Persona-Driven Information Security Awareness

D 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 many 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 which is 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

Industry reports such as the (PwC, 2015) Data Breach report, 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 the target audiences.

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 can be used to understand the culture and audience needs by identifying relevant behaviours and perceptions. Although there have been examples of personas being 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.

In this paper, we present a security awareness process which is both driven by and centred around the use of personas, and its evaluation towards improving awareness driven by the use of personas.

2. THE APPROACH

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

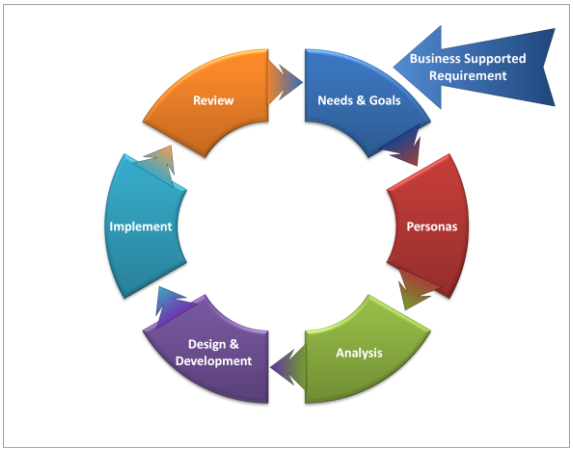

Figure 1: *Persona-Centred Information Security Awareness Cycle*

Proceedings of British HCI 2016 – Fusion, Bournemouth, UK.

Step one of process identifies business needs, goals and chosen awareness theme based on 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 technologies ensuring the process remains up-to-date, then continues on to repeat the cycle of activities and chosen awareness theme.

3. THE RESULTS

We validated this process by devising a security awareness programme for a digital design agency. Based on the evaluation of business needs & goals, Social Engineering was chosen as the required theme for the cycle. We identified that awareness built into daily or weekly activities, preferably bite-size and to-the-point with user-friendly language would best suit the culture.

We created personas based on transcripts from nine interviews with randomly selected employees. These resulted in the creation of three personas, Andy from IT Support in his 20's, Felicity a Developer in her 30's and Rob and Section Manager in his 40's. From a review of the business needs & goals along with persona perceptions & behaviours, this helped focus the awareness needs in context of the business activities and culture, which enabled recommendations of suitable communication methods for the awareness cycle.

We found that the design of the personas allows for their further integration, where the personas may be considered by employees in scenario-based contexts of business interaction. For example, this may be in a factsheet, or booklets indicating what Andy, Felicity or Rob may do in a given attack scenario, such as Social Engineering.

One implementation approach we tested used the personas as attack victims when playing a Social Engineering card game (Beckers and Pape, 2016), which proved to be a useful tool for creating discussion and awareness around Social Engineering. For example, during the game it was identified that Andy may be specifically vulnerable to Voice of Authority attacks, which validated 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 persona.

The personas offered a good level of value towards tailoring business needs within the design process. The personas were perceived to be a good account of an archetype within their roles and reflected their needs, leading to a tailored awareness programme. It would, however, have been beneficial to produce personas covering a range of less technical roles, although it was accepted there was a limited availability of interviews given the timeframe.

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 scenario-based contexts 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 Social Engineering techniques may apply and be mitigated within their own roles and social activities.

Further consideration would however be required towards other approaches that may fully embed the personas within the programme output and culture to offer a stronger integration into the business, as limited testing time could not provide this.

A computer-based learning 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 procedure and with the use of internal marketing and visuals.

3. REFERENCES

Bada, M., Sasse, A, M., Nurse, J.R.C., 2015. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society 2015 Conference paper, p118-131.

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., Passingham, N., 2015. Awareness is only the first step: A framework for progressive engagement of staff in cyber security. UK: Hewlett Packard Enterprise. Available from: http://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf (Accessed on 22/02/16).

Beckers, K., Pape, S., 2016. A Serious Game for Social Engineering. Germany: Technical University Munich (TUM) and Goethe-University Frankfurt.

Cooper, A., Reimann, R., Cronin, D., Noessel, V., 2014. About Face: The Essentials of Interaction Design Cooper. 4thEd. USA: John Wiley & Sons.

Hochleitner, C., Cornelia Graf, C., Manfred Tscheligi, M., 2013. Do You Enjoy Getting Gifts? Keeping Personas Alive Through Marketing Materials. Proceeding CHI EA '13 CHI '13 Extended Abstracts on Human Factors in Computing Systems, Pages 2355-2358, ACM New York, NY, USA 2013.

Lewis, M. M., Coles-Kemp, L., 2014. Who says personas can't dance?: The use of comic strips to design information security personas. Proceedings CHI EA '14 CHI '14 Extended Abstracts on Human Factors in Computing Systems, Pages 2485-2490, ACM, NY USA 2014

Nielsen, 2012. Personas - User Focused Design. Human-Computer Interaction. London: Springer.

PwC, 2015. 2015 Information Security breaches survey. UK: PwC. Available from: http://www.pwc.co.uk/audit-assurance/publications/2015-information-security-breaches-survey.jhtml (Accessed on 01/08/15).

Wilson, M., Hash, J., 2003. National Institute of Standards and Technology - NIST: Building an Information Technology Security Awareness and Training Program. USA: NIST/Computer Security Division Information Technology Laboratory. Available from: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (Accessed on 01/02/16).