A Persona-centered Information Security Awareness

Fon Žiga

Affiliation: Faculty for Computer Science and Informatics, Slovenia

E-mail: Fon, Žiga, zf73000@student.uni-lj

Abstract. Maintaining Information Security and privacy remains a critical concern for businesses, as human factors, whether accidental or malicious, are primary contributors to data breaches. This paper discusses an approach to address these issues by incorporating personas into information security awareness programs. Grounded in empirical data, personas can help identify security risks and tailor awareness activities to meet specific business needs. Findings suggest that a persona-centered approach can adapt to business demands and mitigate security risks through tailored awareness initiatives. [3]

Keywords: Information Security, Security Awareness, Human Factors, Personas, Risk system.

Informacijska varnostna ozaveščenost, osredotočena na osebnostne profile

Ohranjanje informacijske varnosti ostaja ključnega pomena za podjetja, saj so človeški dejavniki, bodisi nenamerni ali zlonamerni, glavni povzročitelji kršitev varnosti podatkov. Ta članek obravnava pristop za reševanje teh težav z vključitvijo osebnostnih profilov v programe ozaveščanja o informacijski varnosti. Na podlagi empiričnih podatkov osebnostni profili pomagajo prepoznati varnostna tveganja in prilagoditi dejavnosti ozaveščanja specifičnim poslovnim potrebam.

Ugotovitve kažejo, da pristop, osredotočen na osebnostne profile, omogoča prilagoditev poslovnim zahtevam in zmanjšuje varnostna tveganja s ciljanimi pobudami za ozaveščanje. [3]

1 INTRODUCTION

In today's digital age, Information Security is a vital concern for organizations, particularly where breaches can lead to regulatory and reputational consequences. As demonstrated in PwC's 2015 Data Breach Report, many data security breaches are linked to human factors. These factors may stem from intentional, accidental, or malicious actions. Consequently, businesses can no longer depend solely on technology and processes, but must integrate people effectively into their security strategies. Traditional methods, such as compliance-based security awareness, fail to consider the unique human factors involved in security risks, leading to a one-size-fits-all approach. [2]

1.1 What are personas?

Personas are archetypes representing user groups based on behavioral and demographic data. This paper outlines a persona-centered approach to enhancing Information Security awareness. Personas are constructed based on empirical data gathered from interviews with staff, enabling the identification of security risks tied to human behavior. These personas can be then integrated into a 90-day awareness cycle tailored to business-specific security challenges. The development of personas involves detailed interviews with staff to understand their behaviors, attitudes, and risks in the security context. These personas represent archetypes that embody user goals and security challenges. By analyzing these user models, businesses can tailor security programs that address actual human risks. [1]

1.1.1 Why use personas?

It is very difficult to tailor security awareness plans based on individuals, since individuals are numerous and usually have varied tastes and personalities. To promote the company's security plan. It's therefore necessary to create different personas. Busy executives, young people, old people, perceived cybersecurity awareness in the group... This also simplifies the role of the company security specialist. Tailored security content is designed based on the identified company personas. [1]

Received
Accepted

1.2 The Role of Personas in Security Awareness

Personas help tailor security awareness by aligning training with user-specific motivations, behaviors, and vulnerabilities, making content relevant to each role. This targeted approach, unlike generic training, drives real behavioral change by using scenario-based exercises for roles like "Client-Facing Consultant" or "IT Specialist." Personas foster a security-conscious culture that meets the unique needs of each group effectively. [1]

2 PERSONAS

Personas in security awareness address unique behaviors, risks, and vulnerabilities across roles, tailoring training to specific security needs. Based on data from staff interviews or observations, personas represent groups like executives handling sensitive data or entry-level employees at higher phishing risk. By aligning training with these personas, organizations can target specific skills and threats, ensuring relevance and effectiveness that generic programs often lack. [1]

2.1 Persona-centered Awareness Challenges

Creating effective security awareness is challenging, especially in engaging diverse staff meaningfully. Many view training as a formality, reducing retention and real-world application. Generic, fear-based content often fails to drive behavioral change and may even discourage participation. Programs that avoid punitive measures and foster positive engagement are more likely to succeed. [1]

2.2 Persona-centered Awareness Opportunities

On the other hand, numerous opportunities exist to make security awareness more engaging and impactful by integrating persona-centered designs. Tailoring security training to different roles and user personas within the organization enhances relevance and retention. For example, integrating interactive tools such as games or simulations that relate directly to employees' specific job functions can make training more practical and memorable. Additionally, aligning awareness activities with organizational culture—such as incorporating security tips into routine meetings or using team-based learning games—has proven effective in fostering a security-focused mindset. [1]

2.3 Design and Development of personas

Tailored security content is designed based on the identified personas. This content includes interactive tools, games, and quizzes to promote engagement and a deeper understanding of security risks This content includes interactive tools, games, and quizzes to promote engagement and a deeper understanding of security risks. Furthermore, it's always a great idea to add sufficient positive enforcement to facilitate security awareness. [1]

2.4 Frameworks for Security Awareness used on created personas

There are several established frameworks for building and managing information security awareness programs, each with unique strengths.

2.4.1 United States National Institute of Standards and Technology

The NIST framework is widely recognized and emphasizes a lifecycle approach that includes planning, executing, and continuously monitoring the effectiveness of security awareness training. NIST's framework focuses on assessing security needs, developing a structured program, and implementing feedback mechanisms to adapt and improve over time. This ensures that the program remains aligned with evolving security threats and business objectives. [1]

2.4.2 EU agency for cybersecurity

Another notable framework is ENISA's three-phase model, which consists of planning and assessing, executing, and evaluating security awareness initiatives. ENISA emphasizes the importance of setting specific goals, securing necessary resources, and regularly updating content to keep pace with changing security needs. ENISA's framework also supports a participatory approach, engaging employees in program development and ensuring awareness materials are tailored to diverse audiences. Additionally, the Security Culture Framework encourages a cultural perspective by embedding security values into daily operations. This framework advocates for a high level of employee participation and a focus on cultivating a shared sense of responsibility for security within the organization. Adopting elements from each of these frameworks can contribute to an adaptable, data-driven, and culturally embedded awareness program that leverages personas for targeted security education. [1]

3 CONCLUSION

This paper highlights the effectiveness of using personas in information security awareness. Tailored approaches to security training are more likely to influence behavior positively, reducing security risks through targeted awareness initiatives.

REFERENCES

[1] Persona-centred information security awareness online, https://www.sciencedirect.com/science/article/pii/S0167404817301566 (25.10.2024).

[2] J. Steinberg, Cybersecurity for Dummies. Hoboken, Nj: John Wiley & Sons, Inc, 2020.

[3] Achieving usable security and privacy through Human-Centered Design, https://library.oapen.org/bitstream/handle/20.500.12657/76226/1/978-3-031-28643-8.pdf#page=90 (25.10.2024).

Ziga Fon is an electrical engineer (UN) specializing in software development with proficiency in C, C++, java and Python. With a strong foundation in electrical engineering and a passion for computer science, he is currently advancing his studies in Computer Science while actively working on projects. In his free time, he enjoys reading science fiction literature, which fuels his enthusiasm for innovation and technology.