Persona-Driven Information Security Awareness

Duncan Ki-Aries
Bournemouth University
Poole, UK
mydevmail2@gmail.com

Shamal Faily
Bournemouth University
Poole, UK
sfaily@bournemouth.ac.uk

Kristian Beckers
Technical University Munich
Munich, Germany
beckersk@in.tum.de

Because human factors are a root cause of security breaches in many organisations, security awareness activities are often used to address problematic behaviours and improve security culture. Previous work has found that personas are useful for identifying audience needs & goals when designing and implementing awareness campaigns. We present a six-step security awareness process both driven by and centred around the use of personas. This can be embedded into business-as-usual activities, with 90-day cycles of awareness themes. We evaluated this process by using it to devise a security awareness campaign for a digital agency. Our results suggest a persona-centred security awareness approach is adaptable to business constraints, and contributes towards addressing security risks.

Information Security; Security Awareness; Personas

1. INTRODUCTION

(PwC 2015) established that a large number of internal data breaches can still be attributed to human factor issues. It could therefore be concluded that designing for security is a challenge. Improved security awareness is important when addressing the human factor, but many security awareness processes fail to engage their target audience.

Personas describe archetypical users of interest to designs (Cooper et al. 2014), and are a popular tool for encouraging people to think of the needs and expectations of a target audience. Personas may also be used within the output of the awareness campaigns, or be extended into promotional giveaway items, such as long living materials or consumables as discussed by (Hochleitner et al. 2013).

When planning security awareness campaigns, personas help understand the culture and audience needs by identifying relevant behaviours and perceptions. Despite examples of personas used within security awareness interventions, e.g. (Lewis and Coles-Kemp 2014), there has been less work showing how the design of security awareness campaigns are driven by them. To address this, this paper presents a security awareness process which is both driven by and centred around the use of personas. We describe our approach in Section 2, before presenting preliminary results using the process to devise a security awareness campaign for a digital design agency in Section 3.

Figure 1: *Persona-Driven Information Security Awareness Cycle*

2. THE APPROACH

We developed a six-step on-going security awareness process (Figure 1). The process is structured around a cycle of activities similar to (Wilson and Hash 2003), but considers the input & output recommendations of (Beyer et al. 2015). These include

on-going awareness, with a range of relevant topics that are targeted, actionable, doable, and provides feedback to help sustain peoples' willingness to change (Bada et al. 2015).

The process begins with a preliminary step whereby a business need and requirement is given, thus supporting and committing to the awareness activities. Step one of process identifies business needs, goals, and chosen awareness theme based on a risk analysis. Step two develops personas based on empirical data collected through observations & interviews, which is transcribed, refined and modelled to produce personas tailored to the business. Step three analyses the personas against the findings of step one, leading to recommendations towards an awareness approach suited to the target organisation. Step four applies selected recommendations for design & development, which considers the resource, budget and communication methods available. Step five begins the implementation of the programme, where metrics may be applied. Step six concludes by reviewing the cycle's effectiveness towards raising awareness, and considers improvements and the integration of new information or technologiy ensuring the process remains up-to-date, then continues on to repeat the cycle of activities and the chosen awareness theme.

3. RESULTS

We validated this process by devising a security awareness programme for a digital design agency, where evaluation of business needs identified Social Engineering (SE) – a means for manipulating people by deception into performing an action or giving out information (Mann 2008) – as the theme.

We created personas based on transcripts from nine interviews with randomly selected employees. These resulted in the creation of three personas, Andy (IT Support), Felicity (a Developer), and Rob (a Section Manager). Reviewing the business needs along with persona perceptions, we identified that bite-sized awareness built into daily or weekly activities would best suit the culture. The personas themselves also allowed their further integration in business scenarios. For example, this may be in a factsheet indicating what Andy, Felicity or Rob may do in a given SE attack scenario.

We evaluated the use of personas as attack victims when playing a SE card game (Beckers and Pape 2016). This proved to be useful for creating discussion and awareness around SE. For example, during the game it was identified that Andy may be specifically vulnerable to "Voice of Authority" attacks; this confirmed findings of the personas at the design stage. The game was trialled in a team meeting environment, with a technical and less technical group, each with four people. The scenario-based approach of the game helped create awareness for participants as they discovered vulnerabilities and risk mitigating factors towards improving security behaviours of the personas.

To provide a level of validation, a review of awareness activities was conducted. The findings suggested the personas demonstrated a potential for their effectiveness for the analysis and design stages. Moreover, personas were better accepted when implemented with scenarios within the awareness activities, which was further evidenced through participatory discussion with the groups. For example, during the card game individuals reflected on how the SE techniques may apply and be mitigated within their own roles and social activities. Further consideration would, however, be required towards other approaches that more fully embed the personas within the programme output, as limited testing time could not provide this. It would also have been beneficial to produce personas covering the minority of less technical roles, although it was accepted there was a limited availability of interviews given the timeframe.

A computer-based training tool may have been useful for extending awareness; this could include content further integrating personas, while offering record keeping functionality and awareness metrics. The agency decided this was out of scope, and further cost-benefit-analysis to determine a number of factors would be required. We believe the benefits of in-house development against Off-The-Shelf services and packages are likely to be considered by the agency for future awareness activities. Promotional items could also be used to further integrate the personas by embedding them within the culture and promoting the awareness programme. However, the budget and production time was not available. Therefore, if considered appropriate for the culture, this may be revisited in future work to determine its effectiveness towards the process or personas.

Future work will investigate the long-term effectiveness of the process towards improving behaviours, reducing risks, and embedding security into an unconscious routine through procedures, internal marketing, and visual design.

REFERENCES

Bada, M., Sasse, M. A., and Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? In *International*

Conference on Cyber Security for Sustainable Society, pages 118–131.

Beckers, K. and Pape, S. (2016). A serious game for eliciting social engineering security requirements. In *Proceedings of the 24th IEEE International Conference on Requirements Engineering*, RE '16. IEEE Computer Society. To Appear.

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., and Passingham, N. (2015). White paper: Awareness is only the first step: A framework for progressive engagement of staff in cyber security. Technical report, Hewlett Packard Enterprise.

Cooper, A., Reimann, R., Cronin, D., and Noessel, C. (2014). *About Face: The Essentials of Interaction Design*. John Wiley & Sons.

Hochleitner, C., Graf, C., and Tscheligi, M. (2013). Do you enjoy getting gifts?: Keeping personas alive through marketing materials. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '13, pages 2355–2358. ACM.

Lewis, M. M. and Coles-Kemp, L. (2014). Who says personas can't dance?: The use of comic strips to design information security personas. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14, pages 2485–2490. ACM.

Mann, I. (2008). *Hacking the Human: Social Engineering Techniques and Security Countermeasures*. Gower.

PwC (2015). 2015 Information security breaches survey. Technical report, PwC.

Wilson, M. and Hash, J. (2003). NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Programme. Technical report, National Institute of Standards and Technology.