an application area of computer work that possesses a number of features that previous research identified as being more attractive to women. We conducted a survey of students at the University of Wisconsin-Whitewater comparing their impressions of computing and analytics professionals, and we found that they held fewer negative and gender stereotypes about analytics professionals than computing professionals. We suggest possible changes that could be incorporated into curriculum and future areas of research to bolster female students' interest in computing careers.

Keywords: women in computing, women in analytics, technology careers, broadening participation in computing

INTRODUCTION

The underrepresentation of women in technology has been recognized for the past few decades. This phenomenon has been the focus of many industry, non-profit, and academic efforts to reverse this trend. Despite these initiatives, the gap stubbornly persists. In 2019, only 21% of CS undergraduate degrees earned in the US were awarded to women (NCWIT, 2020). Research indicates that this disparity is likely due to stereotypes around computing careers and who is likely to be a computing professional. Women often encounter stereotypes that erode their sense of efficacy in computing professions (Cheryan et al., 2009). Furthermore, other research suggests that women lack a sense of belonging, which may explain why some women opt out of the field (Sax et al., 2018). A study by Diekman et al. (2010) found that STEM careers are perceived as inhibiting communal goals (e.g. working with or helping other people). According to Martell, Lane, & Emrich (1996), even small effects of communal motivation could lead to women opting out of STEM careers, especially if such small effects accumulated over time.

A variety of interventions have been deployed in an effort to combat these issues. In addition to industry diversity initiatives, academics have researched the impact of summer camps (Webb and Ronson, 2011; Outlay et al., 2017) and classroom factors (Sax et al., 2018). Other works suggest that a shift in the way we think about computer careers may have a positive impact on this issue. For example, much of the research in this area focuses on students in America or other western societies. However, research on societies across the globe suggest that this phenomenon is not universal (Adya and Kaiser, 2005; Mellström, 2009; Sien et al., 2014). Further, other researchers have suggested that a shift in what we consider to be computer work or computer workers may provide a fuller picture of what it means to work in computing (Vitores & Gil-Juárez, 2016).

In this paper, we take a broader view of computer work by focusing on data analytics. Although analytics is a technical discipline, its focus on interdisciplinary applications and emphasis on the effective communication of discovered knowledge differentiates it from other technical areas of study, such as computer science. Thus, analytics content may be a way to encourage more female representation in computing careers overall by providing a more attractive introduction. Further, there tends to be overlap in curriculum between analytics and other computing professions, such as Information Technology or Computer Science. Greater female interest in analytics could have a positive impact on their perception of those related majors. We administered a survey on gender and negative stereotypes to students enrolled in data analytics courses at a the University of Wisconsin-Whitewater to explore how data analytics is perceived as opposed to more traditional computer professions.

LITERATURE REVIEW

The gender disparity in computing and technology is well known and well-studied. Despite the attention of industry, governments, non-profits, and academics, the gender gap stubbornly persists. Female representation in computer science peaked in 1980 with women representing 44% of degree earners, but has been on the decline for most of the past four decades (Sax et al., 2017). In 2015, a study found that only 1.7% of female freshman respondents intended to major in Computer Science, as opposed to 6.3% of their male peers (Egan, 2015). Further, in 2019, only 21% of those awarded CS undergraduate degrees were women (NCWIT, 2020).

Gender roles and Societal Influence

Gender roles and societal influence are frequently identified as contributing factors the dearth of women in computing (Huffman et al., 2013). Young girls often adopt the belief that tech careers are “men’s work” early in their education (Ramsey and McCorduck, 2005), and this attitude can present a significant barrier to women pursuing the profession (Bock et al., 2013). Further, the image of the IT profession as being boring, nerdy, and socially isolated elevates the challenge even further (ACM, 2009). A 2009 study of college-bound girls and boys showed that slightly more than a third of girls (35%) rated IT as a good major or a very good major. The same study reported that 74% of boys rated IT as a good major or a very good major (ACM, 2009). According to a study by Buzzetto-More (2010), many women students reported that they had not studied computers or programming in high school or were exposed to IT careers. In addition, many of them were discouraged from pursuing an IT-related career. A study by Master et. al. (2015) reported that girls exposed to classes that did not perpetuate negative stereotypes of IT had significantly more interest in enrolling in computer courses (Master et. al., 2015). The result of persistent negative perceptions is a shortage of women in IT majors in college and in IT careers.

Some prior works investigate the differences in societal factors on career choice among different cultures. Hill et al. 2010 found that cultural factors in the U.S. negatively impact how girls perceive their abilities in math, science, and engineering. Gender bias in IT careers is also prevalent in countries other than the US. A study by Vekiri and Chornaki (2008) reports that Greek boys perceived more support for their interests in use of computers than their female counterparts.

Furthermore, parental encouragement and expectations were strong predictors of self-efficacy. In Brazil, the gender gap continues to widen, and women view computer science as a field that is dominated by men (Holanda et al., 2020). Contrarily, in some countries the situation is quite the opposite (Adya and Kaiser, 2005; Mellstrom, 2009). For example, Malaysian girls tended to have positive attitudes towards technology related careers (Sien et.al, 2014). In India, the beliefs about women's incompetency in mathematics or notions of differences in intrinsic intellectual ability do not seem to occur in socio-cultural context (Mukhopadhyay, 2009). Gender does not play any role in acquiring mathematical and problem-solving skills for education in computer-related fields (Varma, 2011). Still, there are less women than men in doctoral education in STEM fields.

"Leaky Pipeline" and Interventions

Many prior works focus on the "leaky pipeline" of women in computing and interventions to retain women throughout their academic careers. However, Vitores & Gil Gil-Juárez (2016) assert that researchers ought to look at the problem more broadly. Specifically, they suggest researchers focus on highlighting a variety of additional research landscapes, including broadening the definition of computing work to include interdisciplinary or intersectional domains. Other works focusing on the leaky pipeline have also found evidence to support the importance of looking at more interdisciplinary computing work. Outlay et al. (2017) found that middle school girls had a greater interest in interdisciplinary computing work (e.g. creating and editing digital videos and music, computer graphics and media) than pure computing (e.g. computer science, computer programming). Kahn & Luxton-Reilly (2016) posit that much of the way computer science is stereotyped (e.g. a male-oriented discipline with little social interaction) alienates females students, and argues that computing courses should incorporate socially relevant examples and exercises to combat this. Further, Margolis and Fisher (2002) found that even women interested in computer science find it more meaningful if the domain is interdisciplinary.

Importance of Human Interaction

The perception that computing careers are more technical rather than people-oriented impacts recruitment efforts. Papastergiou (2008) found that many students chose not to study computer science because they preferred more human interaction. They found that this view is pronounced among female students, with male students more likely to view computer science as human oriented than female students. It may be that this influences female students to select majors with a greater perceived social impact (Buckley, 2009).

In this study, we build on these prior works by investigating attitudes towards an interdisciplinary technology field: data analytics. Data analytics incorporates elements of traditional computing disciplines (e.g. computer programming, databases, artificial intelligence) with technical communication (e.g. storytelling, visualizations) and apply these techniques to a variety of domains. Data science and data analytics are related; however, data science is differentiated by a greater focus on the technical aspects. Similar to other computing domains, data science suffers from a gender imbalance, with women represented only 15-22% of data scientists (Duranton et al., 2020). However, by focusing on a domain such as data analytics that has many socially oriented and interdisciplinary aspects, it may be a fruitful avenue to attract greater female representation.

METHODOLOGY

In this study, we evaluated the differences in negative and gender stereotypes of those in computing careers and analytics careers. In this section, we will discuss our Instrument/Survey, Subjects and Procedure, and Data Analysis.

Instrument/Survey

To gather our data, we distributed an anonymous survey to students enrolled in analytics courses. The surveys consisted of demographic questions, as well as questions we adapted from prior studies designed to measure stereotypes of computer workers (Web and Rosson, 2011; Outlay et al., 2017). These consisted of 7-point Likert type questions (Table 1) where respondents could indicate the degree to which they agreed or disagreed with common negative and gender stereotypes of computer workers. The same questions were then adapted to refer to analytics workers. We obtained IRB approval prior to conducting our survey.

Research question 1: Are negative stereotypes about analytics professionals as prevalent as those about computing professionals?

Research question 2: Are gender stereotypes about analytics professionals as prevalent as those about computing professionals?

Subjects and Procedure

We used a convenience sample of students (N=70) enrolled in at least one data analytics course at the University of Wisconsin-Whitewater. Of those respondents, 16 were undergraduates and 54 were graduate students. Respondents were 52.86% male, 42.86% female, and 2.86% declined to specify a gender, while 75.71% identified as White/non-Hispanic, 12.86% Hispanic, 5.71% Asian or Pacific Islander, 2.86% black/non-Hispanic, and 1.42% other. A minority of our respondents identified as first-generation college students (25.71%).

To gather our data, we distributed an anonymous survey to students enrolled in an undergraduate and a graduate analytics course. Students were invited to complete the survey and were awarded a small amount of extra credit for their participation. The survey was open for several days, and students were allowed to take it at a time and location of their choosing.

Data Analysis

After the survey period ended, results were compiled and analyzed. Our instrument exhibited a good level of reliability, with a Cronbach's Alpha of .8290. As we wanted to compare particular negative and stereotypes about computing professionals as opposed to analytics professionals, we compared responses for each category both for the entire cohort as well as the responses broken out by gender. Statistical significance was established using a t-test.

RESULTS

In this section, we present our results followed by our findings for each of our research questions. Table 1 shows the aggregate responses to the survey, with 1 being strong agreement with the statements and 7 being strong disagreement. A number of statistically significant differences were found between how respondents viewed computing professionals and analytics professionals.

We found that respondents were more likely to disagree with negative stereotypes about computer professionals as opposed to analytics professionals. Respondents disagreed more strongly that analytics professionals are technology geeks (computing professionals: 4.51; analytics professionals: 5.17) and they were less likely to think about computer geeks when thinking about analytics professionals (computing professionals: 4.96; analytics professionals: 5.55). Respondents also felt that the analytics profession was less dominated by men (computing professionals: 4.33; analytics professionals: 5.06), and disagreed more strongly that men were more likely to pursue analytics professions than women (computing professionals: 5.32; analytics professionals: 5.64). This suggests that the answer to our second research question is that gender stereotypes about analytics professionals are less prevalent than those about computing professionals.

Table 1: Results of survey on negative stereotypes and gender stereotypes, with 1: Strongly agree to 7: Strongly Disagree (* p<=0.05; ** p<=0.01)

	Computing	Analytics	Diff.
[Computing | Analytics] professionals tend to be nerds.	5.30	5.17	0.13
[Computing | Analytics] professionals tend to be technology geeks.	4.51	5.17	-0.67**
When I think about [computer | analytics] professionals, I think about computer geeks.	4.96	5.55	-0.59**
The [computer | analytics] profession is dominated by men.	4.33	5.06	-0.72**
Men, rather than women, typically pursue careers in [computers | analytics].	5.32	5.64	-0.32*
[Computer | Analytics] professionals tend to be intelligent.	3.29	3.39	-0.10
[Computer | Analytics] professionals tend to have good problem-solving skills.	3.29	3.35	-0.06
[Computer | Analytics] professionals tend to be willing to keep up with technology.	3.42	3.70	-0.28*
[Computer | Analytics] professionals tend to have good managerial skills	4.99	4.41	0.58**
[Computer | Analytics] professionals tend to have good communication skills.	5.14	4.28	0.87**
[Computer | Analytics] professionals tend to have good people skills.	4.97	4.54	0.43*
[Computer | Analytics] professionals do a lot of programming.	4.22	4.61	-0.39**
[Computer | Analytics] professionals tend to have a strong background in math and science.	4.48	4.14	0.33*

Respondents also indicated that certain people oriented soft-skills were more important for analytics professionals than for computer professionals. Respondents felt analytics professionals were more likely to have strong managerial skills (computing professionals: 4.99; analytics professionals: 4.41). Interestingly, there was no significant difference between perceptions in certain positive stereotypes, specifically high intelligence and strong problem-solving skills. This lends support for our first research question in that there are fewer negative stereotypes about analytics professionals being more technology than people oriented.

We then analyzed our respondents results by gender, as shown in Table 2. While many of the items did not have significant differences in how stereotypes were perceived, some did. Men disagreed more strongly with the negative stereotypes associating analytics professionals with computer geeks and the profession as being dominated by men. Women disagreed more with analytics professionals needing to keep up with technology and having to do a lot of programming. Women agreed more strongly than men that analytics professionals need strong people skills.

Table 2: Differences in perceived negative stereotypes and gender stereotypes by gender (* p<=0.05; ** p<=0.01)

Responses for men	Computing	Analytics	Diff.
When I think about [computer | analytics] professionals, I think about computer geeks.	4.78	4.59	-0.79**
The [computer | analytics] profession is dominated by men.	4.24	5.14	-0.89**
[Computer | Analytics] professionals tend to be willing to keep up with technology.	3.51	3.54	-0.03
[Computer | Analytics] professionals tend to have good people skills.	4.62	4.27	0.35
[Computer | Analytics] professionals do a lot of programming.	4.08	4.35	-0.27
Responses for women	Computing	Analytics	Diff.
When I think about [computer | analytics] professionals, I think about computer geeks.	5.20	5.63	-0.43**
The [computer | analytics] profession is dominated by men.	4.40	4.90	-0.50*
[Computer | Analytics] professionals tend to be willing to keep up with technology.	3.33	3.90	-0.57**
[Computer | Analytics] professionals tend to have good people skills.	5.37	4.77	0.60**
[Computer | Analytics] professionals do a lot of programming.	4.43	4.97	-0.53**

DISCUSSION

In this paper, we conducted a survey of analytics students to investigate the prevalence of negative and gender stereotypes about analytics professionals as opposed to computing professionals. Specifically,

Research question 1: Are negative stereotypes about analytics professionals as prevalent as those about computing professionals?

We found that overall, negative stereotypes about analytics professionals were less prevalent. They were less likely to ascribe the moniker of "geeky". They also were more likely to perceive soft skills as being important for analytics professionals than computer professionals. Based on prior literature, these features are more attractive to female students.

Research question 2: Are gender stereotypes about analytics professionals as prevalent as those about computing professionals?

Our results indicate that respondents were less likely to perceive gender stereotypes about analytics professionals than computer professionals. This may be an important key to helping female students picture themselves as analytics professionals, as prior work has found this perception to be a significant barrier preventing women from pursuing computer careers (Bock et al. 2013).

If analytics is a subset of the general computing and IT field, why does the perception of analytics seem to be more positive? Why is the analytics profession viewed as less geeky, more social, more managerial-focused, and more desirable? We posit that the results stem from three possible explanations at three levels: perceptual, cognitive, and social. These explanations are not mutually exclusive and can co-exist and impact the decision to study in the computing and analytics field simultaneously or none at all. We discuss each possible explanation and offer paths for future research in this domain.

Perceptual Explanation

Living at a time when people of all ages need to process a plethora of information daily (Bawden & Robinson, 2020), individuals attempt to avoid or reduce information overload by using shortcuts in their decision-making (Nathaniel, 2022). Thus, titles and keywords have become their saviors. For instance, most people don't read the news itself but rather read only the headline (Van der Meer et al., 2020; Xie, 2019). Combining the existing stereotypes about women and computing (Vitores & Gil-Juárez, 2016) with daily attempts to reduce cognitive overload by relying on keywords, headlines, and titles can explain the ever-stagnant growth of women in computing and the bigger popularity of the analytics field. It is possible that many will only judge choices, items, and fields of study primarily based on the words used to describe those fields.

For this reason, appearances matter. Using the right word or phrase should not only be a marketing priority but also crucial in any communication. In other words, degree titles, major benefits, and other descriptors must be updated to words the current climate perceives more positively. This is somewhat analogous to corporations and media using constantly outdating certain words and using "politically correct words" instead to be more inclusive and neutral to everyone (e.g., artificial instead of man-made) (Ehlion, 2022). Similarly, in the context of women and computing, one stream of research can investigate which words are neutral or positively perceived by the targeted audience. Survey and focus group studies can be conducted to understand a) what qualities and attributes women are after in a major, b) understand which keywords trigger negative perceptions in their mind, c) investigate new keywords based on the results of (a) and (b).

Cognitive Explanation

The second explanation behind the results can be due to real deficiencies in the computing fields. This is where the issue is not merely surface level concerning using the right words. Rather, this reason deals with computing majors' actual content and offers. Under this explanation, it is assumed that the person has deliberated on their decision and has not mainly relied upon their perception to make a decision. Selecting a field of study and career is a personal choice. Although there are similarities to what all genders value in studies and careers, there are notable differences. For example, for women, a career that helps society and offers more time flexibility to be with family is more important than for men (Pew Research, 2013). Additionally, certain subjects, such as math, create more anxiety in women to the point that "math anxiety" is highlighted as a barrier to entry (AAUW, 2020).

Per this potential reason, the female students may astutely have investigated their options and found that computing doesn't have the desirable qualities they are after (e.g., helping society) and, worse, has attributes such as math, which can be anxiety-inducing. To address this potential cause, colleges must update their degree content and offer more support. This does not mean the colleges should start offering courses that are only desirable to students, ignoring market demands. Rather, the goal is updating the course materials based on the workplace expectations and present them in a way that is more engaging considering the student population, for example by using more examples of women in business, having additional women guest speakers, and intentional diversifying the methods of delivery and networking events. As another example, they should offer more courses and support for more anxiety-inducing topics. This can be beneficial for students of all genders. They should also highlight and discuss the benefits of careers in computing, which resonates more with women. We note these suggestions based on what has been done thus far. However, there is room for future researchers to understand what values female students have in the current age. Surveys and experiments to compare the status quo program curriculum with a novel curriculum that includes content and discussion of values important to women can be an exciting domain of future work.

Social Explanation

The final explanation can be attributed to the representation of women in general in the computing field. If we were to ask a focus group to imagine a person who works in IT or computing, chances are most will describe a man with glasses. When the media has historically depicted people in computing as men, when educational systems from early grades to universities do not attempt to highlight women in computing in history, and when most of the women in prior generations have not entered a career in computing (AAUW, 2020), it is no surprise that many current female students don't wish to enter the field of computing. People observe the world around them to make decisions and use others as role models. When they don't exist, it may feel risky to do something that others haven't. Considering most people, particularly women at younger ages, are more risk-averse (Jianakoplos & Bernasek, 1998), it is understandable why many wouldn't enter the field of computing. This also explains why analytics is more popular because it is novel in the eyes of many. Unlike computing and IT, society has not set expectations and established stereotypes.

Per this explanation, a social movement is required to push women's growth in the computing field. Accordingly, among all three possible explanations offered, this is the hardest to achieve as a change will only everyone from media to existing establishments, men, women, and other groups work together to make the societal shift. As for researchers, they can investigate how much societal reasons influence the decision-making of female college students. There's no denying that society's perception influences a person's perception. However, the degree of this influence can be worth investigating. For example, researchers can identify various societal factors, test their association as antecedents with perceptual factors, and see how both impact decision-making to study various computing majors.

Limitations

There are three main limitations to this study. First, despite the diversity in respondents (both gender and race), all respondents are roughly around the same age. As people age, perceptions will change and grow. Thus, the use of the convenience sample in this case poses an inherent limitation. Additionally, as with any student population from one location, it is possible the students' perceptions are influenced by their environment. While we cannot say that for certain, it is nonetheless a limitation to the findings. Finally, the methodology used in the study was not developed to find causation or establish association. Instead, to observe the existing perceptions of the students. We accepted the limitation in this stage as the study was designed to observe the existing perceptions. However, future work can further expand on these observations through more complex methodologies.

Future Research

Future studies can further improve upon the study's sample size, including students from various majors and expanding the study to middle school and high school. Table 3 summarizes future paths for the research.

Table 3. Summary of Potential Explanations, Possible Solutions, and Future Research

Explanation	Description	Possible Solution	Future Research
Outdated descriptors (Perceptual)	Students are dissuaded by words, titles, keywords due to existing stereotypes	Change the degree titles, keywords, and description to something that while relevant to workplace requirement, is new and positively perceived	Conduct surveys, focus groups to understand the right words to use for computing majors and what qualities are female students are after
Outdated Content (Cognitive)	Students are dissuaded by the content of the major	Update the course requirement, add additional materials that desirable to female students	Conduct experiments, A/B testing between a status quo program curriculum with modified curriculum

			which has integrated the most desirable qualities
Outdated Culture (Social)	Students are dissuaded by how society/culture view computing field	Require a cultural movement at all levels	Research can investigate how societal views impact students' decision in pursuing computing

CONCLUSION

With the decline in participation and representation of women in computing, the current study set out to discover the perceptions of the students regarding this topic. In particular, we surveyed students on negative stereotypes and gender stereotypes with respect to computing fields. We additionally asked students about their perceptions of analytics and compared the results with those from computing. We observed that both negative and gender stereotypes are present more strongly among women. Not only do they perceive computing as a more male-friendly, but they also perceive it as geekier, more tech-oriented, and less social than analytics. While we argue that the causes can be merely based on respondents' perceptions, both cognitive and social reasons could be behind such negative and gender stereotypes. As we move towards a future where technology will dominate all industries, it is crucial to understand the hesitancy that women may have to join the computing field and try to address those reasons because lack of women representation in computing will not only create unhealthy power dynamics in the workplace but may also hinder women from fully realizing their potential (in particular if their hesitancy is due to social or perceptual views) and prevent them from contributing to the future where technology and computing will be the most prevalent and influential career choices. Further, these insights can be leveraged in future research to determine if additional analytics exposure or related interventions can provide a more positive introduction to other computing careers, such as Information Technology or Computer Science.

ACKNOWLEDGEMENTS

The authors would like to thank Manohar Madan for his contributions to this paper, in particular to the Literature Review.

REFERENCES

AAUW. (2020). The STEM Gap: Women and Girls in Science, Technology, Engineering and Mathematics. https://www.aauw.org/resources/research/the-stem-gap/

Adya, M., & Kaiser, K. M. (2005). Early determinants of women in the IT workforce: a model of girls' career choices. Information Technology & People, 18(3), 230-259.

Bawden, D., & Robinson, L. (2020). Information overload: An overview.

Bock, S. J., Taylor, L. J., Phillips, Z. E., & Sun, W. (2013). Women and minorities in computer science majors: Results on barriers from interviews and a survey. Issues in Information Systems, 14(1), 143-152.Buckley, M. (2009). Viewpoint Computing as social science. Communications of the ACM, 52(4), 29-30.

Cheryan, S., Plaut, V. C., Davies, P. G., & Steele, C. M. (2009). Ambient belonging: how stereotypical cues impact gender participation in computer science. Journal of personality and social psychology, 97(6), 1045.

Diekman, A. B., Brown, E. R., Johnston, A. M., & Clark, E. K. (2010). Seeking congruity between goals and roles: A new look at why women opt out of science, technology, engineering, and mathematics careers. Psychological science, 21(8), 1051-1057.

Duranton, S., Erlebach, J., Brégé, C., Danziger, J., Gallego, A. and Pauly M. (2020). What's Keeping Women Out of Data Science? BCG Global. https://www.bcg.com/publications/2020/what-keeps-women-out-data-science

Eagan, K., Stolzenberg, E. B., Ramirez, J. J., Aragon, M. C., Suchard, M. R., & Hurtado, S. (2014). The American freshman: National norms fall 2014. Los Angeles: Higher Education Research Institute, UCLA, 36.

Ehlion. (2022). What is Politically Correct language?

Gupta, N. (2012). Women undergraduates in engineering education in India, A study of growing women's participation. Gender, Technology and Development, 62(2), 153–176. https://doi.org/10.1177/097185241201600202

Hill, C., Corbett, C., & St Rose, A. (2010). Why so few? Women in science, technology, engineering, and mathematics. American Association of University Women. 1111 Sixteenth Street NW, Washington, DC 20036.

Holanda, M., Mourao, R. N., von Borries, G., Ramos, G. N., Araujo, A., & Walter, M. E. (2020, October). What do female students in middle and high schools think about computer science majors in Brasilia, Brazil? A survey in 2011 and 2019. In 2020 IEEE Frontiers in Education Conference (FIE) (pp. 1-7). IEEE.

Huffman, A. H., Whetten, J., & Huffman, W. H. (2013). Using technology in higher education: The influence of gender roles on technology self-efficacy. Computers in Human Behavior, 29(4), 1779-1786.

Jianakoplos, N. A., & Bernasek, A. (1998). Are women more risk averse? Economic Inquiry, 36(4), 620–630.

Khan, N. Z., & Luxton-Reilly, A. (2016, February). Is computing for social good the solution to closing the gender gap in computer science?. In Proceedings of the Australasian Computer Science Week Multiconference (pp. 1-5).

Margolis, J., & Fisher, A. (2002). Unlocking the clubhouse: Women in computing. MIT press.

Martell, R.F., Lane, D.M., & Emrich, C. (1996). "Male-female differences: A computer simulation. American Psychologist," 51, pp. 157–158.

Mellström, U. (2009). The intersection of gender, race and cultural boundaries, or why is computer science in Malaysia dominated by women?. Social studies of science, 39(6), 885-907.

Nathaniel, K.-A. (2022). Mental Shortcuts. The Routledge Handbook of Social Work Field Education in the Global South, 313.

N. C. for Women and I. T. (NCWIT). (2020) NCWIT Scorecard: The Status of Women in Computing. [Online]. https://ncwit.org/resource/scorecard/

Outlay, C. N., Platt, A. J., & Conroy, K. (2017). Getting IT together: A longitudinal look at linking girls' interest in IT careers to lessons taught in middle school camps. ACM Transactions on Computing Education (TOCE), 17(4), 1-17.

Papastergiou, M. (2008). Are computer science and information technology still masculine fields? High school students' perceptions and career choices. Computers & education, 51(2), 594-608.

Pew Research. (2013). What Men, Women Value in a Job. https://www.pewresearch.org/social-trends/2013/12/11/chapter-3-what-men-women-value-in-a-job/

Ramsey, N. and McCorduck, P. 2005. Where are the women in information technology? Report of literature search and interviews. Prepared for the National Center for Women & Information Technology. www.pamelamc.com/html/where_are_the_women_in_it.html.

Sax, L. J., Blaney, J. M., Lehman, K. J., Rodriguez, S. L., George, K. L., & Zavala, C. (2018). Sense of Belonging in Computing: The Role of Introductory Courses for Women and Underrepresented Minority Students. Social Sciences, 7(8), 122.

Sax, L. J., Lehman, K. J., Jacobs, J. A., Kanny, M. A., Lim, G., Monje-Paulson, L., & Zimmerman, H. B. (2017). Anatomy of an enduring gender gap: The evolution of women's participation in computer science. The Journal of Higher Education, 88(2), 258-293.

Sien, V. Y., Mui, G. Y., Tee, E. Y. J., & Singh, D. (2014, May). Perceptions of Malaysian female school children towards higher education in information technology. In Proceedings of the 52nd ACM conference on Computers and people research (pp. 97-104).

Van der Meer, T. G., Hameleers, M., & Kroon, A. C. (2020). Crafting our own biased media diets: The effects of confirmation, source, and negativity bias on selective attendance to online news. Mass Communication and Society, 23(6), 937–967.

Varma, R. (2011). Indian women and mathematics for computer science. IEEE Technology and Society Magazine, 30(1), 39–46. https://doi.org/10.1109/mts.2011.940294

Vitores, A., & Gil-Juárez, A. (2016). The trouble with 'women in computing': a critical examination of the deployment of research on the gender gap in computer science. Journal of Gender Studies, 25(6), 666-680.

Webb, H. C. and Rosson, M. B. 2011. Exploring careers while learning Alice 3D: A summer camp for middle school girls. In Proceedings of the 42nd ACM Technical Symposium on Computer Science Education. ACM, 377–382. Proceedings of the 42nd ACM Technical Symposium on Computer Science Education. ACM, 377–382

Xie, W. (2019). An analysis of fragmented reading and its social impact on college students in the era of new media. Journal of Contemporary Educational Research, 3(3), 33–37.

FROM DEFENSE TO RESILIENCE: PIVOT YOUR PARADIGM TO WIN THE LONG CYBERWAR

Michael S. Wills, Embry-Riddle Aeronautical University – Worldwide Campus
Dr. Aaron M. Glassman, Embry-Riddle Aeronautical University – Worldwide Campus
Dr. Denise Bollenback, Embry-Riddle Aeronautical University – Worldwide Campus

PROPOSED STUDY

Many cybersecurity incidents that happen at small to mid-size businesses involve a failure of security of some kind at a third-party transactional vendor such as a data center, cloud-based e-commerce system, customer relationship management platform, or point of sale system. Since most organizations use multiple platforms for day-to-day operations, there is a functional mesh of systems working together to ensure the organization can transact. For nearly a decade, security professionals have tried to call attention to these vulnerabilities as systems have become more tightly coupled making organizations dependent on these same systems to function. Unfortunately, little if anything has been accomplished to address these mesh-related vulnerabilities when complex, interwoven systems are needed for an organization to transact. It has been well documented that most information technology (IT) vendors are under constant cyberattack and this constant attack is what this paper refers to as the long cyber war. Over the years these attacked have only increased in frequency and duration. The current IT security paradigm is very defense oriented using a defense-in-depth (DiD) model of asset protection. This study will focus on pivoting the DiD model away from a defense focus to a resiliency focus with the authors acknowledge still must contain a strong defense component. Famed author Thomas Kuhn (2012) defined a paradigm shift as a fundamental change in the basic concepts or tenets of a scientific discipline. The proposed research will fill a paradigmatic gap in the existing literature and refocus the core tenets of security away from the present paradigm of defense-focused towards a more robust, inclusive, and holistic paradigm of resilience. Since a paradigm by definition has its own norms and laws from which policies and practices are created (Kuhn, 2012), we believe that a strategic pivot is needed to change what it means to “defend” against cyberattack and help organizations design better policies and practices that are resilience focused. The benefits of this paradigm shift should be of strong interest to IACIS participants and inform the audience as to what it means to pivot towards a new paradigm and rework existing policies and practices by viewing the same problem through a different lens.

BASIS OF STUDY

There are two distinct populations that will be interviewed as part of this study. The first population includes small to mid-size organizations that are dependent on a complex mesh of IT resources to reliably transact. The second population includes vendors who provide IT resources (security and non-security) to small to mid-size businesses. While many business applications have been moved into the cloud; however in-house security teams should not be ignored (Anjum, 2022). These teams often know the infrastructure of the systems much better than a third-party security service. The primary goal of this research is to assess whether resilience models are being used or if more traditional defense-focused models are being used. Since there is no single construct that makes up resilience, a multi-model approach will be used with raters scoring the interviews against a resilience scorecard composed of items from NIST, ISO, ASTM, and other existing standards-focused organizations. This benchmark will help the researchers determine the organizational mindset and focus as well as the mindset and focus of IT vendors who support these small to mid-size businesses. It will also identify how participating organizations compare as well as the current policies and positions that support this mindset.

IMPLICATIONS AND CONCLUSION

The results of this study will help inform organizational policy, practice, and culture as it relates to cybersecurity and will guide future research on how to shift fully towards resilience models as foundational to IT infrastructure from a cybersecurity point of view. Managers also have different perspectives regarding cybersecurity policies and infrastructures designed to support these policies. With a resilience paradigm, decision-makers can better view cybersiecurity as more than a "guard against X threat" concept and embrace the benefits of resiliency models. Such models also benefit decisions makers in that they are partially relieved from having to make difficult decisions about what type of threats to prioritize (Dunn 2023) since the threat landscape is only one facet of a resiliency model. Other disciplines such as aviation/aerospace, healthcare, and nuclear energy have moved towards resilience thinking and embraced the complex realities that sometimes defenses will fail. The results of this study will also serve as a state-of-the-industry perspective from a mindset point of view and help those tasked with creating business continuity plans, disaster recovery plans, and emergency preparedness plans to think more broadly about the role of cybersecurity and potentially shift away from a narrower defense-focused stances and towards a broader resilience-focused point of view. This shift requires us to know the present state of organizational thinking and this research will inform future research on how to complete the paradigm shift as well as bring forth new IT-focused resilience models. This research will also inform IT education to the extent that most professionals are trained using a "fundamentals first" approach. This approach focuses on the technics of cybersecurity (e.g., developing secure code, stopping network intruders, etc.) more so than how to adopt any particular mindset. These fundamentals first approach has also caused security and resilience to be viewed as cost functions as opposed to a value function. It is the hope of this research to update this thinking towards a more value-focused paradigm to which resilience, unlike defense, is generally viewed as positive organizational value.

REFERENCES

Anjum, Iffat, et al (2022). *Removing the reliance on perimeters for security using network views*. Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies.

Dunn Cavelty, et al (2023). *Making cyber security more resilient: adding social considerations to technological fixes*. Journal of Risk Research.

Kuhn, T. S. (2012). *The structure of Scientific Revolutions*. The University of Chicago Press.

CYBERSECURITY CURRICULUM DEVELOPMENT: ENHANCING CYBERSECURITY EDUCATION & TRAINING IN A UNIVERSITY ENVIRONMENT

Chandrashekar Challa, RFL College of Business, Virginia State University, cchalla@vsu.edu
Ephrem Eyob, RFL College of Business, Virginia State University, eeyob@vsu.edu

ABSTRACT

The landscape of cyber careers is evolving continuously. Since the days of computer networking and the advent of cyber threats, the field of cybersecurity has seen progressively increasing changes in hacking and academic initiatives to incorporate cybersecurity education in colleges & universities. The world currently needs more penetration testers, incident responders, threat hunters, and cyber defenders than ever before. The cybersecurity market will reach $262 billion in global spending by 2026 (Kapko, M. 2022). The global security workforce has reached 4.7 million workers (Lake, S. (2022). The US Bureau of Labor Statistics predicts the number of information security analyst jobs to grow by 35%, making this the eighth fastest-growing occupation in the United States (Lake, S. (2022). But the cybersecurity-educated community has not 73ept up with the growing requirement for cybersecurity professionals, resulting in a gap between supply and demand. This paper will analyze current cybersecurity curriculums and suggests a framework to enhance cybersecurity curriculums for colleges and universities with and without cybersecurity programs.

BASIS OF THE STUDY

With each new device connected to a network, cybersecurity concerns increase. It necessitates the need to increase involvement and advancement of cybersecurity education. (Norita Ahmad, et, 2022). We propose using the curriculum framework of the National Centers of Academic Excellence in Cybersecurity (NCAE-C 2022) administered by the National Security Agency (NSA) for Cyber Operations (CO), for Cyber Defense (CD), and for Cyber Research (CAE-R) programs. The NCAE-C program aims to promote and support quality academic programs of higher learning that help produce the nation's cyber workforce.

IMPLICATIONS

We propose that colleges and universities use the technical or non-technical approach to designing their cybersecurity programs at each level; Associate, bachelor's, Master, and Doctorate. The cybersecurity programs should target to create a skilled workforce in the areas of CO, CD, and CR. Colleges and Universities who follow and offer such programs using the CAE framework in their programs will not only create a skilled cybersecurity workforce that will bridge the demand and supply gap between cybersecurity jobs and workforce but also have a chance of getting certified and accredited by accreditors such as the NCAE-C.

ANALYSIS AND CONCLUSIONS

Colleges and universities currently offering cybersecurity programs will be evaluated to match the framework provided by the (NCAE) administered by the (NSA). Such college and university programs will be mapped to the framework provided by NCAE and NSA to arrive at a framework compatibility score to establish alignment of their program offerings to those advocated by NCAE and NSA. The information and data for this analysis will be gathered by visiting the websites of these Colleges and Universities.

Colleges and Universities that have not joined this initiative and are eagerly waiting on the border can distinguish themselves by creating a niche in their program offerings by following one of the tracks; Cyber Operations (CO), Cyber Defense (CD), and Cyber Research (CR) depending upon the factors such as student demographics, geographic location, industry profile, workforce requirements. Depending on the level of degrees offered, these Colleges and Universities can consider either a technical or non-technical track and choose Cyber Operations (CO), Cyber Defense (CD), and Cyber Research (CR) as their adoption strategies in starting their cybersecurity programs. It's important to note that the specific cybersecurity curriculum may vary depending on the educational institution, the level of the program (undergraduate or graduate), and any specialized tracks or concentrations offered. We plan to propose a technical and non-technical framework based on the factors listed above using the framework provided by the National Centers of Academic Excellence in Cybersecurity (NCAE) administered by the National Security Agency (NSA).

REFERENCES

Kapko, M. (2022, October 18) Cybersecurity spending on pace to surpass $260B by 2026. Cybersecurity Drive. https://www.cybersecuritydive.com/news/security-spending-balloons/634365/

Lake, S. (2022, October 20) The cybersecurity industry is short 3.4 million workers—that's good news for cyber wages. Fortune. https://fortune.com/education/articles/the-cybersecurity-industry-is-short-3-4-million-workers-thats-good-news-for-cyber-wages/

Lake, S. (2022, December 8). This cybersecurity job is one of the fastest-growing in the U.S.—and it pays six figures. https://fortune.com/education/articles/this-cybersecurity-job-is-one-of-the-fastest-growing-in-the-u-s-and-it-pays-six-figures/

Norita Ahmad, Phillip A. Laplante, Joanna F. DeFranco, Mohamad Kassab,(July-Sept 2022), A Cybersecurity Educated Community; IEEE Transactions on Emerging Topics in Computing; July-Sept. 2022, pp. 1456-1463, vol. 10.

National Centers of Academic Excellence in Cybersecurity (NCAE-C 2022) administered by the National Security Agency (NSA). Prepared by the Application Process and Adjudication Rubric (APAR) Cyber Defense Working Group (CDWG) October 2022 20221011_CAE2022_ CAE-CD_Designation_Requirements_Ver1.14.

National Centers of Academic Excellence in Cybersecurity, NCAE-C 2023, Proposed Designation Requirements and Application Process, For CAE-Cyber Research (CAE-R) January 2023. 20230119_CAE2023_ CAE-R_ Proposed Designation Requirements Draft22.

National Centers of Academic Excellence in Cybersecurity NCAE-C 2022 Designation Requirements and Application Process For CAE Cyber Operations (CAE-CO) *Prepared by the* Application Process and Adjudication Rubric (APAR) Cyber Operations Working Group (COWG) December 2022 20221207_CAE2022_CAE-CO_Designation_Requirement_Ver1.8.

VULNERABILITIES IN MODERN CONNECTED VEHICLES: A CALL TO ACTION

Kevin Seed, Community College of Allegheny County, kvnseed@gmail.com
Matthew Kisow, Community College of Allegheny County, mkisow@ccac.edu

ABSTRACT

With the increased connectivity of modern vehicles comes more vulnerability to cyber-attacks. In the past decade, the need for cybersecurity in everyday vehicles has increased dramatically. With the increase of technology packed into vehicles and the evolution of new technologies, cybersecurity measures have fallen behind. Several organizations have set standards and guidelines to increase the implementation of cybersecurity.

Keywords: cybersecurity, connected vehicles, autonomous vehicles, vulnerabilities, threats

INTRODUCTION

Our world has become more interconnected than ever before. The technology we carry daily connects us with people and information, all available within seconds from anywhere with a cellular signal (wireless connection). It's not just our phones and personal devices that do this. This also extends to our modes of transportation, such as the cars we drive to the planes that carry us to far-off destinations. With all these vehicles becoming the Internet of Things (IoT) devices, the question of how secure they are is becoming a concern.

Since the early part of the twenty-first century, several vulnerabilities in our modes of transportation have come to light. At the time, automotive companies were focused on putting more and more technology into vehicles for convenience and luxury; proportionally, the number of computer components, called Electronic Control Units (ECUs), increased, and each served its function. One ECU would control the braking system, another the infotainment center, and another engine management. These controls were not initially designed with cyber threats in mind, (Valasek & Miller, 2014).

Known hacking of transportation is not limited to just automobiles. In May of 2015, the FBI detained programmer Chris Roberts in response to a Twitter post that he made after hacking into the avionics and flight control system via the in-flight entertainment system of a Boeing 737/800, "[I] [f]ind myself on a 737/800, [let's] see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? "PASS OXYGEN ON" Anyone ? :), (Anadolu Agency, 2015)" According to a warrant submitted by the FBI, Roberts had hacked into the inflight entertainment system several times between 2011 and 2014. In doing so, he gained a degree of control over the flight controls and, in one instance, caused the aircraft to drift sideways, (Anadolu Agency, 2015).

In more recent times, vehicles are moving toward electrification and automation. At the forefront of this is Tesla with their Enhanced Autopilot controlled by the Tesla Autopilot ECU (APE). The Tesla autopilot system is considered a Level 2 autonomous driving system, (Synopsys, n.d.). This supports adaptive cruise control, lane changing/ centering, self-parking, and summoning the car from a parking spot. This system also creates a very attractive cyber-physical attack surface. For example, researchers at the Tencent Keen Security Lab could gain control of the system and remotely drive the car using a gaming pad, (Tencent Keen Security Lab, 2019).

These are among the many vulnerabilities that have come to light in recent years. And it brings into question what can be done to resolve these issues. Federal agencies have issued best practices, guidelines, and standards for manufacturers that are being implemented. Consumer awareness is also on the rise.

LITERATURE REVIEW

A paper published in 2014 by IOActive, authored by Charlie Miller and Chris Valasek, looked at common systems in several different vehicles investigating/researching how they could be compromised and the potential effects of those systems being compromised, (Valasek & Miller, 2014). They also highlight how the structure of the network and ECU locations within a vehicle can show how difficult or simple a remote attack would be. This was one of the first research papers that brought attention to the potential cyber-physical attack on a vehicle, (Miller & Valasek, 2015; Valasek & Miller, 2014).

In 2015, these same security researchers were able to disable a vehicle using a connected cellular system remotely; this research by Charlie Miller and Chris Valasek was presented at the BlackHat security conference in Las Vegas, NV, (Greenberg, 2015; Miller & Valasek, 2015; Valasek & Miller, 2014). Three years later, a study, "OVER-THE-AIR: HOW WE REMOTELY COMPROMISED THE GATEWAY, BCM, AND AUTOPILOT ECUS OF TESLA CARS," again showed how a cellular-connected vehicle, this time a Tesla, was compromised, (Nie, Liu, Du, & Zhang, 2018).

Another early study by (Jonathan Petit, 2015), "*Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR*" investigated how external sensors could be deceived or blinded. The two products tested in this experiment were the MobileEye C2-270 camera and the Ibeo Illuminance (LUX) 3 Light Image Detecting and Ranging (LiDAR) systems. LUX is equal to one lumen per meter, a measurement of intensity as perceived by the human eye, (NIST, 2016). These and later versions are used in Advanced Driver Assistance Systems (ADAS) and automated driving systems, (Synopsys, n.d.). This particular study was performed in a laboratory rather than a live environment. This is taken into account in their conclusions, but they hypothesize about the viability of each attack method.

The National Highway Traffic Safety Administration (NHTSA), a U.S. Department of Transportation branch, partnered with the National Institute of Standards and Technology (NIST) to create the National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles. This was the first set of guidelines and recommendations by a government agency to facilitate best practices in the automotive industry, (McCarthy & Harnett, 2014).

ISO/SAE 21434 is now the international standard for cybersecurity risk management for road-going vehicles. This standard addresses the perspective of cybersecurity in engineering electrical and electronic (E/E) systems. It allows companies to define cybersecurity policies and processes, manage cybersecurity risks, and foster a cybersecurity culture. ISO/SAE 21434 covers organizational cybersecurity management, project-dependent cybersecurity management, distributed cybersecurity activities, continual cybersecurity activities, development phases, threat analysis, and risk assessment methods. Compliance with this standard is recommended, not compulsatory, (SAE International, 2021; Sembera, 2021).

Organizational cybersecurity management defines cybersecurity policy and governance, setting the rules and processes for cybersecurity. Responsibilities and personnel must be assigned to perform cybersecurity activities, support its implementation, manage risks, manage information sharing, and perform cybersecurity audits. A cybersecurity culture must be established that includes competence and awareness management with a goal of continuous improvement.

Project-dependent cybersecurity management is outlined and includes allocating responsibilities and planning cybersecurity activities for specific projects. The project's tailoring implementation includes reusing existing components, using out-of-context components, and using off-the-shelf components. This may only be used after assessing if said component introduces any vulnerabilities and if the modification would correct those vulnerabilities without introducing new ones. New attack techniques, newly discovered vulnerabilities, and changes in the original design must also be accounted for. A case must then be created for the item or component to explain the degree of cybersecurity it has or provides. An assessment is then made on whether the project results are accepted, conditionally accepted, or rejected.

Continuous cybersecurity activities need to be performed by an organization to meet this standard. They must monitor and collect information on vulnerabilities and potential threats to their products. In the case of an event, an assessment must be made to determine the level of impact and respond appropriately. Vulnerability assessments must be conducted regularly, and a root cause analysis must be performed to determine the underlying cause of any vulnerability, (SAE International, 2021; Sembera, 2021).

In 2016, the NHTSA published a new set of guidelines called Cybersecurity Best Practices for the Safety of Modern Vehicles. This document is an updated version of the NIST Cybersecurity Risk Management Framework Applied to Modern Vehicles. This document has also seen multiple updates in the last few years, with the most recent version published in September of 2022, (U.S. Department of Transportation, 2022). This revision builds upon ISO/SAE 21434, and information gathered through the Automotive Information Sharing and Analysis Center, (Auto-ISAC, n.d.).

The guidelines recommend a layered approach to vehicle cybersecurity that assumes some systems could be compromised. This could reduce the chances of a successful attack and mitigate potential damages. The importance of buy-in from the leadership level to create a cybersecurity culture is highlighted in the guidelines. This commitment to cybersecurity is demonstrated by allocating dedicated resources and personnel, providing continual education on cybersecurity to the workforce, streamlining direct communication channels for cybersecurity-related matters, and allowing personnel to voice considerations in the vehicle safety design process. The vehicle development process must include cybersecurity considerations that account for the vehicle's full lifecycle. This process includes a risk assessment, removing or mitigating safety-critical risks to acceptable levels, and layers of protection for the assessed risks. Suppliers and the OEM should maintain an inventory of hardware and software assets used in each ECU so that if a vulnerability is discovered, the manufacturer can identify what vehicles are affected, (U.S. Department of Transportation, 2022).

The importance of sharing information regarding cybersecurity within the automotive industry was brought forth in Executive Order 13691, "*Promoting Private Sector Cybersecurity Information Sharing*, (Exec. Order No. 13691 Promoting Private Sector Cybersecurity Information Sharing, 2015)." The automotive industry created Auto-ISAC (Auto-ISAC, n.d.) to accomplish this. Using Auto-ISAC, automotive manufacturers, software developers, automotive equipment suppliers, and communication service providers can promptly share information about cybersecurity issues. To gather this information, manufacturers should create vulnerability reporting programs that provide external researchers a means to report vulnerabilities.

The guidelines also go into the more technical best practices for vehicle cybersecurity. Developers may leave access to an ECU open for debugging in the form of an open port. Such ports should be closed if there's no foreseeable need for continued access. If there is a need for continued developer-level access, cryptographic credentials should be used to prevent unauthorized access. The cryptography that the manufacturer employs should be current. Vehicle diagnostic functionality should be limited as much as possible without affecting vehicle repair support and serviceability and should be secured with public key cryptography. If not properly secured, it could be used to compromise safety-related systems. Appropriate cryptography and encryption should also be used with communications to back-end servers, software updates, and over-the-air updates, (U.S. Department of Transportation, 2022).

There are several instances in which a manufacturer will use existing products made by an outside company in one or more of their vehicles. This is covered in the current ISO/SAE standard in distributed cybersecurity activities. It places responsibilities for the components used on both the vendor and the vehicle manufacturer. The vendor has several responsibilities before supplying a component to a manufacturer. Before purchasing from a vendor, the manufacturer will evaluate the vendor to see if they can conform to the standards of ISO/SAE 21434 or the previous implementation of a prior cybersecurity engineering standard, (SAE International, 2021; Sembera, 2021). The vendor must provide a record of their cybersecurity capabilities, including cybersecurity activities, incident response, and a summary of previous cybersecurity assessment reports; once the manufacturer partners with a vendor, responsibility for the component becomes divided. The manufacturer is responsible for validating the cybersecurity of the component on the vehicle level and reporting to the vendor if a vulnerability is discovered. It is then the manufacturer's responsibility to deploy any software updates to correct vulnerabilities in both pre and postproduction vehicles, (U.S. Department of Transportation, 2022).

Keen Security Lab has researched various Tesla models and, in 2017, released a white paper with some of the results. The subject of this particular paper was successful remote attacks on the Tesla Model S and Model X via their Wi-Fi/3G connection. The vulnerabilities that allowed this attack existed in WebKit, a web browser engine initially released in 1998 that supports macOS, Windows, and various Unix-like operating systems, (WebKit, 2023). The vulnerability used exploited the web browser in the Tesla (Nie et al., 2018). The vulnerabilities have been recorded in the Common Vulnerabilities and Exposures (CVE) database, which the MITRE Corporation created with the mission to "identify, define, and catalog publicly disclosed cybersecurity vulnerabilities," (MITRE, 2023). The first vulnerability was local privilege escalation (CVE-2017-6261), a well-known kernel vulnerability that allowed them to gain root access and escape the "AppArmor." AppArmor, initially released in 1998, is a Linux kernel security module that allows system administrators to restrict the capabilities of a program using profiles, (Spennerberg, 2006). They then bypassed code signing protection to insert a customized firmware updater by exploiting a random rename function (CVE-2017-9983). The firmware updater targeted the APE, gaining root access by executing unprivileged commands from the central information display allowing them to bypass the digital handshake, (Nie et al., 2018).

As the increasing need for autonomous vehicles (AV) continues to grow. There will be an increase in vehicle-to-infrastructure (V2I) systems, (Duvall, Hannon, Katseff, Safran, & Wallace, 2019). Curb modifications, staging areas, mobility hubs, and public charging facilities are all part of the new AV infrastructure, and each is vulnerable to physical and cyber-attacks. On April 27, 2023, the Federal Communications Commission published an advisory, "What is 'Juice Jacking' and Tips to Avoid It, (FCC, 2023)." This advisory warned consumers that public charging stations could load malware onto personal devices. These attacks can leave these vehicles at risk, (Johnson, Berg, Anderson, & Wright, 2022); indeed, vulnerabilities in AV and EV charging security are not hard to find, (Root, 2023); researchers from Concordia University highlighted, severe vulnerabilities that included the ability to disable chargers and deploy malware, (Nasr, Torabi, Bou-Harb, Fachkha, & Assi, 2022).

DISCUSSION

Connected Systems

Black Hat security researchers Charlie Miller, a security researcher for IOActive, an independent security research organization known for reporting high-severity vulnerabilities, and Chris Valasek, a security researcher for Twitter, exploited a vulnerability in the infotainment system of a 2014 Jeep Cherokee by accessing the system using the vehicle's cellular connection, (Coyle, 2015; Greenberg, 2015). The two security researchers initially exposed this vulnerability at Black Hat 2015, an annual international security conference (Miller & Valasek, 2015). These researchers remotely accessed this vehicle driven by Andy Greenburg, a Wired magazine writer, down a busy St. Louis highway (Coyle, 2015; Greenberg, 2015). At first, Andy didn't notice any significant changes. Then the security researchers Charlie Miller and Chris Valasek turned on the air conditioning full blast and displayed an image of themselves wearing tracksuits on the infotainment screen.

Things started getting slightly more unpleasant for Andy when the radio station was changed and suddenly turned up to maximum volume. The wipers were turned on while the washer fluid was constantly sprayed onto the windshield. Then finally, the engine of the 2014 Jeep Cherokee was cut off, and the vehicle slowed to a near stop on the busy St. Louis highway, leading Andy to plead for control of the SUV back, (Coyle, 2015; Greenberg, 2015; Valasek & Miller, 2014).

Later, in a parking lot, the researchers further demonstrated how much control they had over the vehicle by taking control of the steering; while the Jeep was in reverse and disabling the brakes, causing the Jeep to end up in a drainage ditch. This was the first widely known incident of a car being hacked and taken control of. The two researchers made their findings known to Chrysler (Jeep's parent company), and a recall was issued to patch the security vulnerability, (Greenberg, 2015).

A researcher for IOActive published an article in 2016 about how he gained access to debug information on their airline In-Flight Entertainment (IFE) system, (Santamarta, 2016). After a quick Google search found a directory of publicly available firmware updates for IFEs across multiple airlines, this finding was reported, and the directory is no longer accessible to the public. Still, the source code for the IFE devices was found on a different site. It is explained that if an attacker were to exploit a vulnerability, the most damage they should inflict would be within the entertainment and PA systems without being able to access the aircraft control domain. Such activities include stealing credit card information, altering displayed information, playing sound clips over the intercom, or crashing the whole system, (Santamarta, 2016). The physical controls of the aircraft and the aircraft control domain should be physically separated from the rest of the internal network, but this isn't always the case. If there is a physical connection, the potential of an attack can't be disregarded.

Sensors

Vulnerabilities in modern vehicles, however, are not limited to remote attacks. Vehicles that employ any level of automation rely on inputs from multiple sensors and cameras all over the vehicle. These sensors are not impervious to deception or tampering. Sensor vulnerability is an emerging cybersecurity area in which vehicle sensor data can be manipulated. The Cybersecurity Best Practices for the Safety of Modern Vehicles states that OEMs need to take the risks of sensor vulnerabilities and signal manipulation into consideration in the vehicle development process, (U.S. Department of Transportation, 2022). Research has shown that creating minor physical changes to the road surface or road signs could fool automated systems. Researchers at Keen Research Labs demonstrated this on a Tesla Model S after remotely obtaining "*root*" privilege of the APE. After gaining the root privilege, the researchers manipulated the parameters for lane detection. In this experiment, called the "*Fake Lane Attack*," three inconspicuous lines were painted on the road. Due to the manipulation, the Autopilot recognized these lines and caused the car to steer toward the oncoming lane, (Tencent Keen Security Lab, 2019).

McAfee Advanced Threat Research studied "Model Hacking," which exploits weaknesses in machine learning algorithms to change results. Using known attack methods that affected image recognition in automated systems and focused on causing traffic signs to be misclassified, (Povolony, 2020). The result was an attack that would cause targeted and untargeted misclassification of traffic signs. When combined with the physical application of stickers to a targeted sign, the sign would be misclassified. A real-world experiment was then conducted using a Tesla Model X with Speed Assist and Tesla Automatic Cruise Control enabled and a 35mph sign with black tape that slightly altered the shape of the number. The result was the system classifying the 35mph sign as an 85mph sign causing the car to accelerate.

Alternatively, cameras and sensors can also be affected by physical attacks. One study experimented with using LEDs and lasers to fully or partially blind a Mobileye C2-270 camera, commonly used in vehicle automation systems. With the use of a 650nm laser, researchers were able to blind the camera partially. The results using LEDs were not successful in fully blinding the camera but were able to confuse the camera using a high output LED matrix, (Jonathan Petit, 2015). This determined that while the light was not particularly effective in blinding the sensor, a laser could have a blinding effect but was limited and not practical for an actual roadside attack.

Third-Party Products

To further complicate this emerging threat landscape, introducing third-party or aftermarket hardware and software presents additional threat vectors to these safety-related systems. Aftermarket systems can present an opportunity for attackers to gain access to a vehicle and its systems. Unlike other vulnerabilities, these are created by consumers installing devices and applications not provided by the original equipment manufacturer (OEM), (U.S. Department of Transportation, 2022).

Introducing third-party (aftermarket) hardware and software presents an opportunity for attackers to gain access to a vehicle and its systems. Unlike other vulnerabilities, these are created by consumers installing devices and applications not provided by the original equipment manufacturer (OEM). As such, the OEM has often not considered these devices when developing the vehicle's internal network security. This issue was recently addressed in the NHTSA Cybersecurity Best Practices 2022 update, (U.S. Department of Transportation, 2022). It states that the OEM should consider consumers connecting aftermarket devices to the vehicle, provide reasonable protections, provide appropriate access, and authenticate any such connection. Aftermarket device manufacturers must also consider that their devices connect to a cyber-physical system. Even if the original purpose of their device may not interact with safety-related systems, they must consider the possibility that access could be gained into such systems through their device and should employ strong cybersecurity protections.

Devices that create vulnerabilities can be any that provide an external pathway or connection. For example, ODB2 (Onboard Diagnostic 2) dongles that run insecure firmware can introduce a vulnerability by providing a threat actor access through Bluetooth or Wi-Fi, (Sembera, 2021). Further, any inadequately secured external device with an internet or mobile connection can introduce vulnerabilities to a vehicle's infotainment system when connected through Bluetooth or Wi-Fi. Consumers should consider any aftermarket device's intended function and purpose when connecting them to their vehicles. Ideally, a device should only be connected for as long as it needs to fulfill its purpose and then promptly disconnected afterward. How these devices transmit information should also be considered. It is well-established that Bluetooth has not been a reliably secure connection method, but it is often used to sync with aftermarket devices. If it is necessary to use one of these devices, the best practice would be to have the connection active only for as long as needed. The device's origin should also be checked, and research if there are any known vulnerabilities in the device.

Third-party applications are also something that consumers should be wary of. Once again, research should be done before installing and connecting to a vehicle. The application's origin should be a strong consideration in whether to download and utilize it. Ensure the application is from a reputable company and research any past or current vulnerabilities. It is also important to know what permissions the application has and what information is being stored. Tesla recently had an issue with a third-party app creating a physical vulnerability with their Model 3's and Model Y's. The vulnerability, discovered by 19-year-old David Colombo, originated from the TeslaMate app. The app is a popular logging tool designed to track energy consumption and location, but apparently, the app also stored the car's API access key (keyless access) and owner information. This allowed Colombo to gain entry to several different vehicles across multiple countries. The data could also be used to attack the affected vehicle remotely. The vulnerability was reported to both Tesla and TeslaMate before he announced his findings. TeslaMate issued a security patch, and Tesla revoked the security certificates for the affected vehicles, (Harel, 2022).

Infrastructure

The infrastructure behind connected vehicles provides attackers with a significant and viable attack surface that is easier to exploit than a direct attack on the vehicle. Infrastructure could be used to create a vulnerability in a connected vehicle or compromise systems that directly support a vehicle or its guidance. This makes it an attractive target to both individuals and state actors.

On October 10th of this year, the pro-Russian hacktivist group "Killnet" announced a distributed denial-of-service campaign against several components of US infrastructure. The announcement highlights "All Airports" as potential targets. That same day they succeeded in taking the websites for a handful of airports, including Atlanta, Chicago, New York, and LA, offline in their attack. The Transportation Security Administration stated that while the websites were taken offline, the attack didn't disrupt operations, (Aratani, 2022; U.S. Department of Transportation, 2022). Even though this attack didn't reach any operations systems, there is a clear need for cybersecurity protections for air traffic management systems.

For road-going EVs, there is a bit of a blind spot in part of the supporting infrastructure. This blind spot is public chargers. There is a significant need to enhance the security of public vehicle supply equipment (EVSE). Part of that need involves protecting customer data such as payment information, account information, locations visited, and the frequency of those visits. Another concern is overcharging. There are redundant safety systems installed in EVs and EVSEs to prevent fires, battery damage, and other safety issues. Despite this, there is a risk that the EV-to-EVSE connection could be compromised and bypass those safety systems. The EV-to-EVSE connection also presents bad actors with another attack surface to the vehicle. This may not affect EV owners who can charge their vehicles at home and never use their EV to travel long distances. However, public charging stations are necessary for those who cannot charge their vehicle at their residence or those using them to travel, (Jonathan Petit, 2015).

CONCLUSION

In our world, where we are constantly connected, our vehicles have become IoT devices with valuable, real-time information and entertainment features. This convenience has also come with its own set of risks. As technology evolves and automation becomes more prevalent, the systems that make it possible must be secured from attack, but cybersecurity measures have yet to catch up.

Several government and industry organizations have recognized the risks and implemented vehicle development and support standards throughout its lifecycle. The NHTSA partnered with NIST to create the first set of cybersecurity guidelines for road vehicles and later released the *Cybersecurity Best Practices for the Safety of Modern Vehicles*. Last year, the International Standards Organization released ISO/SAE 21434, *Surface Vehicle Standards - Road Vehicles - Cybersecurity Engineering.* The NHTSA then expanded on the Cybersecurity Best Practices with an update in late 2022, incorporating and expanding on ISO/SAE 21434. While all these are **voluntary standards** and guidelines, manufacturers must now consider cybersecurity when developing their vehicles.

Connected vehicles have many different vulnerabilities that attackers could exploit. Infotainment centers with cellular and/or Wi-Fi on cars and airliners provide prime targets for potential attackers to access vehicle systems. Sensors are another potential target for attacks. The data transmitted from a sensor can be manipulated into fooling automated systems, and the sensors can be blinded or confused. Third-party products and applications can introduce vulnerabilities to a vehicle's design. While the OEM is responsible for any products used in manufacturing, consumers should use caution when installing new applications or connecting devices. The infrastructure that supports connected vehicles is also a viable attack route. An attack could cause travel disruptions, steal payment information, or cause cyber-physical damage.

While there are areas in which consumers need to take precautions, most of the responsibilities for vehicle cybersecurity fall on the manufacturers. Manufacturers of any modern vehicle need to adopt considerations for cybersecurity through all phases of the lifecycle of vehicles. Adopting these standards is necessary to avoid monetary loss and the loss of trust in a product or brand. Some manufacturers go as far as to challenge hackers to attempt to hack their vehicles in public contests to test and improve cybersecurity in their vehicles, (Lambert, 2020). At the same time, in the past, others have taken legal action to prevent such research from being published rather than addressing the problem, (BBC News, 2013). It has already been demonstrated that connected vehicles have been in service with vulnerabilities for some time. These vulnerabilities are the byproduct of increasing the connectivity of vehicles for the convenience and luxury it offers without consideration for cybersecurity. The standards and guidelines that have been voluntary until now must be made **mandatory.** Leaving compliance to these standards as voluntary is **not** an option as it presents a major risk to public safety.

REFERENCES

Anadolu Agency. (2015, 2015/05/18/). Cybersecurity Expert Accused of Hacking Airplanes. *Anadolu Agency.* Retrieved from https://link.gale.com/apps/doc/A414219616/GIC?u=pitt92539&sid=bookmark-GIC&xid=43691568

Aratani, L. (2022, 10/12/2022). Hackers knock some U.S. airport websites offline. *The Washington Post*. Retrieved from https://www.washingtonpost.com/transportation/2022/10/10/hackers-cyber-attack-airport-websites/

Auto-ISAC. (n.d.). Automotive ISAC. Retrieved from https://automotiveisac.com/faq

BBC News. (2013, 07/29/2013). Car key immobiliser hack revelations blocked by UK court. *BBC News*. Retrieved from https://www.bbc.com/news/technology-23487928

Coyle, J. (2015). FCA Responds To Hackers' Scary Breach Of 2014 Jeep Cherokee: Video. *Motor Authority*. Retrieved from https://www.motorauthority.com/news/1099240_fca-responds-to-hackers-scary-breach-of-2014-jeep-cherokee-video

Exec. Order No. 13691 Promoting Private Sector Cybersecurity Information Sharing. (2015). *Exec. Order No. 13691 Promoting Private Sector Cybersecurity Information Sharing*. Federal Register: National Archives and Records Administration

FCC. (2023). *What is 'Juice Jacking' and Tips to Avoid It*. Federal Communication Commission: Federal Communication Commission Retrieved from https://www.fcc.gov/juice-jacking-tips-to-avoid-it

Greenberg, A. (2015, 07/21/2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired Magazine*. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Harel, A. (2022, 01/27/2022). Let's make the teen Tesla hack a teachable moment. *Tech Crunch*. Retrieved from https://techcrunch.com/2022/01/27/lets-make-the-teen-tesla-hack-a-teachable-moment/

Johnson, J., Berg, T., Anderson, B., & Wright, B. (2022). Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies, 15*(11). doi:10.3390/en15113931

Jonathan Petit, B. S., Michael Feiri, Frank Kargl. (2015). Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. *blackhat.com*, 13. Retrieved from https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf

Lambert, F. (2020). Tesla is challenging hackers to crack its car, and it is putting ~$1 million on the line. Retrieved from https://electrek.co/2020/01/10/tesla-hacking-challenge/

McCarthy, C., & Harnett, K. (2014). *National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles*. (DOT HS 812 073). Washington, DC: National Highway Traffic Administration

Miller, C., & Valasek, C. (2015). *Remote Exploitation of an Unaltered Passenger Vechile.* Paper presented at the Black Hat 2015, Las Vegas, NV.

MITRE. (2023). History. Retrieved from https://www.cve.org/About/History

Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., & Assi, C. (2022). Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. *Computers & Security, 112*(Volume 112, January 2022). doi:https://doi.org/10.1016/j.cose.2021.102511

Nie, S., Liu, L., Du, Y., & Zhang, W. (2018). OVER-THE-AIR: HOW WE REMOTELY COMPROMISED THE GATEWAY, BCM, AND AUTOPILOT ECUS OF TESLA CARS. *blackhat.com*, 19. Retrieved from https://i.blackhat.com/us-18/Thu-August-9/us-18-Liu-Over-The-Air-How-We-Remotely-Compromised-The-Gateway-Bcm-And-Autopilot-Ecus-Of-Tesla-Cars-wp.pdf

NIST. (2016, 03/01/2023). Special Publication 811. Retrieved from https://www.nist.gov/pml/special-publication-811/nist-guide-si-chapter-9-rules-and-style-conventions-spelling-unit-names

Povolony, S. (2020). Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles. Retrieved from https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/

Root, T. (2023, 07/05/2023). EV Charger Hacking Poses a 'Catastrophic' Risk. *WIRED*. Retrieved from https://www.wired.com/story/electric-vehicle-charging-station-hacks/

SAE International. (2021). Surface Vehicle Standards - Road Vehicles: Cybersecurity Engineering ISO/SAE 21434. In (Vol. 2021-09, pp. 81). United States: SAE International.

Santamarta, R. (2016). In Flight Hacking System. Retrieved from https://ioactive.com/in-flight-hacking-system/

Sembera, V. (2021). ISO/SAE 21434 Setting the Standard for Connected Cars' Cybersecurity. Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-setting-the-standard-for-connected-cars-cybersecurity.pdf

Spennerberg, R. (2006, August 2006). Shutting Out Intruders with AppArmor. *Linux Magazine(69/2006),* 30-34. Retrieved from https://www.linux-magazine.com/Issues/2006/69/AppArmor

Synopsys. (n.d.). The 6 Levels of Vehicle Autonomy Explained. Retrieved from https://www.synopsys.com/automotive/autonomous-driving-levels.html

Tencent Keen Security Lab. (2019). Experimental Security Research of Tesla Autopilot. 38. Retrieved from https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf

U.S. Department of Transportation. (2022). *Cybersecurity Best Practices for the Safety of Modern Vehicles*. National Highway Traffic Safety Administration: National Highway Traffic Safety Administration Retrieved from https://www.citationmachine.net/Son/cite-a-websitehttps://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf

Valasek, C., & Miller, C. (2014). A Survey of Remote Automotive Attack Surfaces. *IOActive*, 90. Retrieved from https://ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf

WebKit. (2023). WebKit. Retrieved from https://webkit.org/

TEACHER PREPARATION AND CURRICULUM DESIGN IN CYBERSECURITY

Aryan Patel, Kennesaw State University, apate307@students.kennesaw.edu
Zhigang Li, Kennesaw State University, zli8@kennesaw.edu
Xin Tian, Kennesaw State University, xtian2@kennesaw.edu

ABSTRACT

Cybersecurity consists of the guidelines and techniques used to defend from online hazards. But, with the growing shortage of cybersecurity officers and expanding cyberattacks, cybersecurity knowledge needs to be widespread which is why cybersecurity education is offered as a solution. To find effective methods of instructing cybersecurity, we conducted a literary review on existing propositions. The method consisted of using a flowchart approach which began with using keywords to discover sources, answering our thesis questions, and analyzing data based on criteria. Then, ten sources were finalized based on the performed evaluation. From the research, it was found that cybersecurity education is often inadequate because of a lack of school focus and teachers for cybersecurity. Hence, perspectives towards teacher preparation and collaborative curricula for cybersecurity were given. Some studies focused on media campaigns to promote the growth of cybersecurity education among families and the government. And, other studies focused on training teachers through summer programs, building on existing curricula, and working with experienced cybersecurity professionals. Ultimately, the studies not only focused on helping students learn cybersecurity but also aimed at strengthening teachers' understanding and educational programs, to boost cybersecurity learning to a global, unified level.

Keywords: Cybersecurity Education, Cybersecurity Curriculum, Teacher Preparation, Cybersecurity Awareness, Curriculum Design.

INTRODUCTION

Cybersecurity is defined as the measures taken to protect online users, networks, and data from unauthorized attackers and cyber threats. Specifically, many cyber threats comprise cases involving cyberbullying, online fraud, and racial abuse, which are directed toward vulnerable children on the Internet. And, pairing this with increased reliance on technology after the COVID-19 Pandemic, additional cyber threats have surged, increasing the risk for children online. As a result, many have begun discovering cyber breaches to be a consequence of human error and ineffective cybersecurity education. Ineffective Cybersecurity Education, particularly, is caused by the shortage of cybersecurity instructors in K-12 education and a missing established curriculum. And, to combat this issue and promote K-12 cybersecurity education, school officials and studies found innovative approaches to train cybersecurity educators and improve yearlong cybersecurity courses.

One adopted method includes giving new teachers hours of summer training for effective cybersecurity education and pairing them with industry partners, who can best provide them with updates and reviews of their teaching methods. Another method, similarly, includes promoting collaboration among educators who get to partner with one another to further develop cybersecurity curriculums. Moreover, additional methods also use discrete approaches by using fun activities, like Capture-The-Flag, to enhance student desire and confidence to practice cybersecurity.

The objective of this writing is to understand how to best prepare K-12 cybersecurity educators and establish a developed curriculum. We do this by analyzing the methods mentioned above and seeing the similarities between each method. And, by comparing the numerous studies, we describe which techniques work, and which do not. This can not only provide schools with effective strategies for developing cybersecurity education and training teachers but also reduce those strategies to the strongest possible ones with positive outcomes.

Lastly, the text is organized as follows: The next section covers the methodology that describes how we completed the research for this writing, followed by the literary review that evaluates each study and the validity of each teaching strategy. Then, next is the Discussion Section which elaborates on the similarities and strengths of each study, and the best procedures to train cybersecurity teachers and build adequate curricula. Lastly, the references section is provided to demonstrate the findings and citations of our sources.

METHODOLOGY

To address the challenges of K-12 cybersecurity education, we formed our research around two thesis questions. That being discovering the challenges educators face in the cybersecurity field, and how those educators can learn through training and experience to effectively instruct cybersecurity to K-12 students. Specifically, we answered these questions by conducting a literary review of sources to consider different strategies for preparing teachers and interpreting cybersecurity education. And, we further extended this study by comparing the differing methods from many sources and analyzing how effective each would be given its results.

To gather evidence and sources for review, we used three key steps:
Inclusion Criteria
Data Search and Breakdown
Data Evaluation and Computation

Inclusion Criteria. First, we considered sources in our study that were academically peer-reviewed to validate data and information presented as accurate based on done research and completed conferences. Then, to avoid obsolete sources and translating threats, we developed a requirement for our sources to strictly be in English and published during the 21st century. Moreover, we cut our sources to full-text sources that included abstracts, research results, and discussions to gain as much information as possible. Lastly, our criteria for incorporating sources consisted of matching keywords. This point was crucial for later searching for sources and guaranteeing that the found sources matched our ideals and goals for the project. Particularly, the keywords we analyzed included a combination of: "Cybersecurity Education," AND "Teacher Preparedness," OR "Cybersecurity Curriculum Design," OR "K-12 Learning for Cybersecurity," OR "Cybersafety Awareness," AND "Teacher Preparedness".

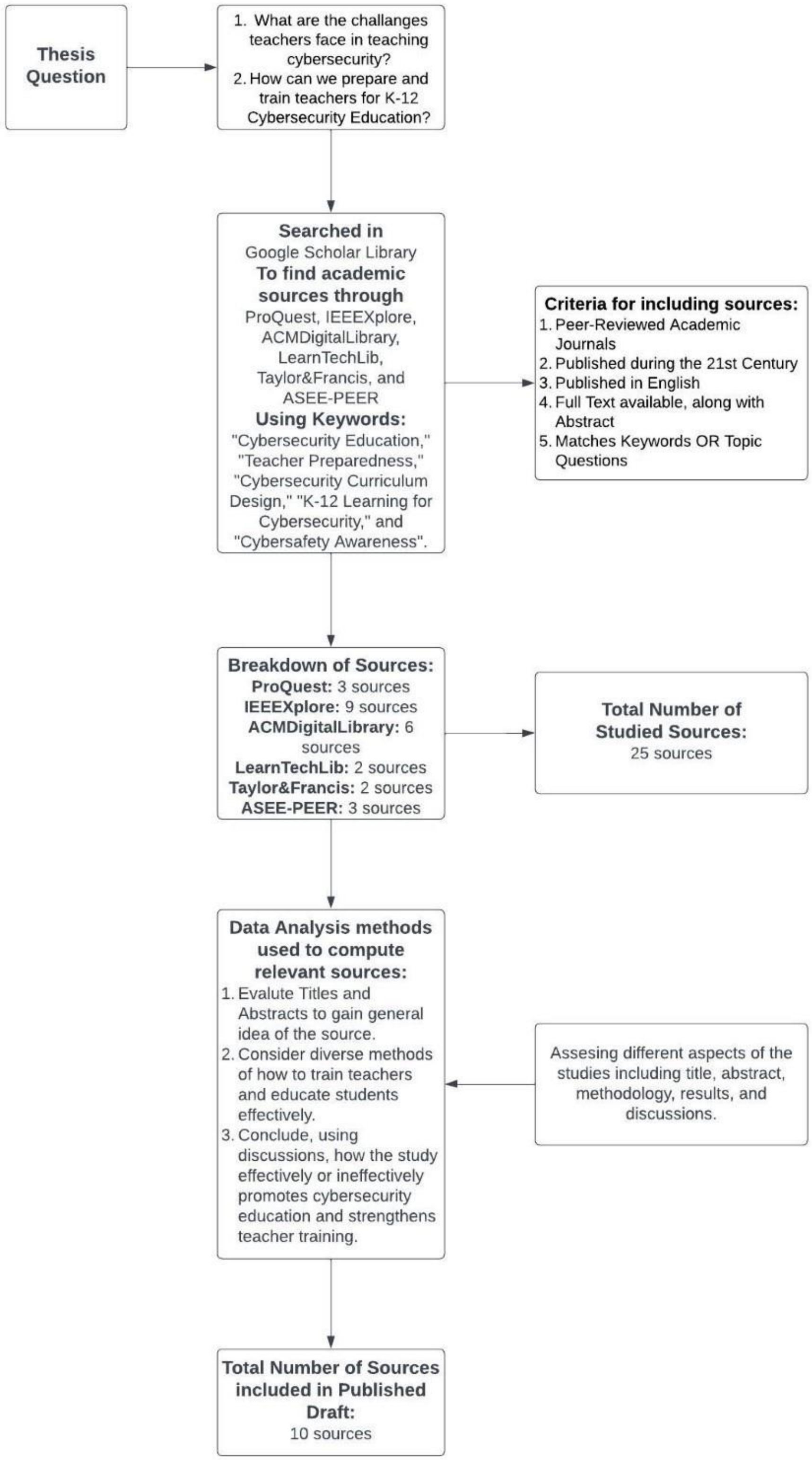
Data Search and Breakdown. Then, adopting the keywords discussed above, we discovered over 50 sources through Google Scholar. This opened our research to many databases including

ProQuest, IEEEXplore, ACMDigitalLibrary, LearnTechLib, Taylor&Francis, and ASEE-PEER. After finding these databases, we analyzed the sources using our criteria and reduced the source count to 25 based on their relevancy to the topic and thesis questions.

Data Evaluation and Computation. We broke down the found number of sources further, from 25 to 10, after analyzing evidence components. We did this by reading the methodologies, results, and discussions contained in each study, and how they correlated with our topic. The ideas that connected to our research questions included explanations of why cybersecurity teaching is important, methods of preparing teachers for cybersecurity education, organization of cybersecurity curriculum for schools, and the results of the tried methods on students. Ultimately, using this technique we how each source efficiently promotes cybersecurity education and strengthens teacher training to compute whether the source should be considered for the final literature review.

This methodology is further illustrated and clarified in the Flowchart (Diagram 1) below.

Diagram 1. Process of gathering sources for Literary Review.



RESULTS

This section consists of our discoveries on cybersecurity education and teacher preparation based on peer-reviewed academic journals. Specifically, non-experimental methods, like literary review, were used to analyze each source and answer our thesis questions about the challenges and preparation of cybersecurity education.

3.1 Why is cybersecurity education important in K-12 schools?

Cybersecurity Education is important for K-12 learners for assorted reasons varying from learning to protect from cyber threats online to learning about safe browsing online. Dawson, et. al point out that after the COVID-19 pandemic cyberattacks on institutions have greatly resulted from an increase in reliance on digital technology. And, pairing this with the shortage of cybersecurity professionals and high expenses that follow cybercrime, Dawson, et al. argue for better implementation of cybersecurity education to not only help reduce cyber threats in schools but to also promote cybersecurity as a professional among the youth (Dawson, n.d.). Likewise, Alrabaee, et al. Report comparable results where a lack of cybersecurity education has allowed for criminals to take advantage of technology to advertise their illegal products, like drugs, and further use technology to attack and target vulnerable organizations. In doing so, the authors seek to promote cybersecurity education by describing and extending the existing efforts cybersecurity programs that are used in education worldwide (Alrabaee et al., 2022). Sanzo, Scribner, and Wu explain in their Paper how cyberattacks have become more common, sophisticated, and harmful because of a reduced number of effective cybersecurity professionals, which is a shortage that results from untapped pools of talent, a lack of diversity, and inadequate standardization within K-16 institutions. In other words, Sanzo, Scribner, and Wu argue that cyber threats happen because of improper standardization and inclusion of cybersecurity education in schools, and argue the importance of how middle schools, high schools, and universities must work together to improve cybersecurity education and combat the shortage of technical professionals (Sanzo et al., 2021). Rahman, et al. use a unique perspective towards cybersecurity by explaining how children using technology and the Internet need to defend themselves against personal cyber risks. Particularly, they argue how children are vulnerable to gaming and gambling addiction, cybersex, and pornography on the Internet, exposed to sharing personal information, and victims of cyberbullying, and a result, must learn about effective strategies, in school, to defend themselves from such problems and safely browse on the Internet to avoid threats and inappropriate content (Rahman et al., 2020).

3.2 What are the best strategies for developing a cybersecurity curriculum and preparing K-12 teachers for education? How can each strategy be effective?

As described above, cybersecurity education is important for challenging worker shortages and learning to defend online, which is why an effective curriculum and teaching methods are needed for such education. According to Dawson, et al., teachers originally believe cybersecurity to be an irrelevant and difficult topic to teach, and do not think much of it; however, when presented with a curriculum and the given problems with cyber threats, they gain the self-efficacy and awareness to teach the topic (Dawson, n.d.). But, when asked to rate their abilities to teach cybersecurity (C3) topics, in a survey, the teachers answered that they lacked confidence and preparation to teach the challenging material. Hence, strategies for better teaching strategies and establishing a unified cybersecurity curriculum for educators are given. Specifically, Javidi and Sheybani, explain a way to create a Cybersecurity Pipeline which can connect teachers, students, parents, and industry stakeholders and raise awareness for cybersecurity education. And, through such Pipeline, teachers can obtain hours of summer training which shows them ways to incorporate cybersecurity education through AP (Advanced Placement) classes and fun-learning environments that include real-world problems (Javidi & Sheybani, 2018). Similarly, in another approach, IT (Information Technology) industry partners are also linked with teachers to teach them specific cybersecurity skills and provide them with learning templates that blend interactive and lecture methods of teaching (Javidi et al., n.d.). This shows the effectiveness of pairing teachers with professionals in the industry who can work together to enhance cybersecurity education in schools and further create more cybersecurity professionals graduating from the same schools. Additionally, skilled IT professionals can not only help teachers create new learning environments but further extend existing efforts. This strategy promoted by Alrabaee, et al. signifies that instead of only providing teachers with ideas, industry stakeholders can conduct a continuous review of cybersecurity educators to measure and update teachers' awareness and skills (Alrabaee et al., 2022). As a result, teachers are informed what they may be doing correctly or incorrectly to reconsider and improve their teaching techniques. Furthermore, another strategy uses a similar idea to pair together educators to establish a unified cybersecurity curriculum. As put by Sanzo, et al., K-12 schools join to create a collaborative curriculum, CIPHER, which incorporates student committees, designs cybersecurity pathways for students, and hosts professional cybersecurity development seminars for teachers (Sanzo et al., 2021). This implementation of a curriculum not only helps teachers gain more insight into preparedness for cybersecurity instruction from other teachers but also helps students work with other students and expand their interest and enjoyment of cybersecurity. Likewise, an approach using games, like Capture the Flag, also engages students together. As put by Leune and Petrilli, gamified simulations of cybersecurity, like Capture the Flag, in a curriculum can help students engage in entertaining activities and learn from real-world problems which also serve as lecture-style instruction. And, when tested, the CTF methods worked as they not only taught students new practical skills but also boosted students' self-confidence about learning serious cybersecurity topics (Leune & Petrilli, 2017). However, the following strategies would still be ineffective if cybersecurity education is not well-known or widespread. The major challenges in cybersecurity education are the lack of educational expertise, funding, and resources, and Rahman et al. Media campaigns, like television and radio broadcasts, would combat this problem (Rahman et al., 2020). Essentially, online promotion of cybersecurity learning challenges would not only influence governments and institutions around the world to develop cybersecurity education but also guide children's and parents' beliefs towards learning the importance of digital security.

3.3 What would be the outcome and impact of each strategy, in terms of cybersecurity education? Each strategy does not only impact students' education through teacher training, but also impacts parents, industry partners, and school departments who raise awareness and work alongside to promote improving cybersecurity education. And, such results are expressed in Diagram 2 below.

Diagram 2. Outcomes for each stakeholder in cybersecurity education.

Stakeholder	Outcome
Students	· Acquire ways to protect self and others online from cyberthreats like cyberbullying. · Learn ways to safe-browse the Internet, avoiding inappropriate content. · Form committees and further enhance thier knowledge of cybersecurity education. · Discover how IT Security can be an effective career path. · Participate in gamified simulations of cybersecurity, like Capture-The-Flag games, to gain interest in cybersecurity education and develop stronger practical skills.
Teachers	· Gain effective training hours for cybersecurity education. · Boost self-efficacy, awareness, and confidence in teaching cybersecurity. · Work with industry partners in the cybersecurity field to gain curriculum tools and feedback to enhance teaching. · Incorporate business-based and social problems of the world in cybersecurity classrooms, using learned strategies. · Participate in professional development sessions hosted by partnering institutions and industry professionals.
Institutions	· Work with other instiutions, including middle schools, high schools, and universities, to develop cohesive techniques for cybersecurity education. · Review and Improve current cybersecurity curricula to advance cybersecurity education and increase awareness. · Host events with gamified simulations of cybersecurity, like Capture-The-Flag and other interactive games, to elevate curiosity about cybersecurity education.
Parents	· Learn about the importance of cybersecurity education and its implementation methods in K-12 schools for children.
IT and Cybersecurity Industry	· Work with K-12 teachers to establish and enhance cybersecurity education. · Hire new cybersecurity professionals from pools of graduated high school and college students.

DISCUSSION AND CONCLUSION

In our literary review, cybersecurity education primarily shared an educational and worker perspective. The view aimed to combat the existing threats of cyber, and aim to overcome them through stronger, unified cybersecurity education. And, most of the studied sources break down the importance of cybersecurity education as a technique to overcome worker shortages and inform the youth of online safety on the Internet. Asghar and Luxton-Reilly emphasize how many, like the researched sources, link cybersecurity education and cyberthreats, “To address the global shortage of Cybersecurity skills, many universities have introduced degree programmes in Cybersecurity... [yet] there is no established global Cybersecurity curriculum currently followed by universities” (Asghar & Luxton-Reilly, 2020). Thus, to assess cybersecurity unemployment and create more workers, many solutions proposed creating a unified cybersecurity education system where teachers would collaborate with other educators and professionals in the Information Technology and Security fields. Additionally, other proposals focused on teacher preparation where teachers would receive the benefits of summer training, learning templates, and continuous teaching evaluation to improve learning outcomes for their respective cybersecurity classes. Lastly, some suggestions focused on building existing curriculums and helping students by engaging them in fun learning activities and communities and demonstrating the importance of cybersecurity through media. In summary, the propositions for a global cybersecurity curriculum can be summed up into three categories. Rowe, et al. describe the recommendations by stating a global curriculum should verify and update elements of cybersecurity, familiarize students with terminology, and evaluate students learning through real-world problems (Rowe et al., 2011). In conclusion, with growing cybersecurity unemployment and increasing cyber threats, teacher preparation and curriculum design become vital processes for ensuring effective cybersecurity education and educating others to defend themselves online.

REFERENCES

Alrabaee, S., Al-Kfairy, M., & Barka, E. (2022, March). Efforts and suggestions for improving cybersecurity education. In *2022 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1161-1168). IEEE.

Asghar, M. R., & Luxton-Reilly, A. (2020, February). A Case Study of a Cybersecurity Programme: Curriculum Design, Resource Management, and Reflections. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (pp. 16-22).

Dawson, K., Antonenko, P., Xu, Z., & Wusylko, C. (2022). Promoting interdisciplinary integration of cybersecurity knowledge, skills and career awareness in preservice teacher education. *Journal of Technology and Teacher Education*, *30*(2), 275-287.

Javidi, G., & Sheybani, E. (2018, October). K-12 cybersecurity education, research, and outreach. In *2018 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). IEEE.

Javidi, G., Sheybani, E., & Pieri, Z. (2019). A Holistic Approach to K12 Cybersecurity Education. In *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)* (pp. 77-80). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Leune, K., & Petrilli Jr, S. J. (2017, September). Using capture-the-flag to enhance the effectiveness of cybersecurity education. In *Proceedings of the 18th Annual Conference on Information Technology Education* (pp. 47-52).

Pusey, P., & Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education*, *28*(2), 82-85.

Rahman, N. A. A., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology, 10*(5), 378-382.

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113-122).

Sanzo, K. L., Scribner, J. P., & Wu, H. (2021). Designing a K-16 cybersecurity collaborative: Cipher. *IEEE Security & Privacy*, *19*(2), 56-59.

BIG DATA: MODERN BEST PRACTICES FOR DATA PROCESSING

Angel Ojeda-Castro, Universidad Ana G. Méndez, ut_aojeda@uagm.edu
Jorge Jiménez-Ramírez, Universidad Ana G. Méndez, jimenezj1@uagm.edu

ABSTRACT

As information flow grows, the massive quantity of facts clutters and piles up to unprecedented amounts. Yet all this bulk of data is so diverse, disordered, and structureless, it becomes strenuous to analyze and extract value from it. Information flow and facts creation does not necessarily refer to valuable data. Many algorithms have been developed to process this aggregate of data. This article reviews the current definitions of big data, summarizes the presently used machine learning techniques to analyze and process big data, and discusses deep learning techniques in contrast with conventional machine learning practices. As big data tends to be irrelevant if it is not properly handled, several deep learning techniques are outlined, and summarized to show ways to extract value from vast information sets. Understanding the deep learning advantage to extract value could help to develop new deep learning approaches for big data handling affairs, or to improve existing deep learning methods to maximize the valuable information that results from the massive aggregates of data.

Keywords: big data, machine learning, data processing, deep learning

INTRODUCTION

Big data are large-scale data sets generated by new technologies, such as mobile devices, points of sale, automated systems, social media, and the Internet of Things (Song et al., 2020). Big data is defined as a vast aggregate of facts that is highly structureless and disordered. (Khan et al, 2014). Retrieval and probing processes derive value from them. Yet a constant need for new technologies and architectures is often a quest without an end (Katal et al, 2013, Collymore et al., 2017). As information growth spurs swiftly, data dimensions surpass their handling capabilities (Power, 2014). Therefore, it becomes cumbersome to manage such large quantities in a reasonable time (Katal et al, 2013; Khan et al, 2014; Neaga & Liu 2014).

Currently, big data is an in-demand notion. It relates to the current and substantial usage of multimedia, social media, and the web throughout a broad span of apparatuses. The widespread use triggers an exponential growth in data hereafter (Neaga & Liu, 2014). Such complexity resolves into a burdensome undertaking to link, match, cleanse, and transform data across systems coming from various sources (Katal et al., 2013). Furthermore, data can be thorough in purview, seeking to cover whole populations or arrangements. Information might be akin; it could hold shared domains that allow the combination of separate information assortments (Kitchin, 2014). Big data is defined as the ability to manage, process, and analyze the five dimensions of data (5V): (Ahmad et al., 2020) volume, velocity, variety, value, and veracity (Wamba & Akter, 2019). The digital tool used for data collection and processing in big data is artificial intelligence (Kulakli & Osmanaj, 2020). The volume of data is generated from different sources, the result of which is the creation of information and observable patterns through data analysis (Casarotto et al., 2021). Data visualization improves the possibility of representing actual information and details in an organized manner leading to greater efficacy (Ridzuan, Nazmee, & Zainon, 2022). The integration of artificial intelligence in analytical business processes maximizes organizational competence in the performance of roles to be more efficient (Tinoco, Parente, Correia, Cortez, and Toll, 2021).

Machine learning is an enclosed action progression that allows computer programs to learn in self-activating ways to better themselves from historical facts. Its techniques are often grouped into supervised, unsupervised, or semi-supervised learning procedures. Machine Learning is one of the sparking novelties causing a pinnacle in the arising technologies promotion cycle expectancy scale (Crespo & Ojeda, 2017).

Deep Learning algorithms befit whenever there is learning from vast groups of unsupervised facts. They learn data depictions in a greedy-tiered manner. Deep Learning results have yielded remarkable outcomes in diverse machine learning applications, such as speech recognition, computer vision, and natural language processing. (Chen & Lin, 2014; Najafabadi et al., 2015)

Deep Learning techniques are appropriate if learning from large sets of unsupervised data is required. In a greedy tier-based fashion, they learn data visualizations. Results from deep learning have produced outstanding results in a variety of machine learning applications, including speech recognition, computer vision, and natural language processing.

LITERATURE REVIEW

Big Data Core Attributes

Big data attributes have increased as the overflow of information faces greater challenges. While the first models consisted of three core characteristics, namely, volume, variety, and Velocity (Bagheri & Shaltooki, 2015), other authors add the core trait of veracity to the mix (Neaga & Liu; Wang & Yuan, 2014). Yet as the bulk of data continues its rise, further traits are considered (Power, 2014; González & Ojeda, 2016) up to seven core principles (Katal et al, 2013; Khan et al, 2014). Particularly, Khan et al, 2014, suggest 6 core principles Volume, Velocity, Variety, Veracity, Validity Volatility, and Value.

Big data volume concerns the input magnitude being generated from all origins such as text, audio, video, social networking, research studies, medical data, space images, crime reports, weather forecasting, and natural disasters, among others (Khan et al., 2014). It also applies to the gathering of vast amounts of data daily consisting of terabytes or petabytes of information (Katal et al., 2013; Chen & Lin; Kitchin, 2014). In terms of the velocity feature, it refers to the information immediacy arising from several starting points (Katal et al., 2013), high in speed, and being brought about in or near real-time (Kitchin, 2014). Notwithstanding, it is not only the velocity to arriving facts that counts, but streaming the swift bestirring information into some big reservoir for further processing and examination.

Namely, such procedures are carried on either to preserve input facts or to oblige some response to the specifics as they come in. (Khan et al., 2014). As variety is concerned, large data are verily diverse. They comprise raw, structured, half-structured, and even structureless facts. Such information is hard to be tackled by the present customary analytic methods (Katal et al.,2013;

Kitchin 2014). Moreover, most data enter straightly from real human interfaces, thus mistakes are most certain in such information. As details variety impacts data unity, the more variety is reckoned in data; the more mistakes it would hold. (Khan et al., 2014). Lastly, veracity bespeaks the truthfulness of data (Khan et al., 2014). Unreliability of the information flow may arise accordingly. Partialness, duplicity, or rough estimates affect the veracity of facts altogether (Neaga & Liu, 2014). Hence it weighs dearly to cleanse big data with extensive instruments and algorithms (Khan et al., 2014).

According to Khan et al., there are three more concepts to consider regarding big data. The concept of validity arises as the contextual accuracy and rightfulness of information. Data could be truthful as itself but inaccurately applied to certain situations. Therefore, it is important to match reliable data with the proper medium, otherwise, validity would be compromised. (Khan et al., 2014). Volatility is defined as the upkeep guidelines of structured facts daily employed in businesses. Whenever the usage expiration is met, the data is eliminated. If upkeep surpasses its span, storage, and security could become costly to enact. Concepts affecting data such as Volume, Variety, and Velocity endow Volatility with weight and meaning herein (Khan et al., 2014).

According to Katal et al., big data value applies to take relevant outcomes from sifted information or to classify it following previously established constraints. Such a system model ought to manage efficiently massive portions of information. Moreover, to extract its worth, it is needed to draw out the most relevant information from all formerly gathered data of the organization. Concerning Khan et al, value is the wanted result of big data handling. There is a willingness to take out the best of any big data class that is collected. Information worth must surpass its price, right of possession, or operation (Khan et al., 2014).

Data Processing Techniques

Machine learning is an enclosed action progression that allows computer programs to learn in self-activating ways to better themselves from historical facts. Machine Learning can be employed in many fields such as bioinformatics, statistics, neuroscience, computer engineering, mathematics, business management, medicine, and computer science, among others. It seeks to solve composite decision-making and analytical chores in a self-activating manner. Many kinds of machine learning procedures exist, to wit, support vector machine (SVM), artificial neural networks (ANN), decision trees (DT), K-nearest neighbors (k-NN), and non-parametric Bayesian techniques (Crespo & Ojeda, 2017).

Even so, traditional machine learning and feature engineering algorithms are not sufficiently productive to draw out the composite and non-linear tendencies widely detected with big data. In contrast, deep learning techniques allow the employment of reasonably easier linear models for big data analysis chores, namely, categorization and forecasting (Najafabadi et al., 2015).

Deep learning bespeaks machine learning methods that wield supervised, half-supervised, or unsupervised policies to acquire hierarchical depictions in deep structures for further categorization in a self-activating manner (Chen & Lin, 2014). Self-activation of information abstraction procedures is the ruling notion behind deep learning algorithms. These sets of rules seek to resemble the human brain's capabilities for verily composite problems as well as its hierarchical knowledge acquisition methods (Najafabadi et al., 2015).

There are different deep learning algorithms, such as deep belief networks (a type of restricted Boltzmann machines), convolutional neural networks, and auto-encoders. (Chen & Lin, 2014; Najafabadi et al., 2015). Often conventional neural networks become shut in local optima of a non-convex objective function. This occurrence gives rise to deficient rendering. A deep belief network (DBN) employs a deep structure with learning depiction capabilities for both labeled and unlabeled data given to it. It includes both unsupervised pre-training and supervised fine-tuning procedures to build the models (Chen & Lin, 2014).

A convolutional neural network bespeaks many hierarchy tiers; some strata work for attribute depiction others classify using a conventional neural network formation (Chen & Lin, 2014). The term Auto-encoder (or auto-connector) stands for three-stratified networks, namely, the input tier, the hidden tier, and the output tier. These auto-encoders seek to learn input depictions in the hidden stratum to rebuild such input in the output tier (Najafabadi et al., 2015).

Although deep learning techniques have displayed wondrous outcomes in many enactments, their preparation is not an easy errand for Big Data learning to complete. The deep stacking network, the tensor deep stacking network, the large-scale deep belief networks, and the large-scale convolutional neural networks are protocols to carry out deep learning for vast information quanta (Chen & Lin, 2014).

METHODOLOGY

The presented research was a literature review, consisting of 19 published articles from 2013 to 2021. Namely, the concepts of big data and machine learning, and deep learning are discussed and analyzed throughout the paper. Furthermore, an analysis of different points of view was carried out to trace the train of thought to gather conclusions to pursue future research based on current trends or needs.

DISCUSSION

Big data bespeaks massive gathering of structureless disordered facts. As it grows to unthinking amounts; there is a need to handle this data appropriately. Many efforts have been made to extract value from big data. Namely, machine learning techniques have proven useful to process data such as support vector machines, artificial neural networks, decision trees, K-nearest neighbors, and Non-parametric Bayesian techniques among others. Yet big data require better solutions to unstructured sets of facts. There is when deep learning algorithms come to play a part in the unruly world of big data affairs. Indeed, deep learning has succeeded to this account superseding conventional machine learning practices.

It is there when it is wise to lead our efforts to apply deep learning techniques to extract value. If such a vast aggregate of facts is unable to give value, in the end, it is worthless. Even so, such value depends on the given context. Understanding the deep learning advantage to extract value could help to develop new deep learning approaches for big data handling affairs, or to improve existing deep learning methods to maximize the valuable information that results from the massive aggregates of data.

REFERENCES

Ahmad, K., JianMing, Z., & Rafi, M. (2020). Librarian's perspective for the implementation of big data analytics in libraries on the bases of lean-startup model. *Digital Library Perspectives*, 36(1), 21–37. https://doi.org/10.1108/DLP-04-2019-0016.

Bagheri, M. & Shaltooki, A. (2015) Big Data: Challenges, Opportunities and Cloud Based Solutions. *International Journal of Electrical and Computer Engineering* 5(2), 340-343.

Casarotto, E. L., Binotto, E., Malafaia, G. C., & Martínez, M. P. (2021). Big Data and Competitive Advantage: Some Directions and Uses. *Rev. FSA*, 18(1), 3–24. http://dx.doi.org/10.12819/2020.18.01.1

Chen, X. & Lin, X (2014) Big Data Deep Learning: *Challenges and Perspectives*. IEEE Access, 2 514-525.

Collymore, A., Rosado-Muñoz, F., Ojeda-Castro, A. (2017) Big Data Analytics, Competitive Advantage and Firm Performance. *International Journal of Information Research and Review*, 4(2), 3599-3603.

Crespo, G. & Ojeda, A. (2017) Convergence of Cloud Computing, Internet of Things, and Machine Learning: The Future of Decision Support Systems. *International Journal of Scientific & Technology Research* 6(7).

González, E. & Ojeda, A. (2016) Big Data and Online Social Networks: Tools for Better Use of Information on Business. *Issues in Information Systems* 17(3), 109-115.

Katal, A., Wazid, M., Goudar, RH. (2013) Big Data: Issues, Challenges, Tools and Good Practices. *IEEE Access*, 404-409 978-1-4799-0192-0/13.

Khan, M., Muhammad, F., U., Gupta, N. (2014) Seven V's of Big Data Understanding Big Data to extract Value Zone 1 *Conference of the American Society for Engineering Education* (ASEE Zone 1) IEEE 978-1-4799- 5233.

Kitchin, R. (2014) Big Data, new epistemologies, and paradigm shifts. *Big Data & Society* (Sage) 1-12.

Kulakli, A., & Osmanaj, V. (2020). Global research on big data in relation with artificial intelligence (A bibliometric study: 2008-2019). International Journal of Online and Biomedical Engineering, 16(2), 31–46. https://doi.org/10.3991/ijoe.v16i02.12617.

Najafabadi, M., Villanustre, F., Khoshgoftaar, T., Wald, R., Seliya, Muharemagic, E. (2015). Deep Learning Applications and Challenges in Big Data Analytics. *Journal of Big Data a Springer Open Journal*, 2(1).

Neaga, I. & Liu, S. (2014). The Knowledge Management Context of Cloud Based Big Data Analytics. *European Conference on Knowledge* 3, 1339.

Power, D. (2014) Using Big Data for Analytics and Decision Support. *Journal of Decision Systems Taylor & Francis Group*, 23(2), 222-228.

Ridzuan, F., Nazmee, W. M., & Zainon, W. (2022). Diagnostic analysis for outlier detection in big data analytics. *Procedia Computer Science*, 197, 685-692.

Song, M., Zhang, H., & Heng, J. (2020). Creating sustainable innovativeness through big data and big data analytics capability: From the perspective of the information processing theory. *Sustainability* (Switzerland), 12(5). https://doi.org/10.3390/su12051984.

Tinoco, J., Parente, M., Correia, A. G., Cortez, P., & Toll, D. (2021). Predictive and prescriptive analytics in transportation geotechnics: Three case studies. *Transportation Engineering*, 5.

Wang, S. & Yuan H. (2014) Spatial Data Mining: A Perspective of Big Data. *International Journal of Data Warehousing and Mining*, 10(4), 50-70.

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J. fan, Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. *Journal of Business Research*, 70, 356–365. https://doi.org/10.1016/j.jbusres.2016.08.009

COLLEGE STUDENT PERCEPTIONS, USAGE, AND ACCEPTANCE OF TECHNOLOGY

Gayle Jesse, West Liberty University, gayle.jesse@westliberty.edu
Anton Schulz, West Liberty University, aschulz@westliberty.edu

ABSTRACT

This research paper analyzed student perceptions of accepting technology in the everyday life of undergraduate college students at a small rural southern university. Specifically, it explored the perceptions and usage, and acceptance of technology. Two hypotheses were tested to determine if time changes student's perceptions of security concerns and technology usage. The quantitative study concluded that both hypotheses were nullified meaning that no effect exists in the population. Implications of the study recommend more focus on cybersecurity awareness possibly through training and if we want people to accept new technology it must have perceived usefulness as indicated by TAM (Davis, 1989). TAM was not directly/specifically used in this study as intended by Davis (1989), but was only used in this study to give more insight to why people do what they do. Limitations to this study included, participant count, population sample size, 2020 participation was lacking due to COVID, and the survey was only administered to general business, management, and CIS students. Concluding that a future qualitive study would provide the needed depth giving the richness as to why students perceive these two topics as they do.

Keywords: cybersecurity awareness, cybersecurity training, disruptive technology, perceived usefulness of information technology, higher education, undergraduate students

INTRODUCTION

The COVID 19 pandemic continues to change the lives of people in many ways. In terms of technology, technology usage has grown exponentially since the COVID-19 pandemic. Statistically speaking, internet services usage when compared to pre-lockdown is of 40% to 100% (Branscombe, 2020). Gen Z, which consists of 16–23-year-olds, the primary sample group of this study, agree to spending more time using their devices such as smartphone (82%), laptops (565), and desktops (34%; Branscombe, 2020). Pew Research Center (2021) stated the following: “90% of Americans say the internet has been essential or important to them, many made video calls and 40% used technology in new ways”. Even though individuals are exposed to and use technology, does it fully help them? Pew Research Center (2021) stated, “40% say they often feel worn out or fatigued from spending too much time on video calls, 33% have tried to cut back on using the Internet or smartphone, and 26% worry a lot or some about paying for their Internet connection”. This research paper analyzed the perceptions of accepting technology in the everyday life of undergraduate college students at a small rural southern university. Specifically, this study explored the perceptions and usage, and acceptance of technology pre, during, and post pandemic.

BACKGROUND AND LITERATURE REVIEW

The following literature review explored the existing research on this topic and what makes this research unique in nature by finding a gap in the existing literature. Thus, highlighting the importance of this research study as well as comparing the results with other similar projects.

Furthermore, the researchers wanted readers to obtain a better understanding of the terminology dealing with the survey questions. Given the broad range of explored topics within the survey questions dealing with technology, the literature review is not formatted in the typical literature review funnel. This literature review is broad in order to encapsulate the survey question concepts.

Information Technology (IT

A crucial part of existing research is defining key terms that are utilized in this student-based survey. Many of the questions were centered on the term information technology (IT). A basic definition of IT is: "It is that it's the application of technology to solve business or organizational problems on a broad scale" (Slyter, 2019). Meaning that IT has a direct and extremely important connection to all business operations. IT is typically involved in this context in every job that revolves around maintaining or expanding a business (i.e., especially in the areas of efficiency and gaining new customers).

IT Security

Another crucial term for this research is the security aspect of IT. Today, the term security can be directly connected to cybersecurity, which focuses on the digital side of security in this context (Von Solms & Van Niekerk, 2013). Therefore, focusing on cybersecurity for this specific research refers to the digital side of college students feeling protected with their information being secure. The security aspect of technology is a priority for most technology users, given the exponential use of technology. There are multiple reasons for placing security at the top of list, but the one primary reason is hacking (Tarter, 2017). As hacking gets more advanced, especially due to the expansion of quantum computing, individuals and organizations using technology are put at a higher risk for being hacked and for data breaches (Tarter, 2017). With that being said, organizations and individuals alike should be making cybersecurity a top priory and increase investment in better cybersecurity practices.

When taking a deeper look at higher education and college students as the primary sample group, it can be observed that cybersecurity is also a growing topic of concern for this group. Rahman et al. (2020) conducted a study and determined that the education system is trying to put more attention towards better cybersecurity but found that there are many challenges with teaching faculty, staff, and college students about cybersecurity. It should be noted that during our research, numerous other sources were found that supported that importance of cybersecurity education should be emphasized and concluded there are many challenges to getting users educated on safe cybersecurity practices and placing it high on the importance scale.

Technology Acceptance Model

Another key term aiding this this research study is the Technology Acceptance Model (TAM) by Davis (1989). TAM has been widely used in the academic research environment and offers a good explanation of why business and users alike are taking advantage of technology. TAM has two factors that are needed in order to be used by the stakeholders. These two technological factors are (1) ease and (2) usefulness (Davis, 1989). Therefore, technology needs to be easy to understand for the customers but also needs to have value for usefulness. TAM was not directly/specifically used in this study as intended by Davis (1989), but is only being discussed in this study to give more insight to why people do what they do.

In addition to TAM, it is necessary to analyze the difference in how current college students versus previous generations utilize technology both in their personal and college lives. Current college students have a different, closer proximity to technology and tend to accept new technology at a faster rate. Furthermore, college students tend to be a highly researched group, especially with technology. Friedman and Friedman (2013) claimed that college students and the younger generation in general, especially Gen Z, are more likely to accept new technology when comparing this to the older generations.

Web 1.0

Since this primary focus of this research project revolved around technology and overall web usage, it is appropriate to gain an understanding of web history. The first version of the web was titled "Web 1.0" and brought web users many fundamental functions. These functions include the "power of Web 1.0 to enable users to access their email from any computer and mobile devices that are connected to the Internet making email valuable in acquiring and transferring knowledge" (Dehinbo, 2010). Meaning users can access personal information in an online setting from multiple devices and locations, noting that this was one of the many key features of Web 1.0. Web 1.0's other features included the importance of property or mainly what the user can access such as websites and making changes. As far as higher education, Web 1.0 was rarely used as it was not viewed as a major benefit for this industry at this point in time.

Web 2.0

Web 1.0 was updated to Web 2.0 sometime around 2010. As with most technological updates, an update was made because of known limitations and improvements were in demand. The primary upgrade was the increased ability to be able to interact better on the web. Web interactive or "stickiness" keeps webpage visitors on a website longer and is more likely to return as the owner of it keeps the website updated on a regular basis with blogs and other interactive features (Mazzei, 2022). A second upgrade to Web 1.0 that was added to Web 2.0 was the capability of multiple people being able to contribute to a website rather than just the owner as with Web 1.0. Wikipedia is a prime example to illustrate this new Web 2.0 feature because anyone with internet access can add content to Wikipedia (Mazzei, 2022). Upon further examination, Web 2.0 had an impact on higher education. One can observe that this added technology feature would later impact higher education drastically through a shift in online learning. Learning could be both synchronous and asynchronous. "Synchronous classes run in real time, with students and instructors attending together from different locations. Asynchronous classes run on a more relaxed schedule, with students accessing class materials during different hours and from different locations" (Wintemute, 2022). As one who knows, Web 2.0 had a huge impact on higher education. Web 2.0 brought about a way to stay interactive with one another on the internet. Gupta and Seth (2014) stated that it had more benefits for social life rather than the application in higher education, but 9 years later those in any level of education, especially after COVID, know the benefits Web 2.0 brought to education.

Web 3.0

Web 3.0 is the next generation of web users and is used to some degree today, but is still in the evolving and accepting stage. As Singh, Debi, & Gulati (2011) described in their extensive study, "Web 3.0 is a term that is used to describe various evolutions of Web usage and the interactions along several paths. These include: (1) transforming the Web into a database, (2) a move towards making content accessible by multiple non-browser applications, (3) the leveraging of artificial intelligence technologies, (3) the Semantic web, and (4) the Geospatial Web, or the 3D web."

Singh et al., (2011) emphasized that Web 3.0 approaches the changes in technology by using the limitation of the previous version. Additionally, Singh et al., (2011) found that Web 3.0 is utilized in many different areas of human life. Furthermore, according to Team (2023), another important feature within Web 3.0 is Artificial Intelligence (AI). More recently, AI has become the topic of conversation and is ever present in our everyday lives. Generally speaking, the population does not fully understand the capabilities of AI from both the negative and positive perspectives. Educationally speaking, the usage of Web 3.0 already has and will have an increasing value for all levels and kinds of online education (Ohei & Brink, 2019). Finally, it can be assumed that since AI revolves around automation, Web 3.0 will have an economic advantage by saving on labor costs.

Microchipping

Another term used in this research was microchipping, as one of the research questions directly addresses this topic. Human microchipping is "typically an identifying integrated circuit device in the form of a radio-frequency identification transponder encased in silicate glass and implanted in the body of a human being" (Banafa, 2022). Human bodies can contain either active (battery) or passive (transmitter/receiver) microchips for a variety of purposes. Some of these purposes have fully supported reasons why people decide to become microchipped (e.g., typically involve getting more information about the human body and tracking certain processes). The data gathered through the microchip can provide healthcare professionals with more detailed information on health statistics; thus, assuming healthcare professionals can make more informed medical decisions due to the gathered data. Without providing too much detail, one should note there are many other purposes and for a variety of industries, but for simplicity, a general example was provided here. When looking at this research question (RQ) in detail, the RQ asks the students "If they could imagine being microchipped?" As mentioned previously, numerous research studies emphasize that young people, including college students, are more likely to accept new technology compared to the older generation (Demuth, 2010). One can assume that the TAM model could be applied to microchipping.

Disruptive Technology

Disruptive technology is an essential term to discuss for the purpose of this research study. Kostoff et al. (2004) described that disruptive technologies often disrupt the workforce, allowing one to enter in and become competitive in a new area. Overall, disruptive technologies cause a revolutionary change in doing things or a new way of doing something because of technological advances. Disruptive technologies ultimately cause change and can evolve from either a variety of diverse technologies or a new technology all together.

Education at all levels and students in general are part of an era of disruptive technologies brought upon by COVID-19. During the COVID-19 pandemic, students, teachers, and professors had to quickly adapt to how classes needed to be taught to keep students at all educational levels progressing through their current classes. This dramatic shift in learning via an online environment (e.g., Zoom, Google Classroom's, etc.) was a disruptive technology that drastically changed education by how classes were taught. More specifically, cellphones are another example of a disruptive technology, and the primary sample group of this conducted research uses on a daily basis. Disruptive technologies and TAM work together and due to the increased exposure to technology at younger ages, students in general tend to have a higher acceptance of new technologies.

METHODOLOGY

Research Design

This explanatory study was designed utilizing quantitative methods. Conducting this quantitative study involved administering over 5 years. Although the study was administered over 5 years, 2020 was impacted by COVID; thus, only one student answered the questions. The research conducted through a survey preserved an objective method. Both Sakai Learning Management System and Microsoft Excel were used to collect and then analyze the data, respectively. The survey was conducted via Sakai poll questions within each course module. Results were entered into Excel and analyzed by computing percentages.

The survey questions focused on a variety of areas to keep students engaged in the course material and to collect information on students' perceptions of technology use. The survey consisted of 14 questions with three major themes: IT and job skills, technology usage, and security. However, two of those three themes were considered in this paper, which were technology usage and security, as the third will be used separate from this publication.

Participants

This research study was conducted at West Liberty University (WLU), which is located in the Northern Panhandle of West Virginia. WLU is considered to be on the smaller side of higher education with enrollment at approximately 2,300 students. Therefore, college students were surveyed as a convenience sample group. To have a better understanding of the sample group, the following should be noted about the survey participants. The student population consists mostly of students within a radius area of 50-70 miles. The family income is low-medium when compared to the national average. Income has a direct correlation to the availability of technology for these students and does impact the results. Furthermore, an additional unique feature of the university is the location of the campus, which is in a rural area on a hilltop with no other significant businesses or high encounters with technology. It takes about 25 minutes by car to go to the next higher-populated area and the lack of utilization of technology should be considered in the analysis of the results.

Table 1: Course Enrollment Statistics

	Fall 2018	Fall 2019	Fall 2020	Fall 2021	Fall 2022	Total
Course Enrollment	25	20	14	29	31	**119**

Research Questions

RQ1: How much of an influence does time have on students' concerns for security?

H1: Students' concerns for security increase over time.

RQ2: How much of an influence does time have on students increasing their technology usage?

H2: Students' over time increase technology usage.

DATA ANALYSIS AND DISCUSSION

RQ1: Do students' concerns for security increase over time?

Security

Data have an economic impact by generating trillions of dollars every year; however, with data being available, a security risk comes with it. Therefore, survey question 4 asked "Personal data has become an economic asset. Do you think that as consumers know what their data are used for and how much it is worth will become reluctant to share data?" A 47.1% response rate was acquired for this question, resulting in mixed responses for yes, no, and maybe with each being in the 30% - 40% range. However, 37.5% of students did state that "yes" people will become reluctant to share data given what it is being used for and the value of the data. Given the response percentages, the hypothesis is false; therefore, a prediction cannot be determined if people will become reluctant to share personal data.

Q4: Personal Data Becoming Economic Asset

	2018	**2019**	**2020**	**2021**	**2022**	**2018-2022**
Yes	42% (5)	25%(1)	0	38%(5)	38% (10)	**37.5% (21)**
No	33% (4)	25%(1)	0	38%(5)	31% (8)	**32.1% (18)**
Maybe	25% (3)	50%(2)	100%(1)	23%(3)	31% (8)	**30.4% (17)**
Responses	12	4	1	13	26	**56**

In 1998, the first human microchip was used and although it had its benefits, the security risk was something to consider. Since human microchipping is growing, survey question 7 stated, "Think about the idea of microchip implants in humans. Would you get a microchip implant?" Question 7 received a 36.1% response rate. A response of 62.8% for "no" to getting a microchip implant clearly indicates a prediction that people are not in favor of getting microchipped at least for now. Leading the researchers to mention an important point to notice in the responses, which is that the "no" responses showed a decline over the 5 years since this study took place. This study did not include a qualitive portion to determine what caused the change in individuals over the 5 years. The researchers are suspecting in this study that the acceptance of microchipping correlates with technology acceptance. People tend to accept technology the longer it is around and for a variety of different reasons.

Q7: Microchip implant

	2018	2019	2020	2021	2022	2018-2022
Yes	27% (3)	0	0	0	21% (4)	**16.3% (7)**
No	73% (8)	67% (2)	0	60%(6)	58% (11)	**62.8% (27)**
Maybe	0	33%(1)	0	40%(4)	21% (4)	**20.9% (9)**
Responses	11	3	0	10	19	**43**

Cybersecurity attacks are increasing exponentially; phishing is the most common. Question 8 on the survey was centered around the growing concerns of cybersecurity, which was as follows, "Have you ever experienced some kind of cybersecurity attack, hack, or virus?" A 34.5% response rate resulted in an 87.8% "yes." Giving the researchers the ability to be able to predict that most people have experienced a cybersecurity attack because the hypothesis was proven true. Noting that most attacks are due to human error (Ahola, 2022).

Q8: Cybersecurity Attack

	2018	2019	2020	2021	2022	2018-2022
Yes	70% (7)	100% (3)	0% (0)	100% (10)	89% (16)	**87.8% (36)**
No	30% (3)	0% (0)	0% (0)	0% (0)	11% (2)	**12.2% (5)**
Responses	10	3	0	10	18	**41**

It is well-known by computer professionals that almost all internet traffic can be monitored, but what about the general population? Therefore, Question 10 asked participants, "Before this class, did you think you were being watched online?" With a response rate of 32.8%, the answer "yes" was chosen by 69.2% of the students. The response of "yes" fluctuated over the 5 years of ups and downs. The researchers hypothesized that the number would increase over the years, but this was not the case. However, one can predict that people know they are being watched online. If one knows they are being watched, does it impact what they do while online?

Q10: Being Watched Online

	2018	2019	2020	2021	2022	2018-2022
Yes	73% (8)	100% (3)	0% (0)	56% (5)	69% (11)	**69.2% (27)**
No	27% (3)	0% (0)	0% (0)	44% (4)	31% (5)	**30.8% (12)**
Responses	11	3	0	9	16	**39**

H2: Students over time increase technology usage.

Technology Usage

Question 3 begins the second half of the focus of this study which was to determine if students are increasing their use of technology over time. More specifically, question 3 stated, "Do you have one of these disruptive technologies such as Alexa or Google Home?" Question 3 had a higher response rate of 47.1%. The data gathered showed an increase from 2018–2019 to 2021–2022, which was anticipated by the researchers. However, the results overall were 42.9% "yes" and

57.1% "no." Although the "no" response was higher, the non-disparity gap between the two response percentages means a prediction cannot be determined because the hypothesis cannot be answered as true or false.

Q3: Alexa, Google Home, or Similar Devices

	2018	2019	2020	2021	2022	2018-2022
Yes	33%(4)	33% (2)	0	67%(8)	40% (10)	**42.9%(24)**
No	67%(8)	67% (4)	100(1)	33%(4)	60% (15)	**57.1%(32)**
Responses	12	6	1	12	25	**56**

Technology has influenced the video game industry. Question 5 surveyed the students with this question, "Do you like to play video games?" Another high response rate was received at 43.7%. The 65.4% "yes" response clearly indicates that we can predict that a majority of students like to play video games. Based on the increased percentages of students answering "yes" to this question, we learn that more students are playing video games. Furthermore, the researchers are assuming that if more students are playing video game, technology usage is increasing over time because more people playing means more time using technology.

Q5: Play Video Games

	2018	2019	2020	2021	2022	2018-2022
Yes	50% (7)	60%(3)	0	70%(7)	77% (17)	**65.4%(34)**
No	21% (3)	20%(1)	100%(1)	20%(2)	14%(3)	**19.2%(10)**
Somewhat	29% (4)	20%(1)	0	10%(1)	9% (2)	**15.4%(8)**
Responses	14	5	1	10	22	**52**

The authors are asserting that increase in ecommerce has a direct correlation to an individual increasing their technology usage because more time online shopping equates to more time using technology (e.g., phone or PCs). This also works in reverse that technology growth increases ecommerce growth. Therefore, question 9 asked students, "Do you buy something online every week?" A 35.3% response rate to this question obtained a result of 78.6% for "no." The researchers did not expect this result. Although these "Yes" and "NO" response percentages statistically allow us to make a prediction that college students do not purchase something online every week, the authors wonder if students considered even minor food purchases via an app on their phone when answering this question.

Q9: Purchase Something Online Weekly

	2018	2019	2020	2021	2022	2018-2022
Yes	23% (3)	0% (0)	0% (0)	33% (3)	18%(3)	**21.4% (9)**
No	77% (10)	100% (3)	0% (0)	67% (6)	82%(14)	**78.6% (33)**
Responses	13	3	0	9	17	**42**

As technology advances in cars, the way we once drove cars is changing. Question 11 asked, "Do you think we should have autonomous vehicles?" This survey question received the lowest response rate of 21%. Given the below 30% response rate, the response does not fully represent the population of students taking the survey. However, the researchers decided to proceed with sharing the results to this question. The results of Q11 were mixed with "yes," "no," and "maybe" all at approximately 30%. Therefore, the researchers cannot make predictions based on the results.

Q11: Autonomous Vehicle

	2018	2019	2020	2021	2022	2018-2022
Yes	22% (2)	50% (1)	0% (0)	14% (1)	25% (4)	**36% (9)**
No	56% (5)	50% (1)	0% (0)	29.% (2)	12% (2)	**36% (9)**
Maybe	22% (2)	0% (0)	0% (0)	57.% (4)	62% (1)	**28% (7)**
Responses	9	2	0	7	7	**25**

The use of emojis is increasing more and more with text messages. Therefore, as technology usage increases, so does the use of emoticons. Moreover, emojis are changing the way we communicate. The rising generation was raised with technology and a different way to communicate. The use of emoji technology allows oneself to express themselves as a deeper level, so question 13 asked students, "Do you have a favorite emoticon?" The response rate to Q13 was 31.1% with 64.9% of the students stating that "yes" they have a favorite emoticon. The researchers can predict that most college students have a favorite emoticon.

Q13: Favorite Emoticon

	2018	2019	2020	2021	2022	2018-2022
Yes	67% (8)	0% (0)	0% (0)	57% (4)	75% (12)	**64.9% (24)**
No	33% (4)	100% (2)	0% (0)	43% (3)	25% (4)	**35.1% (13)**
Total	12	2	0	7	16	**37**

Hypothesis

H1: Students' concerns for security increase over time.

H1 addressed RQ1 which sought to determine if time has an influence on security becoming more of a concern. Although the researchers hypothesized that a time frame of 5 years would show an increase in concern for security and technology usage, this study did not yield that result.

> H1o: There is no statistically significant relationship between time and increase concern for security.

Pew Research Center (2017) found that 64% of Americans experienced a data breach. At the writing of this study in July 2023, a quick Google search of top hits quickly reports that this percentage has not changed and it is has been almost 6 years since the Pew publication date. These finding further support the authors null hypothesis that time does not seem to impact our concerns for security. The bigger question is why, and thoughts on this as well as better practices will be discussed in the next section.

H2o: Students over time increase technology usage.

H2 addressed RQ2 which sought to determine if time has an influence on increasing technology usage. However, researchers determined that college students' technology usage did not increase over time in this particular study.

H2o: There is no statistically significant relationship between time and increase of technology usage.

This result was quite surprising to the researchers. Therefore, the authors asked themselves, why did this number not increase given the world we live in? First, the researchers wondered if the college student age group already uses technology a lot and had the researchers asked elderly individuals over the same 5 years, the results would have probably been different and shown an increased use of technology over time. Second, the researchers realized that people utilize technology for many different reasons. Czaja et al. (2006) stated that education background, careers/jobs, confidence, socioeconomic status, and the individuals over all attitude of technology all affect the use of technology. The researchers feel these reasons found in 2006 still hold true today and realize there could be many factors as to why an increase was not reported.

IMPLICATIONS FOR RESEARCH/PRACTICE

The aim of this research study was to determine if students over time have increased security concerns and technology usage. As stated in the previous section, both hypotheses were nullified and the discussion of these follows.

H1o: There is no statistically significant relationship between time and increase concern for security.

H1 revolved around four questions dealing with participants: (1) sharing their personal data, (2) human microchipping, (3) experiencing a personal cybersecurity attack, and (4) if they thought they were being watched while online. All four questions over the 5 years’ responses remained stagnant over time. The question to ask here is, why are individuals concerns for cybersecurity not increasing? The authors thought on this question and another quick Google search revealed that people are concerned but tend to rely on companies to protect them instead of trying to mitigate cyberattacks on their end. The researchers feel that the implication to take away from H1 is to have more focus on cybersecurity awareness to ensure people have concerns for cybersecurity, which reiterates that most cybersecurity attacks occur due to human error. External research has reported that removing human error results in only about 19 out of 20 cyber breaches ever happening (Ahola, 2022), which implies that cybersecurity awareness training is needed and should be a high priority at both the personal and professional level of one’s life.

H2o: There is no statistically significant relationship between time and increase of technology usage.

H2 revolved around five questions dealing with participants: (1) having an Alexa or Google Home type of device, (2) playing video games, (3) buying something online every week, (4) autonomous vehicles, and (5) favorite emoticons. Four out of the five questions over the 5 years’ responses would be up and then down or vice versa. However, three questions did change over time. Playing video games was up and having a favorite emoticon increased. Having autonomous vehicles increased in both the yes and maybe, but the no responses declined over time. Although one question predicted an increase in technology over time, it was not enough to give the researchers confidence in predicting this. Implications for H2 fall under the category of Technology

Acceptance Model (TAM) by Davis (1989). To recall, Davis (1989) created TAM stating that there are two factors when deciding to use new technology: (1) perceived ease of use and (2) perceived usefulness. Again, TAM was not directly/specifically used in this study as intended by Davis (1989), but was only referenced in this study to provide insight as to why people do what they do. Therefore, the researchers feel that the uniqueness of this study's sample group more than likely explains why this hypothesis was nullified.

The participants of this study more than likely do not see a practical usage and/or do not understand how it is used. The median income for WLU students is low as most students receive state grant funding and having a roof over their head with food on the table has precedence over having the latest technology (e.g., Alexa or Google Home). Furthermore, most college students in general do not have personal incomes that allow for the purchase of something online every week, and the WLU campus as well as its students reside in a rural area with limited internet access. The researchers assume these were the contributing factors as to why H2 was nullified. The researchers cannot comment on the second half of TAM perceived "ease of use" as survey questions were not focused on "ease of use," only usage. The nullified H2 hypothesis in this study implies that if we want people to accept new technology it must have perceived usefulness as indicated by TAM (Davis, 1989). If the new technology does not have perceived usefulness, consumers will not purchase it.

CONCLUSIONS

Future research is needed to add to the depth of this study. Therefore, the main author plans to conduct a follow-up study, but with a qualitative approach. Additional future research will reveal the results to the five remaining survey questions that were not discussed in this paper regarding the importance of IT and its role within the job market. A second future study expanding on this study is to determine if college students are distracted by using Web 2.0 applications. The reasoning for the second study is founded on the generalization that social media plays a significant role in the everyday lives of college students and can be seen at times as a distracting technology. Questioning whether Web 2.0 including social media impacts higher education in a negative or positive direction.

Four limitations were identified in this study: participant count, population sample size, 2020 COVID distribution yielded only 1 participant, and student majors only consisted of General Business, Management, and Computer Information Systems. The participant count of 119 students and an average of 43 responses between the nine questions resulted in an average response rate of 36%. Furthermore, the population sample size was small as well given that the survey was only administered to students taking a particular course and was not distributed to the entire 2,300 student population of West Liberty University. Additionally, given that this survey was administered during the 2020 COVID pandemic, only one student participated. COVID impacted our lives, so this was to be expected due to our lives feeling chaotic from not being "normal." Finally, with only three majors represented out of all majors that a typical college has to offer, it is not a good representation of all college student majors.

Overall, this study provided everyday understandings to the field of CIS through the exploration of cybersecurity concerns and technology usage amongst college students. To recap, the two research questions in this exploratory study nullified the two hypotheses, meaning that no effect exists in the population for either stated hypothesis.

RQ1: How much of an influence does time have on students' concerns for security?

H1: Students' concerns for security increase over time.

H1o: There is no statistically significant relationship between time and increase concern for security.

RQ2: How much of an influence does time have on students increasing their technology usage?

H2: Students' over time increase technology usage.

H2o: There is no statistically significant relationship between time and increase of technology usage.

Finally, this exploratory study revealed two findings or insights into the general population. First, as individuals we need to focus on cybersecurity awareness and the best way to do that is through training and/or continued learning about (1) best cybersecurity practices and (2) best cybersecurity risk mitigation tactics. Second, if a business creates a desire for people to purchase and accept new technology, it must have perceived usefulness as indicated by TAM (Davis, 1989).

REFERENCES

Ahola, M. (2022, June 17). *The role of human error in successful cyber security breaches*. unsecure Blog. https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Banafa, A. (2022, December 21). *Microchips in humans: Consumer-friendly app, or New Frontier in surveillance?* Bulletin of the Atomic Scientists. https://thebulletin.org/premium/2022-09/microchips-in-humans-consumer-friendly-app-or-new-frontier-in-surveillance/#:~:text=What%20is%20a%20human%20microchip,body%20of%20a%20human%20being.

Branscombe, M. (2020). *The network impact of the global COVID-19 pandemic*. The New Stack; 2020. https://thenewstack.io/the-network-impact-of-the-global-covid-19-pandemic/ April 14, Retrieved March 19, 2023.

Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: Findings from the center for research and education on aging and technology enhancement (create). *Psychology and Aging*, *21*(2), 333–352. https://doi.org/10.1037/0882-7974.21.2.333

Davis, F. (1989). Perceived usefulness, Perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*, 319–340. https://doi.org/10.2307/249008

Deninbo, J. (2010). Contributions of Traditional Web 1.0 Tools e.g. Email and Web 2.0 Tools e.g. Weblog towards Knowledge Management. *Information Systems Education Journal*, *8*(15), 1–13. https://files.eric.ed.gov/fulltext/EJ1146926.pdf

Demuth, L. G., III. (2010). *Accepting technology as a solution: A quantitative study investigating the adoption of technology at colleges*. Capella University.

Friedman, L. W., & Friedman, H. (2013). Using social media technologies to enhance online learning. *Journal of Educators Online*, *10*(1), 1–22. https://files.eric.ed.gov/fulltext/EJ1004891.pdf

Gupta, S., & Seth, A. (2014). Web 2.0 Tools in Higher Education. *Trends in Information Management*, *10*(1), 1–11. http://lis.uok.edu.in/Files/9ebfb2f2-5003-47a4-9dfe-d3cdcc6a2020/Journal/27936c53-e2b8-4e4d-9bd0-45466b88ad45.pdf

Kostoff, R. N., Boylan, R., & Simons, G. R. (2004). Disruptive technology roadmaps. *Technological Forecasting and Social Change*, *71*(1-2), 141–159. https://doi.org/10.1016/S0040-1625(03)00048-9

Mazzei, M. (2022). *Web 1.0*. Salem Press Encyclopedia.

Ohei, K. N., & Brink, R. (2019). Web 3.0 and web 2.0 technologies in the higher educational institute: Methodological concept towards a framework development for adoption. *International Journal for Infonomics (IJI)*, *12*(1), 1841–1853. https://infonomics-society.org/wp-content/uploads/Web-3-0-and-Web-2-0-Technologies-in-Higher-Educational-Institute.pdf

Pew Research Center. (2017, January 26). *Americans and Cybersecurity*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity

Pew Research Center. (2021, September 1). *The internet and the pandemic*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/

Rahman, N., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Singh, K., Debi, & Gulati, D. (2011, June). Technological March from Web 1.0 to Web 3.0: *A Comparative Study*. LIBRARY HERALD, 49(2), 146-157.

Slyter, K. (2019). *What Is Information Technology? A Beginner's Guide to the World of IT*. Rasmussen University. https://www.rasmussen.edu/degrees/technology/blog/what-is-information-technology/

Tarter, A. (2017). Importance of cyber security. In *Community policing-A European perspective* (pp. 213–230). Springer, Cham.

Team, T. I. (2023, April 23). *Web 3.0 explained, plus the history of web 1.0 and 2.0*. Investopedia. https://www.investopedia.com/web-20-web-30-5208698

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wintemute, D. (2022, September 28). Synchronous vs. asynchronous classes: What's the difference? TheBestSchools.org. https://thebestschools.org/resources/synchronous-vs-asynchronous-programs-courses/#:~:text=Synchronous%20classes%20run%20in%20real,hours%20and%20from%20different%20locations.

CYBER SECURITY - CHALLENGES DESIGNING THE IOT SMART GRID ARCHITECTURE

Satendra Ch. Pandey, Dayanand Sagar University, satendrachandrapandey.res-soe-cse@dsu.edu.in
Dr. VASANTHI Kumari P, Dayanand Sagar University, vasanthi-bca@dsu.edu.in

ABSTRACT

The speedy proliferation of internet of things (IoT) devices has revolutionized various industries, together with smart fleet management distribution systems, through the development of smart grids. At the same time, the integration of IoT devices into the grid infrastructure poses vastly demanding situations while considering the safety of those systems. This paper examines the demanding situation of cybersecurity in IoT grid designs and finds key areas that require attention to ensure the protection and resilience of the grid.

Studies explore the characteristics of IoT devices that make them vulnerable to cyber threats, consisting of limited computing assets, firmware vulnerabilities, and a loss of standardized security protocols. What are the factors that increase the attack surface and complicate the implementation of effective security measures to include in IoT grid design? Research delves into the specific challenges associated with securing the IoT grid infrastructure. The paper points out challenges to safeguard the caution and reliability of data transmitted between IoT devices and grid management systems.

With the emerging risk in the context of the IoT grid layout. Exploring the potential risks posed by botnets, ransomware, and different sophisticated assaults that could disrupt grid operations and compromise the availability and reliability of security offerings. Research explores the numerous industry standards techniques and solutions to address these challenges. Developing the logical multi-layered security approach with an available and adoptable security mechanism (Physical or logical) for IoT is still a challenging situation. Preventing the grid through legacy methods through network segmentation, encryption, intrusion detection structures, and software updates is not good enough.

For prevention of cyber-attacks, a great collaboration among stakeholders, grid operators, device manufacturers, and cybersecurity specialists are required to broaden standardized protection by developing frameworks and quality security practices through addressing the challenges of cybersecurity in IoT grid design. With the aid of knowledge and addressing, stakeholders need to explore and facilitate comfortable and dependable operations like clever grids, allowing the conclusion of the entire ability of IoT in the transportation region. At the same time, minimizing the risks associated with cyber threats through developing and setting up a standard security layer at an affordable and maintainable cost. Research will identify the causes and prevention mechanisms and future enhancement and challenges.

Keywords: grid designs, firmware, IoT devices, ransomware, intrusion, clever grids.
Subject classification codes: Securing the Internet of Things: Concepts, Methodologies, and

Solutions

INTRODUCTION

The transportation industry is constantly evolving, driven by technological advancements that aim to enhance efficiency, safety, and sustainability. One such technology is the Internet of Things (IoT), which has the potential to revolutionize various aspects of transportation from vehicles, infrastructure and passenger experiences. By connecting physical devices and systems through a network of sensors, actuators, and data analytics, the IoT enables the data generation, collection, and exchange of real-time information, paving the way for intelligent transportation systems (ITS). IoT in transportation holds immense promise, offering a wide array of applications and benefits [Ref 2,3]. For instance, it enables vehicles to communicate with each other (V2V) and with surrounding infrastructure (V2I), creating a connected ecosystem that enhances road safety, reduces congestion, and improves traffic management. Through IoT-enabled sensors and data analytics, transportation operators can gain valuable insights into vehicle performance, maintenance, and fuel efficiency, leading to optimize fleet management with the cost savings. Additionally, plays a crucial role in enabling smart parking systems, public transportation management, and personalized travel experiences for passengers. However, the integration of IoT in the transportation industry also brings various challenges and subjects to considerations likewise security. One of the primary challenges is ensuring the security and privacy of the IoT ecosystem [Ref 4]. With a collection of devices and integrated systems, the risk of cyber threats and unauthorized access increases. Safeguarding the transportation infrastructure, including vehicles, communication networks, and data repositories, becomes fundamental job to preventing potential disruptions and ensuring passenger safety [Ref 5].

1. LITERATURE REVIEW

Explores the research conducted on cyberattacks targeting the IoT grid, focusing on the vulnerabilities, attack techniques, impacts, and mitigation strategies. Research explore the possible device and network level vulnerabilities, attack techniques (Botnets, Malware, Ransomware, Insider threats) , impact of cyber attacks (operational breaches, cascading effects) and mitigation strategies.

1.1 System Design for Security

Moreover, the scalability and interoperability of IoT solutions are crucial factors to consider. As the number of connected devices and data volumes grow exponentially, ensuring the seamless secure integration and compatibility of various IoT components with security services becomes a complex task. Standardization efforts and the adoption of open architectures are essential to enabling interoperability between different IoT devices and systems prevention from attacks, allowing for seamless secure data exchange and collaboration across the transportation ecosystem [Ref 6].

Additionally, the design, deployment, and maintenance of IoT infrastructure in transportation require careful planning and consideration of factors such as power supply, connectivity, and data management with physical and logical security services [Ref 6]. These infrastructure related challenges including reliable network connectivity, deployment of robust sensors and actuators, and the efficient use of data analytics capabilities. Addressing these challenges is crucial for the successful implementation of security and operation of IoT solutions in the transportation industry.

In this context, this research explores the vast potential risks and security challenges associated with utilizing IoT in the transportation industry. It delves into the various applications of IoT in transportation, ranging from connected vehicles and smart traffic management to passenger experiences. Furthermore, the paper examines the key challenges, such as security, scalability, interoperability, and infrastructure considerations, which should be addressed to maximize the benefits of IoT in transportation [Ref 6].

1.2 Enhancement of Security

The adoption of Internet of Things (IoT) technology in the transportation industry brings numerous benefits, such as enhanced efficiency, improved safety, and optimized operations. However, it also presents significant challenges in terms of security. Integrating IoT devices and systems into transportation infrastructure introduces new vulnerabilities and risks that should be addressed to ensure the integrity, availability, and confidentiality of critical transportation systems. Research will examine the key challenges and considerations related to security when adopting IoT in the transportation industry [Ref 7]. Several market leaders and Small and mid-enterprise are offerings bundle of security services. High cost, complex maintenance, and no transparency are causing seamless failures with major loss. Cyber-attacks have been rated the fifth top rated risk in 2020 and become the new norm across public and private sectors. This risky industry continues to grow in 2023 as IoT cyber-attacks alone are expected to double by 2025 [Ref 8]. EMBROKER a cyber security expertise publishes Cyber Attack Statistics and Trends of 2023 which is alarming. Global spending on cyber security product and services is expected to 1 trillion comparatively in last 5 year 2015-2021.

Transportation stakeholders must prioritize security considerations from the design and development stage of IoT systems, implementing robust security measures, conducting regular security audits, and fostering a culture of cybersecurity awareness [Ref 6]. Following are the key factors and prevention methods assessed to somehow address the security challenged while adopting IoT.

Tranportation Challenges in Terms of Security – Adopting IoT

Security Challenges Factors	Source & Prevention 1	Source & Prevention 2	Source & Prevention 3	Source & Prevention 4
Cyber Threats and Attacks	ransomware attacks	data breaches	denial-of-service attacks	unauthorized control
Limited Device Security	firmware updates	strong authentication protocols	secure configuration	Device Upgrades
Data Privacy Concerns	data encryption	anonymization techniques	strict access controls	privacy regulations
Interoperability and Integration	nteroperability	integration	compatibility	functionality
Supply Chain Risk	Implementing robust supply	secure update mechanisms	vetting suppliers	regular audits
System Complexity and Dependencies	Regular security assessments	network segmentation	redundancy measures	manage and mitigate risks

Collaboration between transportation operators, IoT device manufacturers, cybersecurity experts, and regulators is essential to set up industry standards, share best practices, and develop effective mitigation strategies.

By addressing the security challenges associated with adopting IoT in transportation, stakeholders can fully use the benefits of IoT technology while maintaining the integrity, privacy, and safety of transportation systems [Ref 2] [Ref 3].

1.3 Design Model for Security

As previously mentioned, that adding the security during the IoT grid design in transportation management system is given a second thought. There may be a desire to include inside the design mode, strategies in which protection may be embedded into the gadget layout cycles. Inside the literature, there exists a diffusion of threat fashions that preceding architects have used for IT systems. One that became proposed through Microsoft has been selected to offer a design method for methodically identifying threats and vulnerabilities as well as supplying metrics for evaluating enhancements from implementing controls for the diagnosed threats. A greater certainty has a look at what we mean with the aid of danger, threats and vulnerabilities and their risking to every results.

A cyber risk refers to an incident that has the capacity to damage a gadget. Intentional threats consist of spyware, malware, adware groups or malicious moves of disgruntled personnel. Worms and viruses are automatic threats causing harm to systems. Vulnerability refers to a regarded weakness of an asset that can be exploited correctly by chance.

Examples relate to those concerning permissions of humans changed or removed at appropriate instances, record backups, hosted platform, community safety, up-to-date licenses of anti-virus software programs, and many others. Although a chance exploits a vulnerability, there is a potential for loss or damage described as the danger [Ref 21,22].

Danger = f (threat, Vulnerability)

Equation is a generalisation that Microsoft refines in its threat model.

Microsoft classifies risk events using the memory aid STRIDE (Spoofing, Tampering, Repudiation, records disclosure privateness breach or records leak, Denial of provider, Elevation of privilege).

Every danger in STRIDE is associated with a chain of vulnerabilities.

Microsoft defined threat in terms of DREAD as: Hazard = (damage + Reproducibility + Exploitability + Affected users + Discoverability)/five, wherein each parameter is normalised between. The parameters are defined as follows:

Harm: measure of the harm to the device.

Reproducibility: degree of ways reliably the vulnerability can be exploited.

Exploitability: issue to make the most the vulnerability.

Affected customers: number of customers affected.

Discoverability: measure of ease to discover danger.

DREAD can be visualised because the vulnerability degree for every related chance.

The widespread system for risk modelling used on this paper is customized from Microsoft's security improvement cycle for software program and is listed in determine five.

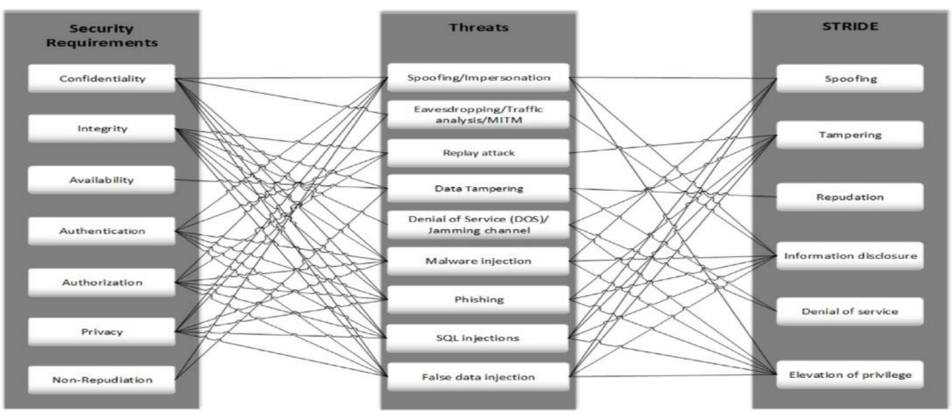
The OpenStack safety group (OSSG) has advised using DREAD metric for measuring vulnerability impact in a cloud context. It's far stated that scoring strategies the usage of STRIDE for classifying vulnerabilities and DREAD for measuring vulnerability effect are each subjective.

Reasoned judgements are to be made at the same time as keeping consistency among the rankings of more than one troubles.

2. METHODOLOGY POSSIBLE CYBER SECURITY ATTACK IN IOT GRID

Methodology provides a general framework for cybersecurity in the IoT grid of the transportation industry [Ref 13,14,15]. However, specific implementations may vary based on the unique requirements and infrastructure of each organization within the industry. "*By 2025, the global cost of cybercrime is projected to reach an estimated $10.5 trillion (INTRUSION, Inc., 2020). With 30,000 websites hacked every day (Bulao, 2022), companies of all sizes need to prioritize cybersecurity. As the prevalence and costs of cybercrime skyrocket, organizations have developed a variety of methods to model cyberthreats and assess cybersecurity risks and vulnerabilities. One of these risk analysis methodologies is DREAD, a threat modelling framework created by Microsoft* [Ref 21].

2.1 Threat Assessment: Identify potential threats and risks specific to the transportation industry's IoT grid. Assess the impact of cyber threats on critical infrastructure, such as traffic management systems, smart vehicles, and communication networks. Evaluate vulnerabilities in IoT devices, including sensors, actuators, gateways, and communication protocols Ref18].



2.2 Risk Management: Prioritize risks based on their potential impact on safety, operations, and privacy. Develop risk mitigation strategies and counter to address identified vulnerabilities. Implement risk management frameworks, such as the NIST Cybersecurity Framework or ISO 27001, to establish processes and guidelines [Ref 22].

2.3 Secure Design and Architecture: Implement secure design principles throughout the IoT grid infrastructure. Employ defines-in-depth strategies to secure network communication, data storage, and access control. Ensure that devices, gateways, and communication protocols follow industry-standard security practices. Implement encryption mechanisms to protect sensitive data in transit and at rest [Ref 7].

2.4 Identity and Access Management (IAM): Establish strong authentication mechanisms for devices, users, and administrators. Implement multi-factor authentication (MFA) to enhance access control. Regularly review and update user privileges and access rights. Employ centralized user management and access control systems.

2.5 Secure Communication: Encrypt data transmission between IoT devices, gateways, and backend systems. Implement secure communication protocols such as Transport Layer Security (TLS) or Secure Shell (SSH). Secure wireless communication channels to prevent spying and unauthorized access [Ref 6,7].

2.6 Security Monitoring and Incident Response: Deploy intrusion detection and prevention systems (IDPS) to monitor network traffic and detect anomalies. Implement security information and event management (SIEM) solutions to aggregate and analyse security logs. Establish an incident response plan to handle security incidents effectively. Conduct regular security audits, penetration testing, and vulnerability assessments [Ref 9].

2.7 Secure Software Development: Implement secure coding practices and conduct code reviews to identify and fix vulnerabilities. Employ software testing techniques, such as fuzzing and static code analysis, to identify potential flaws. Regularly update software and firmware to patch known vulnerabilities [Ref 9,10].

2.8 Employee Awareness and Training: Educate employees, contractors, and stakeholders about cybersecurity best practices. Conduct regular training sessions on identifying and mitigating cyber threats. Promote a security-aware culture to encourage reporting of suspicious activities or incidents.

2.9 Regulatory Compliance and approach: Stay informed about relevant cybersecurity regulations and standards applicable to the transportation industry. Comply with data protection and privacy regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). Engage in regular compliance audits to ensure adherence to regulatory requirements. Foster collaboration among stakeholders, including transportation agencies, IoT device manufacturers, and cybersecurity experts. Participate in information sharing initiatives to stay updated on emerging threats and best practices. Engage in industry-wide partnerships and standards development to enhance cybersecurity in the transportation sector.

3. POSSIBLE CAUSE OF IOT GRID FAILURE IN TRANSPORTATION- SECURITY BREACH?

There are several potential causes that can lead to IoT grid failures in transportation systems. These causes may vary depending on the specific implementation and circumstances, but here are some common factors that can contribute to IoT grid failures [Ref 12,13,14]:

3.1 Hardware or Software Malfunctions: Failures can occur due to defects or malfunctions in the hardware or software components of the IoT grid. This could include issues with sensors, actuators, communication modules, or control systems. Hardware failures can result from manufacturing defects "wear and tear" or inadequate maintenance. Similarly, software failures due to bugs, programming errors, or compatibility issues.

3.2 Power Outages or Interruptions: Transportation IoT grids rely on a continuous and reliable power supply to operate effectively. Power outages or interruptions, whether due to natural disasters, infrastructure issues, or technical failures, can fail IoT devices, communication networks, or control systems. Without a backup power supply or redundancy measures, the entire IoT grid may cease functioning.

3.3 Communication Network Failures: IoT devices in transportation systems rely on communication networks to transmit data and receive instructions. Network failures, such as disruptions, congestion, or equipment malfunctions, can interrupt communication between devices and infrastructure. If devices cannot effectively communicate or receive instructions, it can lead to grid failures, traffic disruptions, or compromised safety measures.

3.4 Cybersecurity Incidents: The interconnected nature of IoT devices introduces the risk of cybersecurity incidents that can compromise the IoT grid. Cyberattacks, such as malware infections, data breaches, or unauthorized access, can disrupt or compromise the operation of IoT devices and infrastructure. Attackers may exploit vulnerabilities in IoT devices or networks, leading to grid failures, data corruption, or compromised safety measures.

3.5 Lack of Maintenance and Updates: Insufficient maintenance practices, including neglecting firmware updates, security patches, or regular inspections, can contribute to IoT grid failures. Without proper maintenance, devices may degrade over time, vulnerabilities may go unaddressed, and system performance may deteriorate, leading to failures or malfunctions.

3.6 Environmental Factors: Transportation IoT grids are vulnerable to various environmental factors that can cause failures. Extreme weather conditions, temperature fluctuations, humidity, or physical damage from accidents or natural disasters can impact the reliability and functionality of IoT devices and infrastructure. Inadequate protection or resilience measures can leave the IoT grid susceptible to these environmental factors.

3.7 Human Error: Human error, such as incorrect configurations, misinterpretation of data, or improper handling of devices, can lead to IoT grid failures. Improper installation, incorrect programming, or inadequate training of personnel responsible for managing and maintaining the IoT grid can result in system malfunctions or unintended consequences.

To mitigate those capability reasons of IoT grid failures, it is vital to put into effect strong renovation practices, often replace software program and firmware, set up backup strength and redundancy measures, invest in dependable communication networks, and prioritize cybersecurity measures to shield in opposition to cyber-attacks. Additionally, enforcing tracking systems, engaging in regular inspections, and presenting comprehensive training to personnel can assist perceive and address capacity troubles before they expand into grid disasters.

4. CYBER-ATTACK EXAMPLES AND LOSSES INTO "IOT GRID" OF TRANSPORTATION

One notable cyber-attack example that targeted an IoT grid in transportation is the 2018 attack on the city of Atlanta's transportation system. The attack, known as the Sam Sam ransomware attack, affected various city services, including the transportation department. Here are some details of the attack and the losses incurred [Ref 15,16]:

4.1 Attack Method: The attackers gained access to the city's computer network and deployed the Sam Sam ransomware, which encrypted files and demanded a ransom for their release. The attack targeted the city's systems, including those associated with transportation management, causing significant disruption.

4.2 Grid Disruption: The attack disrupted several transportation services in Atlanta. The city's traffic light systems got impacted, leading to malfunctioning signals and traffic congestion. This caused inconvenience to commuters, increased traffic accidents, and led to significant delays in the transportation network.

4.3 Operational Delays: Due to the attack, the transportation department had to temporarily halt certain services and manually manage operations, resulting in significant delays and disruptions in transit schedules. This affected public transportation systems, including buses and trains, causing inconvenience, and impacting commuters' daily routines.

4.4 Financial Losses: The attack resulted in substantial financial losses for the city. Atlanta had to invest significant resources in incident response, system restoration, and cybersecurity measures to mitigate the attack's impact. Additionally, the city faced financial losses due to service disruptions, increased operational costs, and potential loss of revenue.

4.5 Reputation and Trust: The attack also had an impact on Atlanta's reputation and the public's trust in the city's transportation system. Such incidents can erode public confidence and raise concerns about the security and reliability of transportation services, potentially affecting ridership and economic activity.

4.6 Recovery and Mitigation Costs: Following the attack, the city had to allocate resources to recover and strengthen its systems. This included conducting forensic investigations, implementing enhanced cybersecurity measures, and investing in backup and recovery capabilities. These efforts incurred added costs for the transportation department and the city.

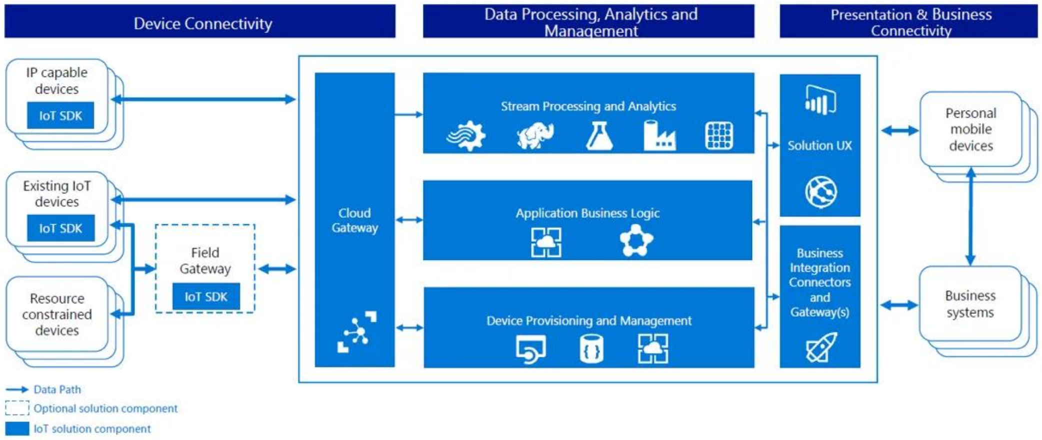


Fig1: IoT reference architecture [Ref 17]

This example illustrates how a cyber-attack on an IoT grid in transportation can have severe consequences, including disruptions to services, financial losses, damage to reputation, and compromised public trust. It underscores the importance of robust cybersecurity measures, proactive monitoring, and incident response capabilities to mitigate such attacks and protect critical infrastructure in the transportation sector.

5. CONCLUSION

In conclusion, this conference paper has explored the critical topic of cyber security in the context of IoT implementation in transportation systems. The widespread adoption of IoT technology in the transportation industry offers significant benefits, but it also introduces new vulnerabilities and risks that must be effectively managed. The paper has highlighted the various challenges and considerations related to security when adopting IoT in transportation, including cyber threats and attacks, limited device security, data privacy concerns, interoperability and integration issues, supply chain risks, system complexity, and dependencies. To address these challenges, a Multi-layered and comprehensive approach to [Ref 12,11]

With security is crucial. The paper has emphasized the importance of physical security, device security, network security, application security, data security, access control, monitoring and analytics, as well as collaboration and governance. Implementing robust security measures, conducting regular audits, and fostering a culture of cybersecurity awareness is essential for ensuring the integrity, availability, and confidentiality of critical transportation systems.

Furthermore, the paper has highlighted potential cyber security attacks and the associated losses that can occur in an IoT grid within transportation. Examples such as denial-of-service attacks, device manipulation, data breaches, man-in-the-middle attacks, firmware exploitation, physical attacks, and botnet attacks were discussed, underscoring the need for proactive defence mechanisms and mitigation strategies.

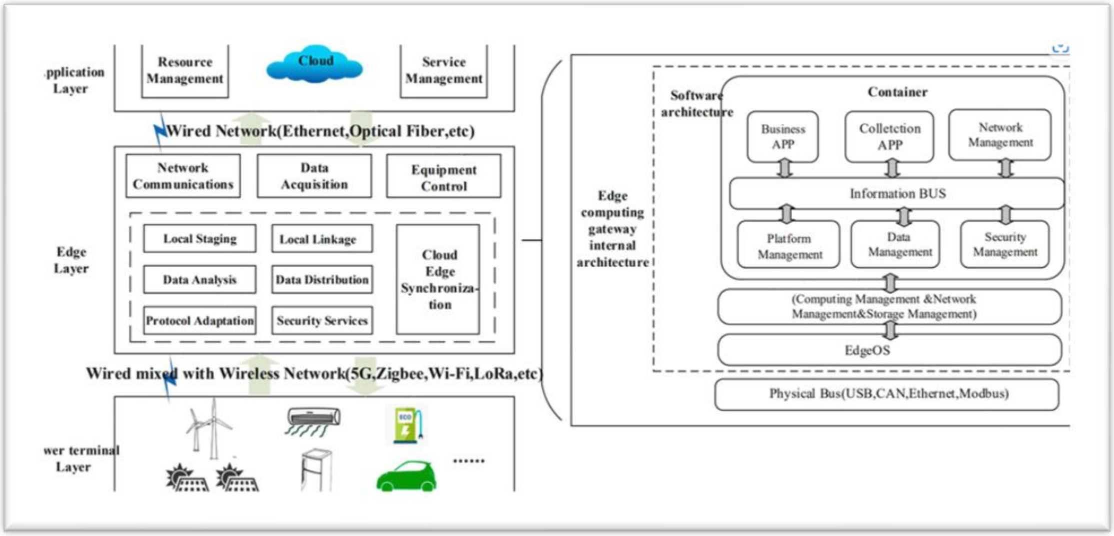


Fig 2, IoT enabled Architecture- layered [Ref 19]

The significance of addressing cyber security in IoT implementations within transportation cannot overlooked. It is imperative for transportation stakeholders, IoT device manufacturers, cybersecurity experts, and regulators to collaborate closely, establish industry standards, and share best practices to build resilient and secure IoT grids which is still missing at most area on IoT implementation. Through doing so, the transportation industry can completely leverage the potential of IoT generation while safeguarding important systems, protecting consumer privacy, and making sure the protection and efficiency of transportation operations. Destiny research on this domain should consciousness on growing advanced security answers, addressing rising threats, and further enhancing the resilience of IoT grids in transportation.
Future work for threat modelling in the IoT grid involves addressing emerging challenges and evolving threat landscapes.

6.FUTURE WORK

Here are some potential areas for future research and improvement which will be considered as key factors

Emerging IoT Technologies: As new IoT technologies and standards emerge, there is a need to develop threat modelling approaches specific to these advancements. For example, technologies such as 5G, edge computing, and blockchain introduce unique security considerations that should be incorporated into threat models.

Machine Learning and AI Threats: The increasing use of machine learning and artificial intelligence in IoT systems introduces new attack vectors. Future threat modelling efforts should consider the risks associated with adversarial machine learning, model poisoning, and evasion attacks to ensure the robustness of AI-enabled IoT systems.

By addressing these areas, future work in threat modelling for the IoT grid can help enhance the security and resilience of IoT systems, mitigate emerging threats, and ensure the safe and reliable operation of critical infrastructure

7.ACKNOWLEDGMENT

We would like to express our sincere gratitude to all individuals and organizations who have contributed to the successful completion of this conference paper on IoT in transportation and its implications for cyber security. First and foremost, we would like to thank the conference organizers for providing us with the platform to share our research findings and insights on this important topic. Their dedication and efforts in organizing this conference are appreciated.

We extend our heartfelt thanks to our supervisor/mentor Dr VASANTHI Kumari P for their guidance, support, and valuable input throughout the research process. Their ability and encouragement have been instrumental in shaping the direction and content of this paper.

We are also grateful to the participants and experts who shared their knowledge and experiences during interviews and discussions, which supplied valuable insights into the challenges and opportunities of implementing IoT in transportation systems. Their willingness to share their ability is appreciated. Additionally, we would like to acknowledge the research assistants and colleagues who have contributed to the data collection, analysis, and review process. Their diligent work and collaboration have significantly enriched the quality of this paper.

8. REFERENCES

[1] IoT Architecture for Smart Grids author Hossein Shahinzadeh and others, Ref URL https://www.researchgate.net/publication/331103655_IoT_Architecture_for_Smart_Grids
[2] Integrating IoT with Transportation Industry: Applications and Benefits, Autor Sanjeev Verma, Ref URL https://www.goodfirms.co/blog/integrating-iot-with-transportation-industry-applications-and-benefits
[3] IoT in Transportation: Solutions and Applications https://www.digi.com/blog/post/iot-solutions-for-transportation
[4] Security & Privacy Issues In The Internet Of Things (IoT) , Author Gwyneth Iredale Ref URL https://101blockchains.com/security-and-privacy-in-iot/#:~:text=You%20can%20find%20insecure%20interfaces,weak%20or%20no%20encryption%20mechanism.
[5] Cyber security challenges for IoT-based smart grid networks Author Kenneth Kimani and others Ref URL https://www.sciencedirect.com/science/article/abs/pii/S1874548217301622
[6] Reliable and secure data transfer in IoT networks , Autor Sarada Prasad Gochhayat and others ref URL https://link.springer.com/article/10.1007/s11276-019-02036-0
[7] Security in Internet of Things: Issues, Challenges and Solutions, Author Irfan Umar and others, Ref URL https://link.springer.com/chapter/10.1007/978-3-319-99007-1_38
[8] EMBROKER study about the cyber security trend ref URL https://www.embroker.com/blog/cyber-attack-statistics/

[9] Edge Computing Application, Architecture, and Challenges in Ubiquitous Power Internet of Things author Dongqi Liu1 and others ,Ref URL https://www.frontiersin.org/articles/10.3389/fenrg.2022.850252/full
[10] Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures author Xing Liu and others, Ref url https://ieeexplore.ieee.org/document/8730298
[11] White papers and reports "Creating secure IoT device identities"– Intertrust Technologies – Ref URL https://link.springer.com/article/10.1007/s11276-019-02036-0https://www.intertrust.com/resources/secure-iot-device-identities/thank-you/?submissionGuid=bc6f6ce5-4450-4225-8509-1777b3113720
[12] E Book - IoT for Smart Grids by Kostas Siozios, Dimitrios Anagnostos, Dimitrios Soudris, Elias Kosmatopoulos, Published by Springer Cham https://www.intertrust.com/resources/secure-iot-device-identities/
[13] Smart Fleet Management System Using IoT written by Priya Singh; Milind Sukram Suryawanshi; Darshana Tak, published by IEEE, Ref URL https://ieeexplore.ieee.org/document/9033578
[14] Cybersecurity in Intelligent Transportation Systems author Plovdiv Branch, Ref URL https://www.mdpi.com/2073-431X/9/4/83
[15] Smart grid security: Attacks and defense techniques author Yoonjib Kim and others, Ref URL https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/stg2.12090 , https://doi.org/10.1049/stg2.12090
[16] A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services author Ioannis Stellios and others, Ref URL https://ieeexplore.ieee.org/document/8410404
[17] IOT reference arcature https://medium.com/@prashunjaveri/an-iot-reference-architecture-fcf1fa0a347
[18] Ref fig Threat modelling of the IoT-enabled Smart Grid ref URL https://www.sciencedirect.com/science/article/pii/S0045790622007066
[19] An Architecture for IoT-Enabled Smart Transportation Security System: A Geospatial Approach Author Jun Zhang, Yichuan Wang, Shuyang Li, Shuaiyi Shi ref Url https://eprints.whiterose.ac.uk/169840/1/An%20Architecture%20for%20IoTEnabled%20Smart%20Transportation%20Security%20System.pdf
[20] SMART Grid security challenges ref URL https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/securing-smart-grid
[21] DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis Ref url - https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/
[22] ISO 27001 vs. NIST Cybersecurity Framework ref URL- https://www.onetrust.com/blog/iso-27001-vs-nist-cybersecurityframework/#:~:text=Operational%20stage%20and%20technical%20level,attempting%20to%20mitigate%20a%20breach.

9. ABBREVIATIONS AND MEANINGS

ITS - intelligent transportation systems
V2V - vehicles to vehicles

V2I) - vehicles to infrastructure
SIEM - Security information and event management
DDoS - Distributed Denial-of-Service
IDPS - Intrusion detection and prevention systems
LoRA - short for long range
NB-IoT - Narrowband-Internet of Things
4G - fourth-generation wireless
USB - Universal Serial Bus
CAN - Controller Area Network
MODBUS - a data communications protocol
OSSG - OpenStack safety group
TLS - Transport Layer Security
SSH - Secure Shell
EDGE - Enhanced Data rates for GSM Evolution
GDPR - General Data Protection Regulation
CCPA - California Consumer Privacy Act

AN ANALYSIS OF VIRTUAL MEMORY ADDRESSING AS A POTENTIAL VULNERABILITY WITHIN LINUX OPERATING SYSTEM

Erich Rice, St. Cloud State University, eprice@stcloudstate.edu
Paul Safonov, St. Cloud State University, psafonov@stcloudstate.edu
Dennis Guster, St. Cloud State University, dcguster@stcloudstate.edu

ABSTRACT

Malicious actors are an ever-present threat to organizations and their systems and applications. Although many of the attacks are focused on the weakest link in information security, the human end-users, those attacks are not the only threat needed to be protected against. Less sophisticated hackers use application layer-based attacks like phishing emails or browser-based exploitations to try and thwart an organization's defense. However, a more capable hacker or malicious group could try to utilize techniques which allow more stealthy extraction and exfiltration of data. These actors could seek to harvest data from memory, thereby potentially being able to bypass security controls placed to prevent and/or log these activities. If the data were to be directly accessed from the real or virtual memory, a malicious actor could access the information they seek while not raising any alarms or efforts to eliminate their attacks. These attacks could also prove to be very useful if carried out on shared computing hardware in which the malicious actors are able to gain access to their targets systems, an example of which would be a public computing cloud where multiple entities share the physical hardware resources through a virtualized environment of hosts and servers. In this paper we perform an analysis of memory within the Linux operating system and try to determine whether virtual memory addressing can be found and utilized by a potential malicious actor using commonly available utilities.

Keywords: data buffer, cybersecurity, linux, utilities, virtual memory

INTRODUCTION

Malicious actors are constantly looking for ways to access and potentially compromise confidential or private data. Often, the easiest method to compromise a system or application is a major consideration for them to consider (Chng et al., 2022). Another thing to consider is the potential of detection in their attempt to access the data, usually if a file system or database are attacked, they will typically be logged and an alert created (Tayag, De Vigal Capuno 2019).

An option for malicious actors to attempt to bypass alerts and the logs they create is to use a lower-level feature of the computing system and access the data directly from the memory. This method is more complex than the attacks at the application layer, such as through phishing emails and the use of malware and malicious web links, however once they are developed and proven they are well shared and become viable for more skilled hackers (Koon, 2022). Therefore, these types of attacks should not be taken lightly by organizations and are backed up by the nearly 70% of Microsoft security issues being memory safety related as found in Cimpanu, 2019. This type of scenario is especially of concern when it occurs on the servers hosting backend services. As an example, a Linux host could be acting as a server used to support an organization's electronic commerce system to facilitate the sale of goods or services online. In this example, the data of multiple potential clients could be potentially compromised if the Linux host is compromised, and its memory mined for useful information.

A good summary of how memory is allocated on a Linux host can be obtained by using the "free -h" command (Linuxize, 2020). In Figure 1 below taken from a Linux host on the authors' private computing cloud, the key is the first row that delineates the real memory. In that row it is found that the system has 31 GB of total real memory.

user@eros2:~$ free -h

total	used	free	shared/buff	cache	available	
Mem:	31G	694M	24G	21M	5.9G	30G
Swap:	8.0G	0B	8.0G			

Figure 1: Existing Memory Allocation on Test System

However, only 694 MB are in use, leaving 24 GB of memory free. Of interest to this paper is the fact that there are 5.9 GB allocated for buffers and cache. In both cases, the use of a buffer and cache, are used to speed up the processing of data. A good example of a buffer would be the process of reading data from a sequential file from the disk, this process can be seen in Figure 2 below. Disk access, even on a solid-state drive (SSD), is significantly slower than reading directly from memory. So, the read request goes directly into memory from disk and the process then pulls from the buffer speeding up the process. However, the process from the disk to the buffer is on-going and the read from the buffer goes on when the process gets the interrupt. The assumption is that the process may have to go through a series of wait states caused by reading other files, waiting for human input, or writing to a log file.

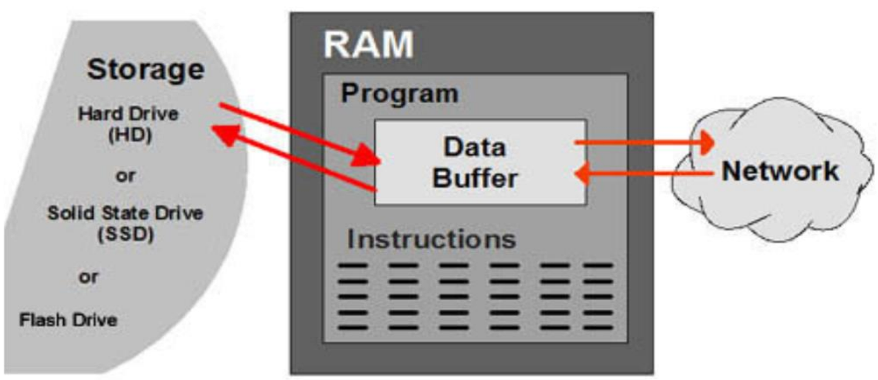


Figure 2: How a Memory Buffer Works (*Definition of buffer,* n.d.*)*

In the case of memory cache, also sometimes called a "CPU cache", information is either read or written quickly to the cache and periodically the cache is cleared (*Definition of cache,* n.d.). After this process has been completed then the cache space can then be reused. It is possible to evaluate some of the characteristics of a file that has been placed in memory on a Linux host. In the example below in Figure 3, a simple java program creates a file called Data.txt and two lines are sent to that file.

```
user@eros2:~$ java ReadWriteZ

Type characters to write in File – Press Ctrl+z to end

Line 1: ps

Line 2: this file contains Data
```

Figure 3: Java program on Test System

However, when we look in the memory using the command "lsof" (Zivanov, 2022) at the open file for the PID (process identification number) 22177 there is no data in the file as indicated by the 0 in italics as seen below in Figure 4.

user@eros2:~$ lsof -p 22177

java 22177 user 6w REG 0,52 *0* 27659826 /rhome/user Data.txt (10.10.3.5:/exports/rhome)

A check on the file system level also reveals that no data has been written as well.

user@eros2:~$ ls -l /rhome/user Data.txt

-rw-r--r-- 1 user professors *0* Nov 10 11:46 /rhome/user/Data.txt

After closing the java program, the data is then written to the file.

user@eros2:~$ cat Data.txt

Line 1: ps

Line 2: this file contains Data

Figure 4: "lsof" Command output on Test System

From the example above in Figure 4 the data is initially going into a memory buffer, and that buffer could be contained in real memory. As the "free" command displayed earlier, it has indicated there were 5.9 GB allocated by the operating system for that purpose. However, it is also possible that the initial location of the data could have been in virtual memory. Regardless, it is hoped that the data that is stored in the memory will not be compromised by a potential hacker. For a malicious actor to access the data in memory they would need to know the relative address of the memory storage area where the data resides. The structure of the memory addresses is expressed as a hexadecimal number, which represents the relative bit address of the data. In some cases, those addresses are fixed, while in other cases (especially when involving virtual memory) those address can vary (Sterling, Anderson, & Brodowicz 2018). In a 64-bit architecture computer, the memory addresses range from 0000000000000000 to ffffffffffffff or 16^16 possible bits (Vostokov, 2023). So even with fixed addressing, guessing where data might be stored is not a trivial matter for a malicious actor seeking certain data. With virtual memory the addresses are likely to change from execution to execution (Sterling, Anderson, & Brodowicz 2018), thus finding a virtual memory address to attack may have a very limited and short lifespan.

However, the processes also need to know where the data is stored so it can map to the data that it needs to continue to operate within the operating system. In the example below in Figure 5, one can see the memory segments related to the process ID 21087. Obviously, this is still a lot of memory to evaluate on a trial-and-error basis to find what you are looking for.

```
user@eros2:/proc/21087/map_files$ ls

55f0371b3000-55f0371bb000  7fe994f19000-7fe994f1b000  7fe995137000-7fe995138000
7fe99513f000-7fe995140000 55f0373ba000-55f0373bb000  7fe994f1f000-7fe994f48000  7fe995138000-
7fe995139000  7fe995140000-7fe995147000
```

Figure 5: PID Memory Segments on Test System

To investigate the probability of a hacker finding the memory address of potentially sensitive data contained in either real or virtual memory, the example that follows uses an existing sequential file and appends data to it. Of course, the file could be attacked directly, however the probability of an attack like that being detected is quite high. So, the rationale of a hacker reading the sensitive data from memory would be that it would be stealthier, thus resulting in a lower chance of detection and an alert being raised. In Figure 6 seen below, the file "filexyz" is opened and appended to by using the Linux "cat" command.

```
user@eros2:~$ ls file*

file2011b  fileEX   filetcp483  filetoremove2  filexyz

user@eros2:~$ cat >> filexyz

sample output

more sample output
```

Figure 6: File “filexyz” on Test System

By looking at the "io" file for process PID 21087 in Figure 7 one can see that 36 characters have been appended to the file but note that the write bytes value is 4096 Bytes, which matches the page size currently being used by the Linux operating system. This allows for cleaner addressing and allocation of memory.

```
user@eros2:/proc/21087$ cat io

rchar: 4979

wchar: 36

syscr: 13

syscw: 4

read_bytes: 0

write_bytes: 4096

cancelled_write_bytes: 0
```

Figure 7: “io” File for PID 21087 on Test System

It is also possible to see if the file is open in conjunction with the process PID of the application. To do so, the list open files command “lsof” can be used (Zivanov, 2022), see Figure 8 below. The file "filexyz" shows up as a regular file containing 62 Bytes of data at this point. Also of note is the fact that it is not currently on the Linux host, but on another host as indicated by the private "10.10.3.5" IP address as the file is housed on an NFS (Network File System) server in the same private cloud environment. This hopefully would make it more difficult for a hacker to attack the file system directly, however it is important to remember that data will be temporarily stored in memory on the host computer prior to being sent across the network to the NFS server for storage.

```
user@eros2:~$ lsof -p 19798 | grep filexyz

cat     19798 user    1w   REG   0,52       62 27659830 /rhome/user/filexyz (10.10.3.5:/exports/rhome)
```

Figure 8: “lsof” for File “filexyz” for PID 19798 on Test System

To determine if the file is in real or virtual memory the "vmtouch" command can be used to ascertain its location (Carrigan, 2020). In Figure 9, we check to see if it is in virtual memory, however it is stored in one page of memory, and it is in real memory. Then the “filexyz” file is "touched" into virtual memory once again taking up one page of 4KB of memory within the virtual memory space. On a side note, it is also possible to remove a file from virtual memory again using the "vmtouch" command (Carrigan, 2020).

```
user@eros2:~$ vmtouch -v filexyz
filexyz
         Files: 1
    Directories: 0
  Resident Pages: 1/1  4K/4K  100%
        Elapsed: 0.001655 seconds
user@eros2:~$ vmtouch -vt filexyz
filexyz
         Files: 1
    Directories: 0
  Touched Pages: 1 (4K)
        Elapsed: 0.001412 seconds
user@eros2:~$ vmtouch -ve filexyz
Evicting filexyz
         Files: 1
    Directories: 0
  Evicted Pages: 1 (4K)
        Elapsed: 0.001375 seconds
```

Figure 9: "vmtouch" for File "filexyz" on Test System

A logical first step a hacker might take to try and resolve the actual relative address in memory is to take advantage of some of the files in the /proc directory. In Figure 10 below for process 30463 the entries for the "cat" command used to open and allow appending to the file "filexyz" are displayed. Note that it provides a beginning and ending relative bit address range in hexadecimal. The first line deals with execution related activities for the file. The second line with reads and the third line with writes to the file. In all lines the memory is protected to prevent overwrites as indicated by the "p" flag.

```
user@eros2:/proc/30463$ cat smaps | grep /bin/cat
5647a41e3000-5647a41eb000 r-xp 00000000 08:02 1310762       /bin/cat
5647a43ea000-5647a43eb000 r--p 00007000 08:02 1310762       /bin/cat
5647a43eb000-5647a43ec000 rw-p 00008000 08:02 1310762       /bin/cat
```

Figure 10: "vmtouch" for File "filexyz" on Test System

It is interesting to note that in line 3, if one subtracts the beginning address from the ending address a value of 1000 hex is obtained. If converted to decimal this would be a value of 4096 or 4KB. By coincidence could this be the 4KB page that contains the buffered data for the file "filexyz"? If so, it may be at risk and a hacker could use a program such as “gdb” to debug it and to read its contents (Stallman et al., 2002).

Below in Figure 11 an attempt is made to use the “gdb” debug program to dump the 3rd memory segment range from above (5647a43eb000-5647a43ec000) using the rights profile of the user that owns that process ID. However, this results in a “Cannot access memory” error.

```
user@eros2:/proc/30463$ gdb

GNU gdb (Ubuntu 8.1.1-0ubuntu1) 8.1.1

(gdb) dump memory ~/catlog 0x5647a43eb000 0x5647a43ec000

Cannot access memory at address 0xa43eb000
```

Figure 11: “gdb” Command Output on Test System

From the example above one can see that finding the address of memory within the Linux operating system is quite possible. Its design is predicated on providing functionality to the system administrator and developers creating applications to be run on it. However, finding an address is one thing, but being able to compromise the data at that address is another. Remember that with virtual addressing the addresses are constantly changing so right off the bat there is a limited window of opportunity for a hacker to take advantage of it. There are also several other built in security precautions as well, most notably related to user rights on the profile level.

Therefore, the purpose of this paper is to evaluate the possibility of data being found in a buffer or virtual address space and being compromised by a malicious actor. The experiments will be discussed from three different rights levels: user/owner, root and kernel module related.

METHODOLOGY

In the introduction an address was found in memory and an attempt was made to try to read that data, though to no avail when using the user level of rights on a Linux system. However, that experiment was then rerun and the sudo command was used to provide root level rights. Once again, the data could not be read using the “gdb” command. Thus, a user space process, even running as root, is still limited in what it can do as it is running in "user mode" and the kernel is running in "kernel mode" which are distinct modes of operation for the CPU itself. In kernel mode a process can access any memory or issue any instruction. In user mode (on x86 CPUs there are several different protected modes), a process can only access its own memory and can only issue some instructions. Thus, a user space process running as root still only has access to the kernel mode features that the kernel exposes to it (Kernel Self-protection, n.d.).

Thus, even the use of the root user has its limitations. Those limitations are imposed by the design of the operating system to differentiate between user space and kernel space. For instance, even though you are a root user, you can't change the speed at which the hard disk rotates if that option isn't provided to you through the driver (you can write a driver that will allow the function, but even then you are not accessing the hardware directly but through the driver), the reason for this is that the actual control of the hardware is all done in kernel space and the way user space accesses it is through system calls.

Note below that when the "gdb" command was run via "sudo" that the address is slightly different than from the previous example. This is because virtual memory is currently being used. So therefore, a hacker trying to use past addressing of a process would be stymied due to the dynamic nature of the virtual memory addressing.

```
user@eros2:~$ sudo gdb

(gdb) dump memory ~/catlog 0x000055c7b524c000 0x000055c7b524c100

Cannot access memory at address 0xb524c000
```

Figure 12: "sudo gdb" Command Output on Test System

One might find this situation confusing because one is often taught erroneously that the root has all rights everywhere. Further, it is often taught that if the root doesn't have the rights needed that it has the right to give itself those rights. All of this is true except in entities controlled by the kernel module (Wazan et al., 2022).

To illustrate this concept, one might look at a zombie process, a zombie process refers to any process that is essentially removed from the system as "defunct", yet still resides in the CPU's memory as a "zombie". As one might expect a zombie process is one that cannot be killed even by using the root and the "kill" command with the "-9" option (Linuxize, 2019). So, if the root owns an apparent process that is a zombie, and if that is killed the zombie process would usually be killed as well. However, because the zombie process is often left over from some kernel function such as a remote procedure call to install the NFS client on a host the process is then owned by the kernel module and hence the root cannot directly kill it.

Fortunately, from a security perspective this concept of kernel ownership carries over to various memory segments as depicted in the example below in which not even the root can read the selected memory address. By using the program from (Kannan, 2018) it is possible to determine the virtual address of a memory variable and later link that virtual address to the actual physical address. When the C executable file named (vm-addr) is run the process ID of that executable is returned along with a virtual memory address.

```
user@eros2:~/OLDHOME$ ./vm-addr

my pid: 29675

virtual address to work: 0x55dcd9526260


user@eros2:~$ ps -al

F S    UID        PID   PPID  C  PRI  NI ADDR SZ  WCHAN  TTY    TIME      CMD

0 S 1895401321 29675  28848  0   80    0 - 1129        wait_w  pts/0  00:00:00  vm-addr
```

Figure 13: "vm-addr" and "ps al" Command Output for PID 29675 on Test System

Once the program executes it remains in a wait state, as seen in Figure 13 for the "ps al" command, so that one can evaluate the memory area. So, then step one is to ascertain if the virtual memory area can be accessed using the debug program "gdb". However, as is shown in the output below in Figure 14 it cannot be found using the debug program as it again provides a "Cannot access memory" error.

```
(gdb) dump memory ~/vmmemlog 0x55dcd9526260 0x55dcd9526360

Cannot access memory at address 0xd9526260
```

Figure 14: "gdb" Command Output on Test System

Step two then is using the second program found on the East River Village utilities (mem-addr) from (Kannan, 2018), this is used to get access to the physical address for the memory variable, see Figure 15 below.

```
user@eros2:~/OLDHOME$ ./mem-addr 30004 0x562c0bb28260

getting page number of virtual address 94747174797920 of process 30004

opening pagemap /proc/30004/pagemap

moving to 185053075776

physical frame address is 0x0

physical address is 0x260
```

Figure 15: "mem-addr" Utility Output on Test System

Step three is then to determine if that memory can be accessed from both a user and root level using the "gdb" debug program. However, once again the memory is protected because it is effectively owned by the operating system kernel.

```
**(For both user and root accounts)**

(gdb) dump memory ~/phyaddlog 0x260 0x270

Cannot access memory at address 0x260
```

Figure 16: "gdb" Command Output for User and Root on Test System

Even though certain ranges of memory addresses are protected, it is sometimes possible to gain access to data via registers and their related addressing. To illustrate this concept a C executable named "add" is run and returns the process PID 30222 as seen in Figure 17 below.

```
user@eros2:~/OLDHOME$ ./add

Enter the number of integers you want to add

3

Enter 3 integers

4

5

user@eros2:~/OLDHOME$ ps -al

F S      UID         PID    PPID  C  PRI  NI ADDR SZ WCHAN  TTY      TIME     CMD

0 S 1895401321 30222  28848  0   80      0 - 1128       wait_w    pts/0    00:00:00   add
```

Figure 17: "add" Program "ps -al" Command Output on Test System

The utility asks for input via the keyboard and note that the last value entered is an ASCII "5" followed by the enter key. Also, note that the process is still running because only two integers have been entered instead of the three indicated in the first stage. Again, this provides an opportunity to examine memory addressing related to this program.

Again, using the "gdb" debug program it is possible to get a summary of the registers and their associated addresses for this utility. This follows on the logic that was developed in (Farra, Guster, & Rice, 2017), where the source index register (rsi) is shown to contain the buffered data from keyboard entries. Which based on its name, the index contains what you would expect to see, for clarification on how it morphed from its original purpose see (Intel 64, rsi and rdi registers, 2014). The "info registers" command shows the starting relative address of the register related to the add program, which is running as process ID 30222. Note that root access was needed to do this as depicted using the "sudo" command. Next, the first 16 Bytes of that register are dumped to a file called "regmem22".

```
user@eros2:~/OLDHOME$ sudo gdb -p 30222

(gdb) info registers

rsi          0x1bd6670       29189744

(gdb) dump memory ~/regmem22 0x1bd6670 0x1bd6680
```

Figure 18: "sudo gdb" Command Output for PID 30222 on Test System

The contents of that file can now be evaluated using the "xxd" (hexadecimal dump) command (Sharma, 2023). As seen in Figure 19, the first two characters of the dump are "35" which is an ASCII "5" the next two characters are ASCII "0a" which is a carriage return (or enter) on the keyboard. Off to the right in the interpreted part one can see that the "35" is depicted as a "5". While this only provides a piece of potentially sensitive data a bot could be programmed to record each data chunk as it happens and store them in a file to be read later. There are of course other registers that could be monitored and potentially compromised as well, but this concept provides the basic scenario.

```
user@eros2:~/OLDHOME$ xxd ~/regmem22

00000000: 350a 0000 0000 0000 0000 0000 0000 0000  5..............
```

Figure 19: "xxd" Command Output on Test System

The next question that needs to be addressed then is, will putting an open file that that is in append mode in virtual space defeat compromising its data via the register attack scenario used above? In this example seen in Figure 20, a file called Data.txt containing 26 Bytes is appended to via the keyboard using the "cat" command.

```
user@eros2:~/OLDHOME$ ls -l Data.txt

-rw-r--r-- 1 user professors 26 Jan  3  2023 Data.txt

user@eros2:~/OLDHOME$ cat >> Data.txt

this is more data.

cat     21120 user    1w   REG   0,52       45 27660056 /rhome/user/OLDHOME/Data.txt
(10.10.3.5:/exports/rhome)
```

Figure 20: "ls -l" and "cat" Command Output for "Data.txt" File on Test System

The file then shows up as a regular open file. Next, the file is placed in virtual memory using the "vmtouch" command which was used earlier. This provides another level of abstraction regarding the true memory address of the data contained therein, see Figure 21 below.

```
user@eros2:~/OLDHOME$ vmtouch -vt Data.txt
Data.txt
[O] 1/1
    Files: 1
    Directories: 0
    Touched Pages: 1 (4K)
    Elapsed: 0.001294 seconds
```

Figure 21: “vmtouch -vt” Command Output for “Data.txt” File on Test System

By using “gdb” debug as before, see Figure 22 below, it is possible to ascertain if all the data is hidden. The same logic as used in the prior example is applied herein and an address for the rsi register (which is being used as a keyboard buffer) is obtained. Note the hex address returned is different than in previous examples seen above. This is a good characteristic of the memory management of the Linux operating system.

```
(gdb) info registers
rsi          0x7f37f9297000   139878380171264
```

Figure 22: “gdb” Command Output for “Data.txt” File on Test System

As seen in Figure 23, the initial 48 Bytes of the register are dumped to a file called “vmtouchfile” (2nd address is 30x higher). When reading this file, it turns out that the register is unaffected by placing the online file in a new virtual memory space. By looking at the interpreted portion of the dump one can see that the line "this is more data" is in fact readable. Again, by monitoring the ongoing transactions of the rsi register, data being written to the file Data.txt could potentially be compromised.

```
(gdb) dump memory ~/vmtouchfile 0x7f37f9297000 0x7f37f9297030
user@eros2:~$ xxd vmtouchfile
00000000: 7468 6973 2069 7320 6d6f 7265 2064 6174  this is more dat
00000010: 612e 0a00 0000 0000 0000 0000 0000 0000  a...............
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

Figure 23: “gdb” Command for “vmtouchfile” Output on Test System

RESULTS

These results illustrate an interesting property about computers. It shows that data is often stored in several places before it reaches its ultimate destination, in this instance via the NSF service across the internal network of a private cloud to a SAN (Storage Area Network), as well as on the

Linux host the file was being manipulated on. Further, some of that data is retained along the way. A good example of this is the propensity to create multiple replications of data in cloud computing. Other examples might be data contained in the keyboard or print buffers on a local host computer.

A computer system is really a series of devices that are often operating at different speeds, hence the need to buffer data by various means. In the latest example, the online file's ultimate destination was hidden space in within virtual memory. However, the data had to go from the keyboard to a register before it got to that point and hence was potentially vulnerable until it got to the hidden space within the virtual memory it ultimately reached.

Therefore, simply using virtualization or virtual memory to obscure the location of data is not to be considered as a viable nor comprehensive security strategy. The literature shows that the use of a multilayered security approach is of the utmost importance and certainly this is an imperative strategy (Koon, 2022). However, it may need to go beyond the rights of users that can access the sensitive data of an organization, as many IAM (Identity Access Management) regimes are currently set up in enterprises (Hummer et al., 2016). The results herein indicate that monitoring memory usage and low-level access to data also merit consideration in a comprehensive security strategy, especially within a public cloud computing environment, which many organizations have moved towards over the course of the last decade and a half.

DISCUSSION

As has been pointed out, the threat to modern information systems and applications will continue to be a major concern for organizations moving forward. Although some organizations still host much of their information technology infrastructure on-premises, most larger organizations have now moved to cloud computing environments such as Amazon AWS, Microsoft Azure, and Google to name a few. This continued move towards cloud computing, especially via large public cloud providers means that organizations will usually not have direct control over the hardware that their systems and applications reside on whether they be in a virtualized or containerized environmenr. Although the large cloud providers provide a good amount of physical and network security, they may not be considering potential memory level attacks on the physical devices themselves. Often you may not realize who your “neighbor” is that cohabitates on the physical machines your virtual machines reside on in in the cloud computing environment. Therefore, the ability to protect against potential memory level attacks becomes an even more crutial thing to be aware of and protect against. If a malicious actor was able to gain access to an on-premises server how much data could they possibly collect? But if that same server was hosting multiple organizations’ sensitive confidential data, then the potential repercussions could be even greater, as in a public cloud computing environment with shared physical resources. If a hacker was able to mine the memory on the physical machine the results could be quite damaging. Although most of the current attacks are centered at the application layer, the Verizon DBIR (Data Breach Investigations Report) typically lists phishing emails as the cause of roughly 80% of data breaches year-over-year, these types of attacks are not the only threat that organizations need to protect themselves against (Verizon, 2022).

The ability to monitor and place protections against the potential theft of data via memory mining or leakage is also a critical security control that organizations need to be aware of and put in place.

More competent hackers or hacking groups might also make use of memory-based fileless methods, such as an Excel spreadsheet file embedded with macros or a website running Adobe Flash to carry out attacks that could be undetectable by conventional defenses, such as the (WAF) web application firewall or some form of endpoint protection, though this would still be delivered typically via an email. Without an adequate amount of cybersecurity in place, malware could be allowed to infect systems without end-users knowing it has occurred. Because of the nature of computer memory, organizations need to know memory-based attacks can be a potential threat vector that they need to be aware of, and place necessary controls and countermeasures in place to monitor and alert if malicious attacks do arise.

REFERENCES

Carrigan, T. (2020, June 10). *Linux commands: Exploring virtual memory with vmstat*. Enable Sysadmin. Retrieved February 19, 2023, from https://www.redhat.com/sysadmin/linux-commands-vmstat

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Cimpanu, C. (2019, February 11). *Microsoft: 70 percent of all security bugs are memory safety issues*. ZDNET. Retrieved March 18, 2023, from https://www.zdnet.com/article/microsoft-70-percent-of-all-security-bugs-are-memory-safety-issues/

Definition of buffer. PCMAG. (n.d.). Retrieved February 10, 2023, from https://www.pcmag.com/encyclopedia/term/buffer

Definition of cache. PCMAG. (n.d.). Retrieved February 10, 2023, from https://www.pcmag.com/encyclopedia/term/cache

Farra, H., Guster, D. & Rice, E. (2017). Security Concerns of Registers in Linux Hosts: Using Debug to Find Memory Addresses of Sensitive Data. Proceedings of MICS 2017, https://www.micsymposium.org/mics_2017_proceedings/docs/MICS_2017_paper_2.pdf

Hummer, M., Kunz, M., Netter, M., Fuchs, L., & Pernul, G. (2016, August 15). *Adaptive identity and access management-Contextual Data Based Policies - EURASIP Journal on Information Security*. SpringerOpen. https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-016-0043-2

Intel 64, rsi and rdi registers. (2014, April 29). Retrieved February 16, 2023, from https://stackoverflow.com/questions/23367624/intel-64-rsi-and-rdi-registers

Kannan, B. (2018, March 2). *Virtual memory to physical memory*. East River Village. Retrieved January 11, 2023, from https://eastrivervillage.com/Virtual-memory-to-Physical-memory/

Kernel Self-protection. (n.d.) Retrieved February 27, 2023, from https://www.kernel.org/doc/html/v4.14/security/self-protection.html

Koon, J. (2022, November 3). *Memory-based cyberattacks become more complex, difficult to detect*. Semiconductor Engineering. Retrieved March 1, 2023, from https://semiengineering.com/memory-based-cyberattacks-become-more-complex-difficult-to-detect/

Linuxize. (2019, December 2). *Kill command in linux*. Linuxize. Retrieved March 18, 2023, from https://linuxize.com/post/kill-command-in-linux/

Linuxize. (2020, July 18). *Free command in linux*. Linuxize. Retrieved February 8, 2023, from https://linuxize.com/post/free-command-in-linux/

Sharma, S. (2023, March 17). *Use XXD command in linux*. Linux Handbook. https://linuxhandbook.com/xxd-command/

Stallman, R., Pesch, R., & Shebs, S., et al. (2002, January). *Debugging with GDB*. Debugging with GDB - Table of Contents. Retrieved March 1, 2023, from https://ftp.gnu.org/old-gnu/Manuals/gdb/html_chapter/gdb_toc.html

Sterling, T., Anderson, M., & Brodowicz, M. (2018, January 5). *Chapter 11 - Operating systems*. High Performance Computing. Retrieved February 24, 2023, from https://www.sciencedirect.com/science/article/pii/B9780124201583000113

Tayag, M. I., & De Vigal Capuno, M. E. (2019). Compromising systems: Implementing hacking phases. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3391093

Verizon (2022) *Data breach investigations report*. Verizon Business. Retrieved May 10, 2023 from https://www.verizon.com/business/en-gb/resources/reports/dbir/

Vostokov, D. (2023). Bytes, Halfwords, Words, and Doublewords. In: Foundations of ARM64 Linux Debugging, Disassembling, and Reversing. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-9082-8_5

Wazan, A. S., Chadwick, D. W., Venant, R., Billoir, E., Laborde, R., Ahmad, L., & Kaiiali, M. (2022). Rootasrole: A security module to manage the administrative privileges for linux. *Computers & Security*, 102983. https://doi.org/10.1016/j.cose.2022.102983

Zivanov, S. (2022, October 25). *LSOF command in linux {14 practical examples}*. Knowledge Base by phoenixNAP. Retrieved February 12, 2023, from https://phoenixnap.com/kb/lsof-command