Open Access License Notice

Virtual Gamification in a PBS-based SETA Program

Krista Stacey
Computer Science
University of South Alabama
Mobile, USA
0009-0007-8824-1974

Jeffrey Landry
Information Systems and Technology
University of South Alabama
Mobile, USA
0000-0003-4144-601X

Abstract—The insider threat remains a significant concern in information security, with self-efficacy and protection motivation emerging as key factors influencing compliance. Security Education Training and Awareness (SETA) programs often address self-efficacy but fail to adequately enhance protection motivation. This paper adopts an educational perspective by incorporating Positive Behavior Support (PBS) pedagogy into a SETA framework, emphasizing the use of virtual gamification and PBS principles to foster a positive, engaging training environment. The proposed nomological model, designed for future testing, evaluates the effects of PBS, gamification, and virtualization on protection motivation and self-efficacy. To bridge the gap between theory and practice, this paper also discusses strategies for direct implementation of PBS-based gamification in organizational settings, such as positive reinforcement, incentivized participation, and adaptive training scenarios. These approaches allow organizations to address immediate security challenges while contributing valuable insights for refining the model. The implications of this research extend beyond compliance, offering a scalable methodology for creating a sustainable, positive organizational security culture.

Keywords—*SETA, PM, SE, Gamification, Positive behavior support (PBS), XR, AR, VR, Information security (InfoSec)*

I. INTRODUCTION

It has been noted by Security Magazine that the biggest threat to Information Security (InfoSec) according to CIOs is that of the insider [1]. The Department of Homeland Security (DHS) of the U.S. established an Insider Threat program to establish policy and funding for what they consider the greatest threat to national InfoSec, basing the necessity of the policy on their report that 29% of their agencies incurred loss attributed to an insider [2].

DHS maintained that the key to any InfoSec policy in regards to an insider threat is that of user awareness and training. To counter this threat, many InfoSec managers implement security education training and awareness (SETA) programs [3]. There have been many studies on how to best implement SETA programs, and some, like Posey et al., suggest that employees who have Protection Motivation (PM) in the organization and are high in Self-Efficacy (SE) are more likely to comply with InfoSec policy [3]. A persisting and debated area of study within InfoSec research is a best approach to crafting a SETA program that increases both PM and SE; one that will succeed with both the malicious insider and the non-compliant insider.

One area that is scarce in SETA pedagogical guidance research is that of K–12 education. Since SETA is an education tool, education pedagogy can be applied [4]. There have been many studies that show students who are educated in a positive environment are more likely to comply with rules, and this compliance contributes to PM and also improves educational success [5]. This theory, commonly called Positive Behavior Support (PBS), is an organization-wide philosophy that is implemented with the growth/success of the student as a focus instead of correction/punishment for wrongdoing [6]. This provides the basis for the first research question. RQ1: Will a SETA program designed with PBS principles increase protection motivation and self-efficacy, thereby increasing InfoSec policy compliance?

Furthermore, one growing methodology in education and training that follows PBS-based philosophy is gamification, which allows learners to feel immersed and rewarded when they show mastery of the learning objectives (LOs) [7]. This gamification can be combined with another emerging method, mixed-reality (XR) simulated training/gaming [8]. XR simulations can include a varying degree of virtual reality that can further immerse and reward the user. This has shown to make learning more engaging and outcomes more successful, though at what intensity/level of gamification and virtualization is effective is still being investigated [9]. Also, combining the two methods with PBS needs further investigation in the SETA application. This leads to the second research question. RQ2: At what combination of intensities of virtuality, gamification, and PBS implementations will a SETA program developed in XR increase InfoSec policy compliance over traditional methods?

II. BACKGROUND

A. Insider Threat

Going back to foundational research in risk analysis such as Straub and Welke [10], organizations have been recommended to put countermeasures in place to protect their information technology and data. Their model, the Security Action Cycle, advises managers to implement deterrence, prevention, detection, and remedies through, as Warkentin and

Johnston [11] proposed, security policies, procedures, and practices. The problem, as Spears and Barki [12] noted, is that most managers focus on the technical and outside factors alone and not on the people who are more likely to use and abuse the system: the insider. Furthering the problem is that there are two types of insiders to be concerned about regarding information security: the malicious insider and the non-compliant insider. The differences between the two are mainly motivational, and organizations should implement policies, procedures, and practices that reinforce the security action cycle at the user level that will reduce the impact of both.

The characteristics of a malicious insider were studied in depth by Liang et al. [13]. In this paper, there is a focus on a factor an organization can control that leads to an insider committing a malicious attack on resources: their PM of the work environment. The malicious insider may feel isolated or in conflict with others in the organization, or they may be disgruntled with a work policy, situation, or environment. Whatever is motivating the insider, their intent becomes to harm the organization through a willful disregard or breach of policy for some gain, whether personal or monetary. The counteraction to this is to increase the user's PM [14]. While opportunity is usually the focus of InfoSec, an increase in PM may mitigate some of their motivation to act [15]. A 2022 study by Sharma and Aparicio found that PM is an effect of organizational culture affecting both facets of PM: coping appraisal and threat appraisal, leading to better compliance [16].

While PM factors into the non-compliant insider, SE is also a major factor of compliance for this group. Guo et al. [17] focused specifically on the non-compliant insider and found that job performance goals and social norms heavily affect an insider's compliance. This environmental stress is a factor that lessens one's PM [18]. Other studies also suggest that perceived SE in compliance [15] and rationalization of non-compliance [14] factor into an insider's intentions and behaviors. As Siponen and Vance [19] noted, when an insider is rationalizing or neutralizing their behaviors, they often are not aware of the risk they are causing to the organization and want to just get their jobs done. Warkentin et al. [20] also found neural correlates of SE to increased PM as opposed to fear-based deterrence practices (Hypothesis 3). Increasing one's SE and PM can help a user stop neutralizing behavior and increase compliance (Hypotheses 1 and 2).

As Liang et al. [13] noted, it is difficult to observe actions and behaviors of the malicious insider. Since SE influences PM and PM is a factor for both groups, this paper does not differentiate between the two and treats all insiders as users. Implementable methods to address one's PM and SE's effects on PM present some gaps in the research.

B. SETA

PM can be addressed in InfoSec policy and practice research during the deterrence and prevention stages of the security action cycle. Straub and Welke [10] proposed that deterrence is where policy and training are important, and where managers can influence the PM of the insider threat. D'Arcy et al. [21] further expanded deterrence theory into three categories: "user awareness of security policies; security education, training and awareness (SETA) programs; and computer monitoring." Awareness of security policies as well as awareness of threat vulnerabilities and punishments due to non-compliance are important. Such awareness, as Boss et al. [22] note, appeals to the insider's fear responses. Adequate fear appeals in making users aware of security can help motivate (particularly non-compliant insiders) users to follow policy. However, other studies, such as those by Warkentin et al. [20], contradict the effectiveness of fear in InfoSec applications.

When training employees on the necessary procedures to implement the policy, Johnston et al. [23] and Spears and Barki [12] suggest that the language and job of the users must be considered, as this will increase their self-efficacy and response-efficacy of handling threats. Including different levels of users in the training creation may help to increase protection motivation and further deter unintentional breaches of policy. In addition, computer monitoring is a deterrent for both non-compliant and malicious insiders as there is knowledge that there is enforcement of the policies and procedures as well as more probable identification of the culprits responsible. This also lessens intents and behaviors, and reinforces social norms of compliance [10]. This social norm reinforcement in turn helps the SETA to be effective [17]. In summary, it can be surmised from the literature that an effective SETA program is influenced by PM, and the program itself influences SE and compliance with InfoSec policy.

C. PBS

Inside of a SETA program, users are analogous to students. There is InfoSec literature that addresses SETA in the scope of a user [21], [23], as well as studies that discuss pedagogy in general workforce training such as Davis in 2014 [24]. Conversely, education research shows educational methodology for adolescents in digital literacy [25]. Focusing on SETA and education-related research, Curran [26] conducted a literature review to classify the pedagogical necessities of a SETA program. Kam et al. [27] showed the importance of interest in a successful cybersecurity training program. There is also some research on using pedagogy that meets users at their educational level [6], [23], but not on their behaviors in regard to their "education." There is a gap in the research on a pedagogy for SETA that treats insiders as students in regards to educational behavior.

More specifically, one can consider the malicious and non-compliant insiders as students that misbehave and do not conform to the rules and expected norms of their educational institution. Managers need to employ methods to correct misbehavior and encourage behavior (i.e., compliance with policy). There is educational literature on how to address (mis)behavior of students, going back to authoritative models of zero-tolerance and "name-taking" [28] to more modern

ideas of clear communication and work/play balance to improve engagement as a natural misbehavior deterrent such as Abacioglu in 2021 [29]. One notable pedagogy that focuses on improving organization-wide behavior is the theory of positive behavior supports, more commonly known in education as PBS [6]. Young et al., in their guide on PBS, state that behavior intervention and successful learning rely on fundamental principles. First, behavior is a purposeful way of showing need. The need, in this situation, is to complete a work-related task. When misbehavior, such as password insecurity, is condoned or rewarded, then the deviance is learned as a way of satisfying need. This leads to the second principle that deviance is naturally learned as a result of daily behaviors and interactions. To correct learned misbehavior, the third principle of PBS is that there must be a positive behavior replacement along with "meaningful reinforcement" of the correct behaviors [6].

There are four key components to PBS implementation: 1 - Set clear long-term learning objectives (LOs), 2 - Find data-backed methods of achieving those objectives, 3 - Identify user needs and monitor progress, and 4 - Have supports in place for long-term success [6]. Within each component, there is a realization that learners are unique in their needs and abilities, and the education meets them at where they are. This means that some users will need more intervention in their training than others. Inside of this individualized approach, appropriate behavior is encouraged through positive reinforcement.

PBS places emphasis on school climate (i.e., environment). A "healthy" environment is one where everyone feels welcomed and supported [6]. PBS, when employed at the school-wide (i.e., organizational) level, reduces misbehavior while also supporting academic success (SE) and PM [5]. (Hypothesis 4) Lin et al. [30] also noted that climate can help foster proactive behavior in a business setting. These successes and relationships in turn contribute to the "healthy" environment. Studies have shown PBS implemented in home environments with children that have specialized needs and behaviors [31], but there was not a discovery of any studies where PBS is applied to an organizational SETA program. Since PBS has improved behavior in educational and home settings, it can be hypothesized that it will also improve behavior in a workplace, i.e., compliance. (Hypothesis 5)

D. Gamification

While the majority of the PBS method is that of creating a positive environment, focus must also be placed on the methodologies used to implement learning [6]. One such approach to training that has been gaining attention in literature is gamification, the use of gaming elements such as points, scenes, badges, and puzzles in a non-gaming setting [9]. Li and Chu [32] showed improved interest and success in K-12 reading after using gamification. This stream of research has addressed gamification of SETA, but not how gamification can affect PM [33]. SETA can be further gamified to fit into PBS constructs by adding a skill level component to the training, similar to how players can choose the difficulty of their games. This correlates to the PBS idea that education meets the learner where they are. As "lower-level" users progress, they are positively rewarded by "leveling-up" and are more able (or self-efficient) to achieve more difficult LOs. This "leveling-up" can also address gaps noted by Dicheva et al. [7], which show gamification is not as effective when the game is not individualizable. Also, the individuality of a PBS-based game may address the findings of Bohne´ et al. [9], which found high levels of gamification did not lead to an increase of mastery. (Hypotheses 6, 7, and 8)

E. XR Simulations

Another emerging trend in education is the use of mixed reality (XR) simulations. XR is a term used to describe any application that uses virtual reality (VR) and/or augmented reality (AR) [34]. In any industry where a simulation can save time and money, people are looking to XR to achieve realistic, immersive renderings over classic 3D modeling such as in architecture [35]. XR is used to simulate potentially dangerous situations such as driver's education or medical training [8]. The immersion, interactivity, and replicability of tasks in XR lend it to be a useful tool in simulation-based training. These same aspects can also contribute to a PBS system, similar to methods of gamification. In SETA programs, Herbert et al. [36] addressed improvements in network security training effectiveness when using an AR approach, and Lankton et al. [37] found a human-like interaction with technology builds more trust in the system. However, there is a gap in the research on studying the effects of XR simulations in a SETA program when combined with gamification and PBS. As XR simulations allow for immersion, individuality, and positive experience, it is hypothesized that, like gamification, using XR in SETA programs will improve PM and SE. (Hypotheses 9-11) The Hypotheses are formally stated in Table I. It is these hypotheses that form the nomological model presented in the next section.

TABLE I. Hypothesis

Num	Hypothesis
1	PM as measured by belonging increases Information Security policy compliance
2	SE increases Information Security policy compliance.
3	SE positively affects PM.
4	Positive Behavior Supports positively affects PM.
5	Positive Behavior Supports positively affects compliance.
6	Gamification of training positively affects the user's PM.
7	Gamification of training positively affects the user's SE.
8	Gamification of training positively affects compliance.

Num	Hypothesis
9	XR simulation training positively affects a user's PM.
10	XR simulation training positively affects a user's SE.
11	XR simulation training positively affects a user's compliance.

III. NOMOLOGICAL MODEL

These hypotheses can be combined to form a nomological model as presented in Figure 1. It is from this model that a methodology can be constructed. A nomological model is an ideal choice for structuring this research as it establishes a comprehensive and theoretically grounded framework to test hypotheses. Unlike simpler causal models, a nomological approach accommodates the interplay of multiple constructs—such as PBS, gamification, and virtualization—and their collective influence on protection motivation (PM) and self-efficacy (SE). By explicitly defining directional relationships based on established theory, the model avoids symmetrical reflection—a common limitation in simpler correlational studies where reciprocal causation could be misinterpreted. Symmetrical reflection is mitigated by grounding the constructs in tested theories, such as Protection Motivation Theory and PBS, which dictate unidirectional causal pathways from predictors (e.g., gamification intensity) to outcomes (e.g., improved InfoSec policy compliance). This theoretical basis ensures clarity in the cause-and-effect relationships tested, providing a robust framework for subsequent experimental and longitudinal studies.

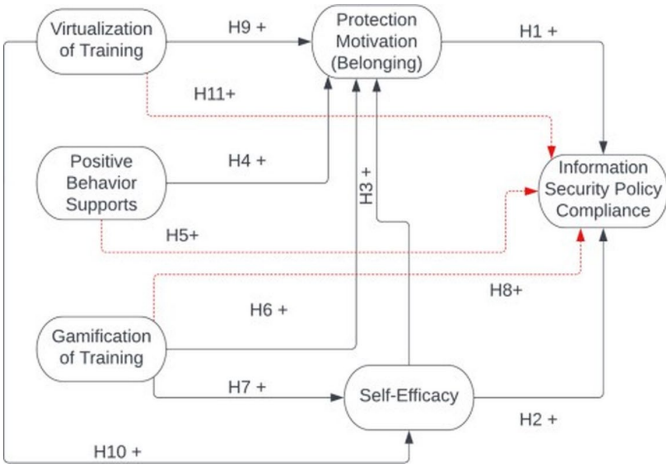

Fig. 1. Nomological Model

IV. METHODOLOGY

In order to test the preceding model, a 2x2x2 factorial lab experimental model followed by action research is proposed. According to Bhattacherjee [38], a factorial design is appropriate when multiple independent variables are being tested. In this case, the independent variables are PBS, gamification, and virtualization of the gamification. This leads to eight possible combinations of a SETA training scenario, and each independent variable can be examined independently, while any interaction effects can also be observed. Action research is where the researcher is involved in the treatment. In this case, a gamified VR SETA program that uses PBS would be employed at an organization, and its longitudinal effects would be studied. This design would also allow for the researcher to adapt the treatment to the needs and evolution of the organization, which is a core construct of PBS [6].

A. SETA combinations

To further illustrate the factorial design, a low PBS–low gamification–low virtualization SETA program would be typical of what organizations currently employ. This would consist of a video or lecture training followed by a quiz and no positive feedback or reinforcement. According to the hypothetical model, this training should contribute the least to PM and SE, and therefore result in less effectiveness and compliance to InfoSec policy. In contrast, a high PBS–high gamification–high virtualization training would consist of training employed as a game in a completely virtual environment that offers rewards and encouragement as the users "level up." There would be, in the virtual world, other signs of PBS, such as encouraging flyers. According to the theoretical model, this simulation should contribute the most to PM and SE and therefore result in more effectiveness and compliance to InfoSec policy.

As a proposed scenario, the user would be trained on a security topic or threat such as phishing. Phishing is the use of deceptive messaging to lure a user to enter sensitive information on an insecure channel. This topic choice falls in line with other gamification of SETA studies reviewed by Simpson and Brantly. [39]. For this experiment, all users would take a pre-survey to measure their PM as a sense of belonging, perceived SE in completing SETA tasks, and intentions to comply with InfoSec policy. The traditional scenarios would have the user read or view information about phishing and pass a quiz. Gamification could be employed by adding in points and rewards for correct answers, as well as an end-of-level goal that the user or player would want to achieve, such as successfully keeping certain information secret for an important covert mission. The virtualization would immerse the user in either the traditional or gamified training. PBS theory would also be applied in low or high treatments of individualization and positive feedback to create eight distinct phishing training scenarios. The finalized content of these trainings would be validated by SETA experts for content validity. After the training, all users would be reassessed via a post-test survey to measure their PM, SE, and intentions to comply, as well as give an effectiveness evaluation of their training.

B. Experimental Setup

As Bhattacherjee [38] noted, laboratory experiments are high in internal validity when properly conducted. This involves picking valid test subjects. For this experiment, any and all levels of users in any type of organization that deals with information would be valid subjects. Therefore, it would be ideal to pick a random sampling of the general adult population and then randomly assign them to one of the eight scenarios. Their perceptions of PM, SE, and intention to comply with InfoSec policy would be assessed via pretest and posttest surveys, such as those employed by two-group designs. The posttest survey would also measure the perceived effectiveness of the training. The surveys would use a 5-point or 7-point Likert scale to measure the items. The pre- and post-test surveys are reviewed by experts in InfoSec and then piloted to a small panel to ensure question clarity, reliability, and validity.

C. Determining Results

After the experiment, the quantitative data from the surveys and experiment are collected [38]. As there are multiple constructs and variables included in this study, both univariate and bivariate analyses of the data are recommended. This will show not only cause-effect relationships but also any correlations and interaction effects. Then, validity of those results must also be performed to ensure the methodology was sound and reproducible.

D. Discussion

In implementing the proposed experiment methodology, there is no way to discern between the malicious insider and the non-compliant insider other than the user admitting to such in the pre- and post-test surveys. Liang et al. [13] noted that malicious insiders are not likely to volunteer information about their behaviors or intentions. This is further reasoning for why the model treats all insiders as the same.

One weakness of the proposed methodology is that training scenarios alone do not create a positive, reinforcing environment, which is key to PBS. After the initial study, it is suggested that a longitudinal action research design be applied to the scenario that achieved the most favorable results in terms of PM, SE, and compliance. As a suggested secondary study, action research would involve providing the chosen organization with the VR game training as well as the PBS training to create the "healthy" PBS environment that would further promote compliance. Then, through additional observation, surveys, interviews, and follow-up interventions, the methodology can further be improved and studied [38]. The longitudinal nature of this design also studies behaviors rather than intentions, which can further explain any correlations between the two. Furthermore, longitudinal action research opens an opportunity to further explore the duality of the insider threat, as events that can be identified as malicious or non-compliant can be observed, as well as how further treatment affects those two groups.

While the suggested methodology is robust, there are other methods that could be used to test parts of the nomological model presented. A secondary methodology for RQ1 could be a dual case study of SETA training effectiveness at two or more organizations. Ideally, there would be a contrast in levels of PBS characteristics of the organizations to make a good comparison. The organizations could be chosen in terms of some rating of compliance to policy or a workplace satisfaction factor or employee belongingness rating. Case studies are high in external validity as they represent real-world representations of the phenomenon, with a multiple case study extending the internal validity that a single case study would be lacking [38]. This method is also a good combination of deductive and inductive research, as the hypothesis that positive training leads to compliance can be tested while the in-depth observations would help discover other factors that may alter the hypothesis development. The instruments used in this study are more qualitative in nature as they would include interviews and observations, but quantitative data such as reports and surveys can be included to further validate the study via statistical analysis. While this methodology would help distinguish between the malicious and non-compliant insider, a follow-up methodology would have to be conducted to test the virtualization and gaming elements posed by the second research question.

It is also possible to test PBS, virtualization, and gamification preferences, as well as measure SE and PM via survey methods. This methodology would be useful in an inductive approach to forming the hypotheses about each construct in relation to its effect on compliance. As Bhattacherjee [38] noted, surveys are high in external validity, helping to develop hypotheses that are also generalizable for a secondary study. This method is not good for a more deductive approach as it is low in internal validity. This survey would consist of agreement statements to test the constructs of positivity, virtualization, and gamification, and also shed light on employee opinions on how those constructs factor into their perceived effectiveness of training and their intentions to comply with training. It would also have statements regarding any SETA training participants have had and their compliance attitudes before and after that training. The statements would be implemented with a 5- or 7-point Likert scale. The instrument would have to be validated through an expert panel (SETA experts) and then piloted to produce a final survey instrument. During and after the survey, non-response, sampling, social desirability, and recall biases would have to be accounted for in order to defend the validity of the study. Moreover, this would be a quantitative method where statistical analyses of the results would be paramount. The weakness of this method is that there is no testing of the hypotheses, so it would just be further help in creating and editing the model.

While the proposed methodology is robust in covering both research questions, it is a time and resource-intensive undertaking. The SETA scenarios for the experiment would have to be created, which would include software

development and testing. To make the model even more generalizable, scenarios other than just the phishing presented would need to be formulated. Also, the proposed longitudinal action research by definition is a lengthy and involved process. Furthermore, the study would have to solicit an organization willing to implement the program and be studied for the time required.

In addition to testing the proposed nomological model, practitioners could directly implement virtual gamification as a practical approach to improving compliance with InfoSec policies. This approach allows organizations to harness the benefits of gamified training and virtual environments while aligning with PBS principles to create an engaging and supportive learning experience. By incorporating positive messaging and reinforcement, organizations can foster a culture of compliance and growth. For instance, tailored feedback and recognition can be provided during training sessions to reward progress and reinforce positive behaviors.

Incentivizing participation through tangible or symbolic rewards, such as badges, leaderboards, or certifications, further aligns with PBS by promoting intrinsic and extrinsic motivation. Practitioners could also integrate ongoing support systems, such as peer mentoring or accessible resources, to ensure employees feel equipped to succeed. Modular training scenarios with adjustable gamification intensity could allow gradual deployment while monitoring individual progress and adapting to the organization's needs. By implementing these methods, practitioners can gather real-world insights, refine their training strategies, and contribute to the iterative improvement of the proposed model while addressing immediate security challenges.

V. CONCLUSION

This paper addresses the critical question of how to mitigate the insider threat through a Security Education Training and Awareness (SETA) program grounded in Positive Behavior Support (PBS) pedagogy and enhanced by virtual gamification methodologies. The proposed nomological model serves as a theoretical framework for future research, providing a robust structure to test hypotheses about the interplay of PBS, gamification, and virtualization in improving protection motivation (PM) and self-efficacy (SE). The time-intensive nature of this methodology highlights the need for careful design and execution, yet its potential to offer tailored, data-backed solutions for InfoSec compliance makes it a valuable contribution to the field. Beyond testing the model, practitioners have an immediate opportunity to implement virtual gamification directly within their organizations. By integrating PBS principles such as positive messaging, incentivizing participation, and providing ongoing support, organizations can foster an engaging and supportive environment that encourages compliance. The practical application of PBS and gamification, through strategies like modular and adaptive training scenarios, allows organizations to address immediate security challenges while simultaneously contributing to the refinement of theoretical frameworks. These implications emphasize the dual importance of theoretical validation and real-world application. While the model provides a structured roadmap for understanding the effectiveness of PBS-driven gamification, the practitioner-focused approach ensures that organizations can proactively improve their training programs and InfoSec compliance. Together, these strategies highlight the transformative potential of combining positive reinforcement, gamified learning, and virtual environments to address one of the most pressing threats to information security today.

REFERENCES

[1] M. Lauver, "CISOs list top cyber threats to enterprises in 2022," Security Magazine, 2022. [Online]. Available: https://www.securitymagazine.com/articles/97667-cisos-list-top-cyber-threats-to-enterprises-in-2022.

[2] United States Congress: Committee on Homeland Security, Department of Homeland Security Insider Threat and Mitigation Act of 2015: Report Together with Dissenting Views (to Accompany H.R. 3361) (Including Cost Estimate of the Congressional Budget Office), 2015. https://www.govinfo.gov/content/pkg/CRPT-114hrpt321/html/CRPT-114hrpt321.htm

[3] C. Posey, T. L. Roberts, and P. B. Lowry, "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," Journal of Management Information Systems, vol. 32, no. 4, pp. 179–214, Oct. 2015, doi:10.1080/07421222.2015.1138374.

[4] Y.-Y. Chan and V. K. Wei, "Teaching for Conceptual Change in Security Awareness," IEEE Security & Privacy, vol. 6, no. 6, pp. 67–69, Nov. 2008, doi:10.1109/MSP.2008.157.

[5] K. Martens and K. Andreen, "School Counselors' Involvement with a School-wide Positive Behavior Support System: Addressing Student Behavior Issues in a Proactive and Positive Manner," Professional School Counseling, vol. 16, no. 5, pp. 313–322, Jan. 2013. https://doi.org/10.1177/2156759X1201600504

[6] E. Young, P. Caldarella, M. Richardson, and R. Young, Positive Behavior Support in Secondary Schools: A Practical Guide. New York, NY, USA: The Guilford Press, 2012.

[7] D. Dicheva, C. Dichev, G. Agre, and G. Angelova, "Gamification in Education: A Systematic Mapping Study," Journal of Educational Technology & Society, vol. 18, no. 3, pp. 75–88, Jul. 2015. https://www.jstor.org/stable/jeductechsoci.18.3.75

[8] D. Patel et al., "Developing Virtual Reality Trauma Training Experiences Using 360-Degree Video: Tutorial," Journal of Medical Internet Research, vol. 22, no. 12, p. e22420, Dec. 2020, doi: 10.2196/22420.

[9] T. Bohné, I. Heine, F. Mueller, P.-D. J. Zuercher, and V. M. Eger, "Gamification Intensity in Web-Based Virtual Training Environments and Its Effect on Learning," IEEE Transactions on Learning Technologies, pp. 1–19, 2022, doi:10.1109/TLT.2022.3208936.

[10] D. W. Straub and R. J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making," MIS Quarterly, vol. 22, no. 4, pp. 441–469, Dec. 1998 https://www.jstor.org/stable/249551.

[11] M. Warkentin and A. C. Johnston, "IT Governance and Organizational Design for Security Management," Information Security Policies and Practices, pp. 46–68, Jan. 2008 http://130.18.86.27/faculty/warkentin/BIS9613papers/WarkentinJohnston2008_StraubBookChapter_GovernanceForSecurity.pdf.

[12] R. Spears and H. Barki, "User Participation in Information Systems Security Risk Management," MIS Quarterly, vol. 34, no. 3, p. 503, 2010, 10.2307/25750689.

[13] N. (Peter) Liang, D. P. Biros, and A. Luse, "An Empirical Validation of Malicious Insider Characteristics," Journal of Management Information Systems, vol. 33, no. 2, pp. 361–392, Apr. 2016, url 10.1080/07421222.2016.1205925.

[14] R. Willison and M. Warkentin, "Beyond Deterrence: An Expanded View of Employee Computer Abuse," MIS Quarterly, vol. 37, no. 1, pp. 1–20, Jan. 2013, 10.25300/MISQ/2013/37.1.01.

[15] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, "A Meta-Analysis of Research on Protection Motivation Theory," Journal of Applied Social Psychology, vol. 30, no. 2, pp. 407–429, 2000, 10.1111/j.1559-1816.2000.tb02323.x.

[16] S. Sharma and E. Aparicio, "Organizational and Team Culture as Antecedents of Protection Motivation Among IT Employees," Computers & Security, vol. 120, p. 102774, Sep. 2022, 10.1016/j.cose.2022.102774.

[17] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: A composite behavior model," Journal of Management Information Systems, vol. 28, no. 2, pp. 203–236, 2011, doi:10.2753/MIS0742-1222280208.

[18] J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," Journal of Management Information Systems, vol. 31, no. 2, pp. 285–318, Oct. 2014, doi: 10.2753/MIS0742-1222310210.

[19] S. Siponen and A. Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," MIS Quarterly, vol. 34, no. 3, pp. 487–502, 2010, doi: 10.2307/25750688.

[20] A. C. Johnston, M. Warkentin, A. R. Dennis, and M. Siponen, "Speak Their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making," Decision Sciences, vol. 50, no. 2, pp. 245–284, Apr. 2019, doi: 10.1111/deci.12328.

[21] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, vol. 20, no. 1, pp. 79–98, Mar. 2009, Accessed: Mar. 02, 2023. [Online]. Available: https://doi.org/10.1287/isre.1070.0160.

[22] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," MISQ, vol. 39, no. 4, pp. 837–864, Apr. 2015, doi: 10.25300/MISQ/2015/39.4.5.

[23] A. C. Johnston, M. Warkentin, A. R. Dennis, and M. Siponen, "Speak Their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making," Decision Sciences, vol. 50, no. 2, pp. 245–284, Apr. 2019, doi: 10.1111/deci.12328.

[24] D. J. Davis, "The Pedagogy of Leadership and Educating a Global Workforce," International Journal of Progressive Education, vol. 10, no. 2, pp. 32–36, Jun. 2014, Accessed: Apr. 26, 2023. [Online]. Available: https://ijpe.inased.org/makale/2437.

[25] F. J. R. Estrada, C. E. George-Reyes, and L. D. Glasserman-Morales, "Security as an Emerging Dimension of Digital Literacy for Education: A Systematic Literature Review," Journal of E-Learning & Knowledge Society, vol. 18, no. 2, pp. 22–33, Aug. 2022, doi: 10.20368/1971-8829/1135440.

[26] T. (Terri) Curran, "Information Security (IS) Training: Instructional Design Project," Journal of Applied Learning Technology, vol. 5, no. 3, pp. 24–30, Summer 2015, Accessed: Apr. 26, 2023. [Online]. Available: https://scholar.google.com/scholar?oi=bibs&cluster=11558608854080586471&btnI=1&hl=en.

[27] H.-J. Kam, D. K. Ormond, P. Menard, and R. E. Crossler, "That's Interesting: An Examination of Interest Theory and Self-Determination in Organisational Cybersecurity Training," Information Systems Journal, vol. 32, no. 4, pp. 888–926, 2022, doi: 10.1111/isj.12374.

[28] L. Canter, "Let the Educator Beware: A Response to Curwin and Mendler," Educational Leadership, vol. 46, no. 2, pp. 71–73, Oct. 1988, Accessed: Apr. 27, 2023. [Online]. Available: https://files.ascd.org/staticfiles/ascd/pdf/journals/ed_lead/el_198810_canter.pdf.

[29] C. S. Abacioglu, M. Volman, and A. H. Fischer, "Teacher Interventions to Student Misbehaviors: The Role of Ethnicity, Emotional Intelligence, and Multicultural Attitudes," Current Psychology, vol. 40, no. 12, pp. 5934–5946, Dec. 2021, doi: 10.1007/s12144-019-00498-1.

[30] C. Lin, J. L. S. Wittmer, and X. (Robert) Luo, "Cultivating Proactive Information Security Behavior and Individual Creativity: The Role of Human Relations Culture and IT Use Governance," Information & Management, vol. 59, no. 6, p. 103650, Sep. 2022, doi: 10.1016/j.im.2022.103650.

[31] M. Hieneman and S. A. Fefer, "Employing the Principles of Positive Behavior Support to Enhance Family Education and Intervention," Journal of Child and Family Studies, vol. 26, no. 10, pp. 2655–2668, Oct. 2017, doi: 10.1007/s10826-017-0813-6.

[32] X. Li and S. K. W. Chu, "Exploring the Effects of Gamification Pedagogy on Children's Reading: A Mixed-Method Study on Academic Performance, Reading-Related Mentality and Behaviors, and Sustainability," British Journal of Educational Technology, vol. 52, no. 1, pp. 160–178, Jan. 2021, doi: 10.1111/bjet.13057.

[33] T. D. Ashley, R. Kwon, S. N. G. Gourisetti, C. Katsis, C. A. Bonebrake, and P. A. Boyd, "Gamification of Cybersecurity for Workforce Development in Critical Infrastructure," IEEE Access, vol. 10, pp. 112487–112501, 2022, doi: 10.1109/ACCESS.2022.3216711.

[34] P. A. Rauschnabel, R. Felix, C. Hinsch, H. Shahab, and F. Alt, "What is XR? Towards a Framework for Augmented and Virtual Reality," Computers in Human Behavior, vol. 133, p. 107289, Aug. 2022, doi: 10.1016/j.chb.2022.107289.

[35] Y. Zhang, H. Liu, S.-C. Kang, and M. Al-Hussein, "Virtual Reality Applications for the Built Environment: Research Trends and Opportunities," Automation in Construction, vol. 118, p. 103311, Oct. 2020, doi: 10.1016/j.autcon.2020.103311.

[36] B. Herbert, G. Wigley, B. Ens, and M. Billinghurst, "Cognitive Load Considerations for Augmented Reality in Network Security Training," Computers & Graphics, vol. 102, pp. 566–591, Feb. 2022, doi: 10.1016/j.cag.2021.09.001.

[37] N. K. Lankton, D. H. McKnight, and J. Tripp, "Technology, Humanness, and Trust: Rethinking Trust in Technology," Journal of the Association for Information Systems, vol. 16, no. 10, pp. 880–918, Oct. 2015, Accessed: Apr. 04, 2023. [Online]. Available: https://aisel.aisnet.org/jais/vol16/iss10/1/.

[38] A. Bhattacherjee, "Social Science Research: Principles, Methods, and Practices," 3rd ed. Tampa, FL, USA: Open Textbook Library, 2019. [Online]. Available: https://open.umn.edu/opentextbooks/textbooks/social-science-research-principles-methods-and-practices

[39] J. Simpson and A. Brantly, "Security Simulations in Undergraduate Education: A Review," Journal of Cybersecurity Education, Research and Practice, vol. 2022, no. 1, Jul. 2022, doi:10.62915/2472-2707.1086.