MLA Studios

WCS494

Kwabena Preko

In an epoch defined by the rapid and ceaseless evolution of technology, the looming specter of cyber threats casts an ever-growing shadow over organizations on a global scale. As the digital landscape continues its dynamic transformation, cybercriminals adapt their tactics, underscoring the imperative for organizations to fortify their defenses with robust cybersecurity measures. Within the intricate tapestry of defense strategies, a notable vulnerability emerges—the human factor. Employees, unwittingly and often due to a lack of awareness or engagement in cybersecurity best practices, become inadvertent contributors to security risks. This introduction delves into a pervasive and pressing issue confronting organizations across diverse sectors—the ineffectiveness of traditional employee cybersecurity education methods. Conventional approaches, relying heavily on uninspiring methods such as emails and PowerPoint presentations, falter in their ability to capture the attention and commitment of the workforce. Consequently, there exists a palpable gap in understanding and a lack of seriousness toward cybersecurity threats, leaving organizations exposed and vulnerable to malicious attacks.

The urgency of addressing this multifaceted problem is underscored by a myriad of studies, real-world incidents, and disconcerting statistics. The Ponemon Institute's comprehensive "Cost of a Data Breach Report" consistently identifies human error as the predominant cause of data breaches, constituting a staggering 23% of incidents in their 2020 report. This sobering statistic underscores the pivotal role that employees play in the cybersecurity landscape and emphasizes the crucial need for effective training methodologies. Surveys and research findings resonate with the narrative of insufficient engagement with traditional training methods. A discerning study conducted by Wombat Security reveals a significant proportion of employees expressing their dissatisfaction with existing cybersecurity training materials, deeming them both tedious and irrelevant to their professional roles. This pervasive disengagement creates a critical chasm

in the comprehension and practical implementation of cybersecurity measures within the organizational framework. Real-world incidents serve as poignant reminders of the gravity of this gap. Major data breaches, often splashed across headlines, consistently feature human error as a contributing factor. Whether employees unwittingly succumb to sophisticated phishing scams or neglect established security protocols, the aftermath of such incidents is characterized by substantial financial losses, reputational damage, and the looming threat of legal repercussions. In response to this urgent and complex problem, the proposed innovation emerges as a beacon of transformative change—an inventive solution poised to revolutionize the landscape of cybersecurity education. The core tenet of this innovative approach involves a departure from traditional methods, introducing a novel and dynamic strategy: the integration of humorous short videos. These videos are meticulously crafted to inject an element of entertainment into the educational process, strategically leveraging the power of humor to not only capture the attention of the audience but also to make cybersecurity training a not merely tolerable but genuinely enjoyable experience.

The landscape of cybersecurity education stands at a critical juncture as organizations grapple with the escalating threats posed by cybercriminals. Traditional methods of imparting cybersecurity knowledge, such as emails and PowerPoint presentations, have faced criticism for their inefficacy in engaging and effectively educating employees. This review synthesizes scholarly literature to provide a comprehensive understanding of the problem surrounding conventional cybersecurity education and delves into the innovative approach of using humorous short videos as a transformative solution.

"Get a red-hot poker and open up my eyes, it's so boring." In the realm of organizational cybersecurity, the implementation of Security Education, Training, and Awareness (SETA) programs stands as a fundamental strategy to enhance the cybersecurity posture. However, despite the significant investment and effort directed toward these programs, a growing body of research, exemplified by the study involving 20 Australian employees, illuminates a prevailing dissatisfaction among workforce participants. This dissatisfaction reveals a nuanced challenge in the cybersecurity landscape – the engagement of employees in SETA programs. The study underscores the significance of managerial role modeling and the design of workplace systems as essential elements for effective non-cybersecurity training. Yet, in the context of cybersecurity education, these factors alone may not suffice. An intriguing revelation from the research is the pivotal role played by the behavior of colleagues in shaping employee perceptions of SETA programs. Unlike traditional training, where misbehavior may have less impact, in the cybersecurity domain, the missteps of colleagues emerge as a more influential factor in shaping the overall perception of the program. This source not only highlights the discontentment among employees regarding SETA programs but also underscores the need for a tailored and context-specific approach in cybersecurity training initiatives. As organizations navigate the complex terrain of enhancing cybersecurity awareness, the challenge extends beyond conventional training paradigms. Addressing this challenge demands an exploration of the unique dynamics within the cybersecurity realm, where the behaviors of colleagues weave intricately into the fabric of employee engagement. Thus, the quest for effective cybersecurity training necessitates a holistic understanding of organizational dynamics and a targeted approach that goes beyond conventional training methodologies. "Enterprise Cybersecurity Training and Awareness Programs: Recommendations for Success"

In the pursuit of fortifying organizational cybersecurity, enterprises invest in cybersecurity training and awareness programs to cultivate active engagement among employees, ensuring compliance with security policies. However, the efficacy of these programs often falters as employees find themselves disinterested and bored with the conventional training approaches. Recognizing the criticality of success in cybersecurity training and awareness programs, this source puts forth a set of best practices and actionable insights to reinvigorate engagement and effectiveness. The paper emphasizes the need to bridge the gap between cybersecurity training and employees' personal lives, acknowledging the interconnected nature of individuals' online and offline experiences. By reinforcing security procedures and guidelines, the source advocates for a comprehensive integration of cybersecurity principles into employees' daily routines. The concept of instilling a "relaxed alert" state among employees stands out as a unique approach, recognizing the importance of maintaining vigilance without inducing stress or fatigue. Moreover, the source delves into the challenge of cybersecurity fatigue, a weariness specific to cybersecurity-related behaviors or advice resulting from overexposure. It proposes strategies to minimize this fatigue, ensuring sustained engagement. The overarching goal is to assist enterprises in developing cybersecurity training and awareness programs that are not only economical and effective but also inherently engaging. This source contributes valuable insights into innovative strategies for successful cybersecurity training, emphasizing the integration of cybersecurity principles into the fabric of employees' lives. By acknowledging the need for relevance, reinforcing security practices, and addressing the nuances of cybersecurity fatigue, organizations can pave the way for more engaging and impactful cybersecurity training initiatives.

"Design and Evaluation of a Cybersecurity Awareness Training Game" Within the dynamic realm of education and training, a transformative avenue is explored through serious games, as detailed in the source titled "Design and Evaluation of a Cybersecurity Awareness Training Game." This study pioneers a departure from traditional rote learning methods, introducing an Activity Theory-based Model of Serious Games (ATMSG) to revolutionize cybersecurity awareness training. The essence of the study lies in creating a cybersecurity awareness training tool that not only imparts knowledge but also actively engages users through gameplay. The ATMSG model serves as a guiding framework, emphasizing the importance of intertwining cybersecurity concepts with active cognitive involvement. By aligning with the principles of activity theory, the game provides users with an immersive environment, compelling them to think critically about security within the context of the gameplay. The evaluation of the game's demo presents encouraging results, indicating that the narrative-driven gameplay effectively enhances players' understanding of cybersecurity challenges and solutions. This innovative approach not only introduces a paradigm shift in cybersecurity training but also aligns with our innovation's commitment to making cybersecurity education entertaining and engaging. Relating this source to our innovation, which focuses on humorous short videos to make cybersecurity education enjoyable, both approaches share a common goal—breaking away from traditional, mundane methods. Just as serious games infuse playfulness into learning, our innovation leverages humor and brevity in video formats to capture attention and enhance comprehension. Both strategies acknowledge the importance of engagement, making the learning experience not only informative but also enjoyable for the workforce, ultimately contributing to a more resilient cybersecurity posture.

"Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue.” In the ever-evolving landscape of cybersecurity, a pervasive challenge known as cybersecurity fatigue is explored in the source titled "Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue." This form of work disengagement is specific to cybersecurity and manifests as weariness or aversion toward cybersecurity-related behaviors or advice, stemming from prior overexposure to demands or training. The source introduces a comprehensive four-component model, a pioneering conceptualization capturing all dimensions of cybersecurity fatigue. By delving into attitudinal and cognitive aspects, the model considers overexposure to workplace cybersecurity advice and actions, offering a nuanced understanding of this phenomenon. The multidisciplinary review draws insights from management, psychology, and information systems, presenting a framework to identify and address different types of cybersecurity fatigue. The practical implications of this model extend beyond theoretical concepts. Practitioners can utilize the four-component model to discern the type of cybersecurity fatigue affecting employees and adapt organizational processes accordingly. The source also enriches the understanding of cybersecurity fatigue through three illustrative case studies, demonstrating its application in real-world organizational contexts. Relating this source to our innovation, which strives to make cybersecurity education entertaining, both approaches recognize the importance of addressing employee attitudes and perceptions. By acknowledging and mitigating cybersecurity fatigue, organizations can create a more conducive environment for our innovative and engaging cybersecurity education materials, fostering a workforce that not only comprehends cybersecurity principles but also actively participates in their application.

"Generic and Unusable: Understanding Employee Perceptions of Cybersecurity Training and Measuring Advice Fatigue" The source titled "Generic and Unusable: Understanding Employee

Perceptions of Cybersecurity Training and Measuring Advice Fatigue" delves into the intricate realm of Security Education Training and Awareness (SETA) programs. Often criticized for their failure to reduce organizational cyber risk, SETA programs are scrutinized through two insightful studies in this source. In the first study, a unique repertory grid technique is employed to examine employee responses to a series of SETA videos. Through 24 in-depth semi-structured interviews across diverse industries, key themes emerge, shedding light on the content, style, and design of cybersecurity training videos. Notably, employees' perceptions are influenced not only by these elements but also by their preconceptions of cybersecurity principles and the perceived characteristics of the intended audience. The second study introduces the Cybersecurity Advice Fatigue Scale (CAFS), a self-report measure specifically designed to quantify the fatigue resulting from suboptimal cybersecurity advice. The scale, based on qualitative analyses from the first study, reveals a five-factor structure aligning with the identified themes. The results underscore the influence of employees' inferences about corporate motivations behind SETA programs on their receptivity to the content. Linking this source to our innovation, which strives to make cybersecurity education entertaining through humorous short videos, both approaches converge on the significance of understanding and addressing employee perceptions. By quantifying advice-related cybersecurity fatigue, organizations can tailor our engaging cybersecurity training materials to mitigate fatigue factors, fostering a more receptive and participative workforce in the fight against cyber threats.

"Reinforcing Cybersecurity Hands-on Training With Adaptive Learning" In the dynamic landscape of cybersecurity education, the source titled "Reinforcing Cybersecurity Hands-on Training With Adaptive Learning" introduces a pioneering perspective — the integration of adaptive learning to enhance the student experience. Acknowledging the varied capabilities and

motivations of students, this research explores the impact of adaptive learning in the context of cybersecurity training. The study commences with an analysis of the performance of 95 students across 12 training sessions. Notably, less than half of the students completed the training without displaying any solutions, highlighting the challenges of traditional training approaches. A simulation is then employed to envision how students might fare in a training session with multiple paths of varying difficulty. Based on this simulation, the researchers propose a novel tutor model for adaptive training, taking into account students' proficiency before and during training. The subsequent case study involving 24 students validates the effectiveness of adaptive training in comparison to the original static format. Results indicate that the adaptive training format does not overwhelm students, enabling them to navigate alternative training phases with lower difficulty. The proposed adaptive format, applicable to various cybersecurity topics, emerges as a promising approach to improving the overall student experience in cybersecurity education. Relating this source to our innovation, both approaches prioritize enhancing the learning experience. While adaptive learning tailors the training to individual proficiency levels, our innovative videos aim to captivate and educate by infusing humor into the educational content. Together, these approaches contribute to a more dynamic and engaging cybersecurity training environment, ensuring that students not only grasp the material but also find the learning process enjoyable and effective.

"Cyber Security Training in Small to Medium-sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs" In the context of small to medium-sized enterprises (SMEs), the source titled "Cyber Security Training in Small to Medium-sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs" sheds light on the challenges faced by these organizations in providing effective cybersecurity training. Unlike

larger businesses that routinely invest in such training, SMEs often grapple with awareness and resource limitations, leading to a higher vulnerability to security breaches. The research underscores that while some investments are made in training, the design and delivery of cybersecurity training programs in SMEs often fall short. Rather than incorporating established learning theories and adult learning principles, these programs tend to be technical and knowledge-based. The source argues for a shift in perspective, advocating for an exploration of training effectiveness by evaluating how well it addresses employee needs within the organizational context. The qualitative approach employed in the study, involving interviews with SME business owners, reveals insights into how organizational culture influences attitudes and perceptions toward cybersecurity. The findings expose the limitations of current training approaches, demonstrating a need for a more psychologically informed lens to understand human behavior and learning in the workplace. Relating this source to our innovation, both approaches address gaps in traditional training methods. SMEs, facing unique challenges, can benefit from a more holistic understanding of employee training needs. Our innovative videos, designed to captivate and educate, align with the call for a psychologically informed approach, providing a dynamic and engaging alternative to traditional cybersecurity training for SMEs.

In the ever-evolving landscape of cybersecurity, the challenges of traditional education methods and the innovative solution of humorous short videos resonate across diverse academic disciplines, providing a comprehensive understanding of the multifaceted nature of these issues. I will now explore how concepts from psychology, communications and media studies, education, business and management, and visual arts and design converge to shed light on the problem and solution at hand.

Psychology Courses: Courses in psychology lay the groundwork for understanding the human element in cybersecurity breaches. Concepts such as cognitive biases, decision-making processes, and social engineering tactics become crucial when examining the reasons behind human errors that contribute to security incidents. The innovative use of humorous short videos aligns with principles from positive psychology, acknowledging the impact of a positive and engaging learning environment on knowledge retention and behavior.

Communications and Media Studies: In the realm of communications and media studies, the effectiveness of video-based training and the strategic integration of humor into educational content take center stage. These fields delve into the psychology of communication, the impact of visual storytelling, and the role of humor in engaging audiences. The innovative approach of using humorous short videos mirrors principles from these courses, emphasizing the power of visual communication and the strategic use of humor to convey complex information in an entertaining and memorable way.

Education and Pedagogy: Courses related to education and pedagogy contribute insights into effective teaching methodologies, particularly in addressing the challenges of employee disengagement and dissatisfaction with traditional training methods. Learner-centric approaches and the importance of tailoring educational content to meet the needs and preferences of the audience align with principles discussed in these courses. The exploration of innovative solutions, such as humorous short videos, reflects an awareness of pedagogical principles aimed at fostering engagement and active participation in the learning process.

Business and Management Studies: The consequences of cybersecurity breaches, explored in literature, align with discussions in business and management courses. The organizational impact of employee actions, encompassing financial losses, reputational damage, and legal

repercussions, ties into principles of risk management and organizational resilience. The innovative solution of humorous short videos aligns with strategic management principles, recognizing the need for creative approaches to mitigate risks and enhance organizational cybersecurity culture.

Visual Arts and Design: The exploration of video-based training and the role of visual elements in enhancing learning outcomes draws parallels with courses in visual arts and design. Principles of visual communication, graphic design, and storytelling become relevant when crafting effective and engaging educational content. The choice of humorous short videos as an innovative strategy reflects an appreciation for the visual and creative aspects of communication that transcend traditional textual methods.

In conclusion, the interdisciplinary nature of these issues underscores the interconnectedness of diverse fields of study. The problem of ineffective cybersecurity education and the innovative solution of humorous short videos showcase the importance of drawing from a variety of disciplines to address complex challenges. This highlights that effective solutions often require a synthesis of insights from psychology, communication, education, business, and visual arts, emphasizing the value of a well-rounded education in navigating the intricacies of contemporary issues in cybersecurity education.

This is how we will determine whether our innovation is effective. Establish Measurable Metrics: Identify measurable metrics that align with the defined objectives. Quantitative metrics could include factors such as the reduction in security incidents, improved employee compliance with security protocols, or increased knowledge retention rates. These metrics provide tangible data points for evaluation.

Pre- and Post-Assessment: Conduct pre- and post-assessments to gauge the knowledge levels and awareness of employees before and after the implementation of the innovation. This can involve surveys, quizzes, or other assessment tools to quantify the impact on participants' understanding of cybersecurity concepts.

Engagement Analytics: Utilize engagement analytics to assess how actively participants interact with the humorous short videos. Track metrics such as view rates, completion rates, and interaction levels. High engagement is indicative of content resonance, while low engagement may signal the need for adjustments.

Behavioral Changes: Evaluate changes in employee behavior regarding cybersecurity practices. Monitor whether there is a noticeable reduction in security incidents, an increase in the reporting of suspicious activities, or improved adherence to security policies. Observable behavioral changes are strong indicators of effectiveness.

Feedback and Surveys: Collect qualitative data through feedback and surveys. Solicit input from participants regarding their perceptions of the training content, its relevance to their roles, and their overall experience. Qualitative insights provide valuable context and uncover aspects that quantitative metrics might miss.

Long-Term Retention: Assess the long-term retention of cybersecurity knowledge. A successful innovation should contribute not only to immediate understanding but also to sustained awareness over time. Periodic assessments or follow-up surveys can gauge knowledge retention beyond the initial training.

Comparative Analysis: Conduct a comparative analysis against traditional training methods. Compare the effectiveness of the humorous short videos with previous training approaches,

considering factors such as engagement levels, knowledge retention, and behavioral changes. This comparative perspective helps validate the innovation's impact.

Adaptability and Scalability: Evaluate the adaptability and scalability of the innovation. A successful cybersecurity education innovation should be flexible enough to accommodate evolving threats and scalable to meet the needs of a growing workforce or changing organizational dynamics.

Cost-Benefit Analysis: Perform a cost-benefit analysis to determine the economic efficiency of the innovation. Assess the costs associated with content creation, implementation, and maintenance against the benefits derived, such as reduced security incidents and enhanced organizational resilience.

Continuous Improvement: Embrace a culture of continuous improvement. Solicit ongoing feedback, analyze performance data, and be prepared to iterate on the innovation. Continuous refinement ensures that the cybersecurity education strategy remains effective in the face of evolving threats and organizational changes.

What is needed for successful implementation of humorous short videos necessitates technical expertise in video production, animation, and content creation. Collaboration with professionals or teams proficient in these domains to ensure the production quality aligns with educational objectives. Technical competence ensures that the videos are not only entertaining but also effectively convey critical cybersecurity concepts. Crafting engaging and informative content is at the heart of the innovation. Collaborate with content creators, scriptwriters, and subject matter experts to develop narratives that seamlessly integrate humor with cybersecurity principles. Striking the right balance between entertainment and educational value is essential to

maximize the impact on the target audience. Adequate resources, both financial and technological, are critical for a successful implementation. Allocate budgetary resources for video production, technology infrastructure, and any necessary software or tools. A robust financial foundation ensures that the project has the necessary resources to navigate potential challenges and meet quality standards. Forge strategic partnerships with cybersecurity experts, industry leaders, or educational institutions. Collaborate with these stakeholders to gain insights, validate content, and enhance the credibility of the initiative. Partnerships can also provide access to a broader audience and diverse perspectives, enriching the overall educational experience. Before full-scale implementation, conduct pilot programs within the organization to gather feedback and assess the effectiveness of the humorous short videos. Establish feedback loops with participants, trainers, and cybersecurity professionals to identify strengths, weaknesses, and areas for improvement. This iterative approach ensures that the final implementation is refined based on real-world insights

Our summary for next steps will begin by initiating the development of the initial set of humorous short videos. Working closely with content creators and subject matter experts to ensure that the content aligns with cybersecurity best practices while maintaining an engaging and humorous tone. The initial videos will serve as the foundation for the broader implementation. Establishing the necessary technology infrastructure to support video hosting, distribution, and tracking. Consider platforms that allow easy integration with existing learning management systems (LMS) for seamless deployment and tracking of training modules. A robust technological foundation is essential for scalability and accessibility. We will provide comprehensive training for trainers who will be delivering or facilitating the cybersecurity education program. Equip them with the necessary knowledge about the content, the objectives

of the initiative, and effective strategies for incorporating the videos into training sessions. Trained facilitators are key to ensuring that the innovation is effectively communicated to the workforce. We will also launch a pilot implementation within a specific department or user group. Monitor participant engagement, gather feedback, and assess the impact on cybersecurity awareness and behavior. The pilot phase serves as a valuable testing ground to identify any unforeseen challenges and refine the implementation strategy. Based on the feedback received during the pilot phase, iterate and refine both the content and delivery strategy. Continuously engage with participants and trainers to address any emerging issues and enhance the overall effectiveness of the humorous short videos. An iterative refinement process ensures that the implementation aligns with evolving organizational needs. With the lessons learned from the pilot phase and refinements in place, scale up the implementation to encompass the entire organization. Deploy the finalized set of humorous short videos as a core component of the cybersecurity education program. Leverage the technology infrastructure to track participation, monitor progress, and gather ongoing feedback for continuous improvement. Establish a robust evaluation framework to measure the long-term impact of the innovation. Utilize quantitative metrics, such as knowledge assessments and engagement analytics, alongside qualitative feedback to gauge the effectiveness of the humorous short videos. Regularly assess the program's success in achieving cybersecurity awareness and behavioral objectives. In conclusion, turning the innovative vision of humorous short videos into a reality requires a strategic combination of technical expertise, creative content development, resource allocation, strategic partnerships, and a carefully planned implementation roadmap. The next steps involve the meticulous execution of content development, technology setup, training, pilot programs, iterative refinement, and ultimately, the full-scale implementation. By navigating these steps thoughtfully and adapting to

the evolving landscape, organizations can bring about a transformative shift in cybersecurity education, fostering a cyber-aware workforce through engaging and effective means.

Citations

Reeves, A., Calic, D., & Delfabbro, P. (2021). “Get a red-hot poker and open up my eyes, it's so boring” 1: Employee perceptions of cybersecurity training. *Computers & security*, *106*, 102281.

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249-257.

Huynh, D., Luong, P., Iida, H., & Beuran, R. (2017). Design and evaluation of a cybersecurity awareness training game. In *Entertainment Computing–ICEC 2017: 16th IFIP TC 14 International Conference, Tsukuba City, Japan, September 18-21, 2017, Proceedings 16* (pp. 183-188). Springer International Publishing.

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open*, *11*(1), 21582440211000049.

Reeves, A., Calic, D., & Delfabbro, P. (2023). “Generic and unusable” 1: Understanding employee perceptions of cybersecurity training and measuring advice fatigue. *Computers & Security*, *128*, 103137.

Fagbule, O. (2023). *Cyber Security Training in Small to Medium-sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs* (Doctoral dissertation, Bournemouth University).

Seda, P., Vykopal, J., Švábenský, V., & Čeleda, P. (2021, October). Reinforcing Cybersecurity Hands-on Training With Adaptive Learning. In *2021 IEEE Frontiers in Education Conference (FIE)* (pp. 1-9). IEEE.