Persona-centred information security awareness.

KI-ARIES, D. and FAILY, S.

2017

COMPUTERS & SECURITY 70 (2017) 663–674

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Persona-centred information security awareness

Duncan Ki-Aries *, *Shamal Faily*

Bournemouth University, Department of Computing & Informatics, Fern Barrow, Poole, UK

ARTICLE INFO

Article history:
Received 24 January 2017
Received in revised form 27 July 2017
Accepted 1 August 2017
Available online 9 August 2017

Keywords:
Information security
Security awareness
Risk
Human factors
Personas

ABSTRACT

Maintaining Information Security and protecting data assets remains a principal concern for businesses. Many data breaches continue to result from accidental, intentional or malicious human factors, leading to financial or reputational loss. One approach towards improving behaviours and culture is with the application of on-going awareness activities. This paper presents an approach for identifying security related human factors by incorporating personas into information security awareness design and implementation. The personas, which are grounded in empirical data, offer a useful method for identifying audience needs and security risks, enabling a tailored approach to business-specific awareness activities. As a means for integrating personas, we present six on-going steps that can be embedded into business-as-usual activities with 90-day cycles of awareness themes, and evaluate our approach with a case study business. Our findings suggest a persona-centred information security awareness approach has the capacity to adapt to the time and resource required for its implementation within the business, and offer a positive contribution towards reducing or mitigating Information Security risks through security awareness.

1. Introduction

Information Security issues are now prevalent concerns for organisations, specifically where issues directly impact upon regulatory, risk-based or reputational concerns resulting from intrusions and losses of data. Industry reports such as the PwC 2015 Data Breach report (PricewaterhouseCoopers LLP, 2015) highlight a large number of internal data breaches are still directly attributed to human factor issues, either intentional, accidental or with malicious intent. Businesses can no longer rely solely on process and technology for risk reduction of security issues, and need a greater consideration towards people integration with process and technology.

Although mandated for some, security education, awareness and training can support general understanding of issues through mandatory or annual refresher content. Several approaches exist for addressing security awareness, however, their focus is generally towards achieving compliance aspects. For example, applying and maintaining data confidentially, integrity and availability risk reducing controls. In most cases, a blanket approach would be applied without tailoring to the actual human factors involved. Human interaction that is central to business, processes, and system interaction therefore needs to be understood if security awareness needs are to be effectively addressed.

Research suggests current security awareness approaches do not entirely meet this requirement of designing for the user.

* *Corresponding author.*
E-mail addresses: dkiaries@bournemouth.ac.uk (D. Ki-Aries), sfaily@bournemouth.ac.uk (S. Faily).
http://dx.doi.org/10.1016/j.cose.2017.08.001

As a means to bridge this gap, an opportunity is presented to explore Human Computer Interaction (HCI) techniques that could be incorporated into a security awareness approach. We illustrate the application of such techniques through the use of *personas*. Personas are archetypical descriptions of users that embody their goals (Cooper, 1999). By representing archetypes of business users, personas offer insights into users that may otherwise be overlooked. Personas as user models can also be useful for identifying threats, vulnerabilities and likely areas of risk in their given environment (Faily and Fléchais, 2010a). The output of the personas could, therefore, be used to tailor security awareness needs using relevant topics and content addressing current business and people risks. Personas may also be incorporated into the awareness content itself, or potentially used for other process and procedure modification or security and risk assessment purposes.

To explore the potential of adopting a user-centred approach to security awareness, this paper illustrates an approach where the creation and application of personas was used to address business specific human factors within awareness activities. Our approach uses personas as a means of identifying audience needs and goals for security awareness requirements. These aim to address relevant human factors to reduce risk and improve a security minded culture. To demonstrate how personas may be integrated into an on-going cycle of security awareness, the steps taken leading to the design and implementation are incorporated within six on-going awareness programme steps. These build on positive features of other awareness approaches where they apply, making it relevant to persona integration and business tailored security awareness output. This can be embedded into business-as-usual activities with 90-day cycles of awareness themes to ensure a more frequent up-to-date approach towards addressing relevant security risks through security awareness.

To provide an overview in support of our approach, we begin by first considering existing frameworks and communication approaches for security awareness in Section 2. We consider current challenges, benefits and drawbacks, and how the use of personas may be integrated. Based on the research findings, we address the research gap by presenting a process for a persona-centred methodology in Section 3, integrating personas to help identify and reduce risk through tailored security awareness. Findings from testing elements of the approach with a case-study business, referred to as Company X, are detailed throughout Section 4. In Section 5 we discuss observations from the application of one approach towards combining HCI techniques into security awareness design requirements, aiming to reduce or mitigate Information Security risks. We then conclude in Section 6 and detail directions for future work.

2. Related work

2.1. *Information security awareness challenges and opportunities*

Raising awareness and changing security behaviour can be challenging, given the audience must be engaged with the reality of threats, and understand the process for identifying and addressing issues or concerns. The audience must then be motivated into applying positive behaviours, change risk perceptions (Roper et al., 2006) and engrained behaviours, supported by relevant topics that are not overly information-heavy (ENISA, 2006).

Challenges identified by Bada et al. (2015) found annual awareness and compliance orientated programmes were often treated as tick-box exercises and do not always lead to desired behaviours. Some approaches rely on invocations of fear to change behaviours, or result in a lack of motivation and ability to meet unrealistic expectations, which may derive from poorly designed security systems and policies (Bada et al., 2015). In some cases, security awareness goals were clearly identified and communicated. However, on a cultural level, people did not feel a need to browse internal security guidance as users did not believe they had security concerns (Maqousi et al., 2013). Some felt a lack of reward or recognition for applying positive behaviours, or did not feel empowered to make information or technology security decisions (Dominguez et al., 2010).

Awareness programmes were more likely to be successful when receiving top-level buy-in, business-wide support engaging with awareness, commitment and co-operation towards a security culture, using a participative creative design process tailored to business needs. Awareness should be communicated by a variety of means relevant to the business, its people and culture, and is best reinforced using an on-going 90-day programme (Manke and Winkler, 2012).

Delivery of awareness content should be engaging, appropriate and on-going, with a range of relevant topics that are targeted, actionable, doable and provides feedback to help sustain people's willingness to change (Bada et al., 2015). Communications must reinforce each other with a consistent message delivered across a number of channels to a culture addressed in a synchronous manner that supports the goals of the awareness programme (Beyer et al., 2015; Roper et al., 2006). Also, consider effectiveness across genders, generations or roles, of focusing on communicating how to achieve something, rather than dictating what should not be done (Manke and Winkler, 2012).

Baseline measures should be taken to establish needs and metrics relevant to the target audience and programme output (ENISA, 2006). Measuring the level of awareness is, however, more complicated, given that questionnaires can indicate a level of knowledge, but may not imply levels of motivation to improve behaviours (Bada et al., 2015). Awareness evaluation may be built-in using evaluation cycles embedded into the programme's awareness activities, and be considered at levels of Management, Audience, and Effectiveness against measurable performance objectives of awareness topics (Roper et al., 2006). Breach notifications or queries may also increase, therefore clarity may be required as to whether more issues are occurring or the increases are due to raised awareness (Roper et al., 2006).

An awareness programme should use simple consistent rules of behaviour for employees, offering increased perception of control and better acceptance of suggested behaviours. Cultural differences in risk perceptions should be considered when

embedding positive security behaviours with support, knowledge and awareness (Bada et al., 2015).

2.2. *Information security awareness approaches*

Responsibility, trust, communication, and co-operation are said to be the four cornerstones of an engaging security culture. Using an approach that motivates and empowers employees to play an active role in security is important towards achieving awareness and positive behaviours. Awareness output should be tailored to employees' organisational context, addressing specific security needs on an on-going basis to reinforce awareness, embedding security practices into normal routine of a security minded culture (Beyer et al., 2015).

ENISA (2006) awareness initiatives use a three-phase approach of Plan and Assess, Execute and Manage, Evaluate and Adjust. This includes sub-steps considering resource, budget, project team, programme materials, defines goals and objectives, programme implementation, evaluation of effectiveness, and considers updates ready for the next cycle to begin when required (ENISA, 2006).

The NIST special publication by Wilson and Hash (2003) offered a comprehensive guide towards designing, developing, implementing and maintaining a framework using a lifecycle approach to address Information Security risks and awareness. A needs assessment would first be conducted establishing business needs, risks, resource, geography, roles, responsibilities, budget and other project related dependencies (Wilson and Hash, 2003). Following implementation, feedback mechanisms with manual and automated monitoring and tracking should assist measurement of the programme's effectiveness. Furthermore, new approaches, policies, procedures and technology should be considered and incorporated into revisions of the programme, ensuring it remains effective and up-to-date (Wilson and Hash, 2003).

Other similar life-cycle approaches include The Security Culture Framework (Roer, 2015) that offers a generic approach towards promoting security awareness. This aims to set organisation goals and measures, involve the right people in the project cycle, understand the audience and build trust, choose relevant activities and topics, then plan, execute, measure and revise the programme (Roer, 2015). Alternatively, the Security Awareness Cycle (Mannerud, 2014) establishes baseline metrics, identifies the relevant audience, desired behaviours and high risks, and solutions to facilitate a behavioural change mitigating risks (Mannerud, 2014). Whereas, the framework by Maqousi et al. (Maqousi et al., 2013) had similar steps, but gave a specific focus towards methods of delivering computer and web-based security awareness.

An awareness programme can also be approached as a branded marketing activity promoting Information Security to employees as a product. This incorporates techniques such as surveys and focus groups to understand required design content and context, with added branding addressing elements of emotions, values, impressions and expectations, supported by relevant security metrics (Hinson, 2013).

Awareness content and communications may cover a range of delivery methods and topics applicable to business requirements and available resources. This should incorporate ease of use, scalability, interactivity, and accountability, with continued improvement being a main goal (Wilson and Hash, 2003). Awareness material should be developed towards relevant roles, behaviours and required skill-sets applicable to functions (Wilson and Hash, 2003). Another approach uses an on-going life-cycle for the awareness communications avoiding ineffective repetitive general advice, and tailored to business needs and behaviours (Beyer et al., 2015). Communication methods could include participatory methods such as games, quizzes, short video clips, or short topic briefs included as part of team meetings, which may incorporate rewards or recognitions for positive behaviours (Beyer et al., 2015). Other methods include face-to-face training sessions, e-mail messages, presentations by speakers (Dominguez et al., 2010), guidelines, booklets, posters, and awareness training workshops.

Gundu and Flowerday (2013) note that security campaigns may require additional budget in terms of direct and indirect costs included in production and maintenance of the programme, although it is suggested that use of e-learning can reduce distribution costs (Gundu and Flowerday, 2013). Online tools could also enable greater user interaction, such as online forums, news sections, alerts, and surveys. This could be delivered by a range of web-based tools, and maintained with appropriate up-to-date content. A review of relevant awareness metrics could then be conducted by specific reviewing team, or administrative and technical staff (Maqousi et al., 2013).

2.3. *Persona research*

Many of the awareness frameworks and approaches reviewed relied on some form of data collection to understand the environment, and in varying degrees, its people and culture. Personas – archetypical descriptions of users that embody their goals – could instead be used as a tool primarily within the design stage to address these areas. Within focus groups or team meetings, considering how personas might behave is also a useful technique for on-going awareness building. Rather than modelling inaccurate general stereotypes of users, the use of personas representing archetypes of business users can be used. This approach was arguably first popularised by Cooper (1999) and has since grown in their usage across different domains, such as marketing, websites and interface designs using varied design approaches.

Nielsen (2015) identifies four common design approaches used for personas:

- A goal-directed perspective that considers psychological aspects of the design process;
- A role-based approach focusing on specific target roles and collects a range of data through qualitative and quantitative methods;
- A fiction-based perspective usually designed using intuition or assumptions to formulate the personas;
- An engaging perspective created with the use of data.

According to Norman (2004), fiction based or assumptive perspectives are used to create an empathetic focus in the design process. Whereas, engaging perspectives provide a story-oriented approach towards visualising character descriptions using a narrative building the story's beginning, middle and

end (Nielsen, 2015), supported by story and scenario contexts (Madsen and Nielsen, 2010).

When creating personas, the design team is likely to include a range of roles (Pruitt and Grudin, 2003) who may begin by obtaining and analysing background information and data from various sources, leading to a view towards areas of user focus. This view may be debated, agreed and refined leading to representative personas that can be built upon with relevant supporting scenarios (Nielsen, 2012). Personas should be generative and engaging, using scenarios to apply them to relevant situations. This approach is similarly used in marketing where persona-focused storytelling is essential to branding (Herskovitz and Crystal, 2010).

Atzeni et al. (2011) provide an approach that aims to develop Attacker Personas using the process of data collection, reference elicitation, affinity diagramming to graphicalise the problem space, which helps with characteristic development, and concludes with the creation of the persona. Faily and Fléchais (2010a) adopt a user-centred design approach resulting in the creation of personas that may be used for a number of analysis purposes. Coupling personas with relevant scenarios and expected behaviours can be an effective means of validating the assumptions made.

Acceptance is an important feature of the design process, and is based on review, opinions or feedback from the design team's participatory interaction. If acceptance becomes an issue, it is necessary for designers to argue the characteristics of personas. Faily and Fléchais (2010b) illustrate an approach for doing this using Toulmin's Model of Argumentation to justify a claim about a characteristic, strengthening the foundations of the persona, while guiding the elicitation and analysis process. Personas may then be disseminated using programme specific scenarios, and should be reviewed annually to confirm the relevance of certain personas, carry out updates to the descriptions, or create new versions when required (Nielsen, 2012).

A more general approach taken by Stewart (2014) is based upon the Pareto principle, whereby in the context of security and awareness, 80% of the risk to be addressed derives from 20% of the topics to be covered. Therefore, the challenge of identifying relevant topics is addressed using personas. Interviews are undertaken with a target sample of the audience, which may equate to between 8–12 personas covering a range of departments. Relevant risks and behaviours towards security are assessed leading to the creation of targeted awareness materials, which may incorporate personas enabling their characters to become embedded within the organisation (Stewart, 2014).

The output incorporating the persona characters and communication of the persona-based awareness is suited towards internal or online means of standard communication, posters, or flyers. Hand-outs or novelty giveaway promotional items may also act as future guides or reminders towards awareness (Pruitt and Grudin, 2003). Research carried out by Hochleitner et al. (2013) gave a specific focus towards giveaway promotional items that integrated personas. This considered seven different marketing styled items providing information relating to each persona.

When comparing the effectiveness of long-living marketing materials against consumables, the consumables such as birthday cake, QR code cookies, or bottled drinks offered a fun and quirky interaction towards the personas, yet offered the least amount of information. Long-living materials such as a persona savings box or posters presented more information about the persona, but had the least interactivity. This suggested technological applications such as online quizzes could be incorporated to improve the efficiency and interactivity of long-living materials (Hochleitner et al., 2013).

Previous work by Pruitt and Grudin (2003) identified potential issues when using personas. For example, incorrect construction of personas without using relevant data led to unbelievable character types being created. Other issues include a lack of budget or resource towards the design, implementation, and suitable delivery methods. Or, the potential use of personas was not maximised, contributing to a lack of understanding towards how personas could be applied across the development and implementation cycles (Pruitt and Grudin, 2003). Personas may however be maximised by introducing initiatives such as a persona "Fact of the Week" campaign that could utilise email as a delivery medium.

In summary, for personas to be successful they should be grounded in data relevant to the business and their employees, and support focused requirements using participatory or cooperative design methods that give focus towards users. Integrating the personas with story-based scenarios to consider how they would apply to the persona can achieve engagement and anticipation towards user behaviours. Moreover, by maximising the use of personas this increases the likelihood of success within a programme (Pruitt and Grudin, 2003). Personas also have the potential to be used within the Social Engineering card game (Beckers and Pape, 2016) as an awareness activity in group or team meeting environments, or be integrated throughout the business embedding them into the culture.

3. Methodology

When considering the research of related work, despite a wealth of security awareness approaches, many focus on standard compliance related awareness topics. Very few, however, really consider relevant business-specific human factors identifying actual security awareness needs of people interacting with process and technology to support business goals. None offer a consistent HCI method of integrating human factors into security awareness using personas.

When designing for the user, the integration of HCI tools such as personas was found to offer requirements engineers or user-experience designers an important and useful means of understanding the user audience behaviours, needs and goals. Personas also offer potential towards security requirements for identifying risks (Faily and Fléchais, 2010a) that may otherwise have not been considered. The concept of using personas for awareness was discussed (Stewart, 2014) along with approaches towards incorporating personas in awareness materials (Hochleitner et al., 2013; Pruitt and Grudin, 2003).

To align HCI concepts with security awareness, we considered areas of benefit for integrating personas to identify business-specific needs and goals of users. This would aim to provide a means of addressing human factor related security risks, leading to a tailored approach to security awareness activities. From the review of current awareness approaches, we

Fig. 1 – Persona-centred information security awareness methodology cycle.

identified challenges and strengths of programme steps and communication approaches. The need for interaction, participation and co-operation was presented as a consistent theme adding greater success factors to awareness programmes.

We then considered how personas could integrate into a cycle of steps and activities for design and implementation of security awareness. Most widely used awareness approaches reviewed contained between 3–7 steps to establish: Needs and goals, for design and development, implementation, and a review and measure of effectiveness. Methods from these approaches best suited to assist the integration of personas were identified. This enabled general steps and considerations to form the basis of our proposed methodology, some of which were tested with Company X.

Fig. 1 shows the main steps of the life-cycle beginning with a preliminary step and continues with six on-going steps inheriting many of the positive consistent features discussed within Section 2. However, the key feature of this particular approach includes the use of personas at the design stage, with options for further use within the campaign communications. Personas could also be utilised outside of awareness activities addressing other security risks.

By following the steps of the methodology, we aimed to provide a framework offering specific, measurable, attainable, realistic and timely objectives towards meeting the goals. This allows flexibility of integration into business-as-usual activities, while adapting the process to suit business type and needs. The process can be maintained by a working group providing oversight and review on a quarterly or annual basis. Personas may then to be refreshed and updated, ensuring they continue to accurately reflect business user needs and security risks related to the current threat landscape.

3.1. *Preliminary step*

Before a programme can begin, it must be driven by a business need and supported requirement for implementation. To achieve this goal, a business decision to commit to on-going Information Security awareness should be given, with Senior management buy-in, support and commitment. A Stakeholder team of representatives from key departments across the business should be initiated, conducting introductory meetings to set up the initial project team and objectives. Inter-departmental co-operation towards engaging with awareness activities and promoting a security culture is paramount to its success.

3.2. *Step 1 - Needs and goals*

To focus and prioritise the programme output, activities are used to elicit business needs and goals towards Information Security awareness. These include assessments, surveys and focus groups to establish business needs and current security culture, locations, risks, roles, responsibilities, resource, budget, and any other identified project related dependencies. Current awareness threat trends should also be considered, together with issues or breaches where human behaviour was the likely root cause. A current snap-shot of metrics relevant to Information Security issues should also be established. Finally, general requirements and the target audience should be confirmed before choosing a theme, and conducting topic-specific research.

3.3. *Step 2 - Personas*

This step is perhaps the most crucial given the dependency on integrating personas as a tool to identify human factors and security risk. This should begin by organising interviews with a random selection of users from across the business. The interviews are used as a basis to gain necessary data for constructing personas. Interview questions should be prepared before conducting interviews for persona data collection to ensure context specific questions are incorporated.

Interviews can be recorded then user responses are transcribed to enable elicitation of relevant behaviours from data. Alternatively, good note-taking of interviews could be used, but is harder to elicit data in detail. The identified characteristics are written on post-it notes as factoids, then grouped based on behavioural clusters. Relevant information to support each persona are drawn from the grouped factoids then presented as affinity diagrams leading to the creation of persona templates. Based on findings from the empirical data, these templates are elaborated into detailed archetypes of typical users suitably tailored to the business.

Throughout the creation of personas, it is important to maintain traceability from the data to the finished persona to ensure the credibility of each persona and their characteristics. Artistic licence may be permitted when bringing to life the archetypical character, such as choosing a representative photograph to help humanise the persona, or describing their back story. However, to ensure they are archetypes, the core of the persona, e.g. their attitudes, motivations and business context, must be derived from the data. Each persona can then be presented in such a way to begin to reap the benefits of business-specific user models brought to life as recognisable employee archetypes.

When repeating the awareness cycle, personas may be reviewed during the following cycle, but may be replaced with new versions annually, or as required. This is to ensure that as the threats evolve, or security culture and awareness improves, personas continue to accurately reflect current business user needs and security risks, for which we can address through tailored security awareness.

3.4. *Step 3 - Analysis*

A critical analysis is undertaken against the identified behaviours and characteristics of each persona. This is considered against business needs, risks and requirements to establish and prioritise awareness needs. Using simple consistent rules of behaviour, desired behaviours can be considered with realistic expectations to integrate persona needs using scenario-based contexts. Business risks, issues, needs and goals are considered against persona roles, together with behaviours, cultural contexts, differences in risk perceptions, and the applicable skill-sets required to apply the learning. Stakeholders are encouraged to participate in the creative design process. Any other relevant points and observations can then be considered before target behaviours and areas for relevant awareness content delivery are agreed.

3.5. *Step 4 - Design and development*

Design requirements to address identified security risks are derived from critical analysis and topic-specific research. This provides direction for design and development of tailored content, whilst utilising available resources and means of communication.

Updates to future iterations that may currently be out-of-scope are considered for planning at a later stage, e.g. system-based awareness. Delivery methods and resources should be agreed considering ease of use, scalability, interactivity, and an element of accountability. Awareness that engages people on a personal level should be applied, which can motivate and empower employees to play an active role in Information Security.

Content requirements are specified for a consistent message delivered across various channels. Branding can be incorporated, making the material relevant and personalised to the organisation, its goals and people, promoting Information Security to employees as a product. Other required styling may be incorporated to address elements of emotions, values, impressions and expectations leading to relevant design content and context. How the personas can be incorporated into awareness material output can be considered, thus maximising their potential where possible.

Participatory design methods for communication may incorporate games, quizzes, short video clips, or short topic briefs included in team meetings. Also, posters, novelty or promotional items, Web and system-based development tools. Or, guidelines, booklets, on-going news sections, online and Social Media alerts, surveys, or forums. Industry proven security best practices could also be used to provide content of awareness material. There are a number of options available, however these should be tailored to the context of persona and business needs, using available resource and budget.

3.6. *Step 5 - Implement*

To ensure a timely implementation, a roll-out strategy should be prepared taking into account the required staff availability and other business priorities. The delivery of tailored content and communication methods around other priorities should be planned and implemented. Baseline metrics relevant to the audience and awareness cycle should be established, and the effectiveness of certain elements of the awareness activities is measured where required.

3.7. *Step 6 - Review*

The Review stage provides feedback-loops to identify the effectiveness, benefits, drawbacks, and improvements for the awareness cycle. Evaluation metrics might vary in type dependent upon the nature of the business, but may measure effectiveness of the awareness cycle against baseline metrics. On-going effectiveness may use feedback mechanisms, such as manual and automated logging, system and internet logging, monitoring and tracking. Also, issue reporting, root-cause analysis, Helpdesk trends, e.g. password resets, desk and environment spot-checks, surveys or questionnaires, internal Phishing or Social Engineering campaigns.

Review the findings to understand and agree required updates or modifications to policies, procedures, or the awareness process. Consider new technology or threats to be incorporated into subsequent revisions of the cycle, ensuring it remains up-to-date and effective against current business and persona needs. Continue back to Step 1, repeating the on-going 90-day cycle by first establishing the current business risks, threats and goals for the next cycle.

4. Applying the methodology – findings

To support design, implementation and testing of certain elements of the persona-centred awareness methodology, we applied our approach to a case-study business referred to as Company X. This specifically helped us validate the notion of personas being used as a means of addressing human factors security risks, for which guides the selection and design of tailored security awareness. Also tested were specific parts of the proposed process steps that could be used to integrate the use of personas within a security awareness cycle.

Due to limitations of the available time-frame for testing, combined with other business priorities for Company X, some task outputs from the preliminary step and Step 1 of the methodology were assumed to some degree. This was supported by interviews and observations confirming senior management and the business as a whole were already very security focused and committed. The willingness to participate in trying something new to improve their security awareness was another positive indication. Testing of the project therefore begins with the relevant theme and topic-specific research at the end of Step 1, findings of which are discussed in Section 4.1.

4.1. *Step 1 - Needs and goals*

Preliminary discussions with Company X took place to manage requirements and expectations, understand the culture,

business needs and goals. It was determined topics relating to Social Engineering would be the chosen theme for the current instalment of the awareness programme. Social Engineering can be described as means of manipulating people by deception into performing an action or giving out information (Mann, 2012), which can bypass or undermine other technological security controls.

Card games such as Ctrl-Alt-Hack are designed to help improve security awareness in group-based environments (Denning et al., 2013). A similar type of game developed by Beckers and Pape (2016) acts as a training activity on Social Engineering techniques with the aim of identifying possible weaknesses. As part of our topic specific research, we evaluated this Social Engineering card game, where a number of attack types were carried out by players against a pre-designed persona, their system or workstation. The game-play was at first a little slow whilst understanding the game mechanics, but improved with repetition, allowing focus to be on the awareness of attack types and styles. Participants had a good level of understanding towards the subject matter, so it was unclear how less technically experienced people may understand the game or terminology. This suggested the game may be an ideal candidate for implementation.

4.2. *Step 2 - Personas*

A number of approaches towards the design and use of personas were considered. Given the nature of the application and context of the business, a goal-based approach was largely adopted with some role-based elements. The process for persona creation can be viewed similar to that of Atzeni et al. (2011).

In preparation to begin the process, interview questions were created for data collection leaving scope for additional questions where required. These would aim to elicit relevant information from employees describing behaviours and perceptions relating to the business and Information Security. Nine interviews were conducted with randomly selected employees based on their availability during the interview day. According to Yin (2013), randomisation is also said to assist with data validity. The interviews offered insights into day-to-day life covering a range of roles and experience at Company X, demonstrating a generally security minded culture with a positive attitude towards Company X.

The audio recorded interviews were transcribed to give text-based accounts, then reviewed to identify relevant behaviours, characteristics and perceptions that could be extracted. The identified information was written onto post-it-notes and placed on a wall into categories based on the approach used by Cooper et al. (2014) to broadly identify:

Aptitudes – What education and training the user has, and ability to learn;
Skills – User abilities related to the product domain and technology;
Activities – What the user does, frequency and volume;
Motivations – Why the user is engaged in the product domain;
Attitudes – How the user thinks about the product domain and technology.

Through analysis, 281 relevant pieces of data were identified corresponding to various activities, behaviours and perceptions. These were sub-grouped into variable types such as internal and external motivations, or differing attitudes towards awareness, risks or challenges. The data were duplicated into the affinity diagrams for further visual analysis. The Activities grouping, for example, and its six distinct sub-groupings demonstrated a likely split in persona roles. It should however be noted that although the design approach for the personas lends itself towards a goal-based approach, it was useful to determine the likely roles to help with the representative split of the other data categories.

As a means of comparing the persona role data, Company X recommended the use of a Radar diagram to visually demonstrate the most common roles or activities from the data listed; these were often used within Company X when creating user-experience personas for system design purposes. After a number of tests, the best approach of comparing data in the diagram was to divide the generally perceived percentage of workload for each person interviewed, then re-order the rows of data relating to interviewees whereby the data visually flowed and activities crossed over various role types. For example, a typical person from IT may devote 100% of their day to technical activities, whereas a person at Manager level would split their time between client and team management or other activities.

Based on the output of data specific to the business, roles, users, and behaviours, it was determined that three personas could be derived, each of which presented relevant characteristics and behaviours to address. To keep within the context of Company X, gender and age of the personas were derived based on the interviewees. For example, persona one was based on two males and one female, generally in their 20's.

The remaining behaviour data were colour-coded consistent with the Radar diagram. This provided visual validation of relevant behaviours and perceptions applicable to each persona, enabling traceability from the persona to the affinity diagrams and relevant factoids applied, originating from business users. Images representative of each persona were sourced online under a Creative Commons License, enabling each persona to be viewed as a fictional person, bringing the three archetypes to life. The images were also helpful towards visualising and reflecting on the persona as an archetype, not a stereotype, when applying a story-based narrative aligned with the main behaviours and perceptions.

When validating the design of the personas with Company X, although the persona descriptions were deemed as appropriate representations of business users, the wordiness of the full personas was noted. Therefore, it was suggested that the descriptions could be broken into bullet points presenting an overview for each persona. This prompted development of a further Lite version of the personas, using another approach by Cooper et al. (2014) to identify each persona's Life, Experience and End Goals. The full personas were reviewed to identify descriptions within these categories and refined to a one-line summarised statement, resulting in a more concise overview for each persona.

It could be argued this summarising approach may have been used with the post-it-note wall, however, it was important to maintain a high degree of fact-finding and original

context as closely as possible. By doing this, the intention was to strengthen data validity by providing a true account within the main persona templates, allowing for further refinement if required. This reduces risk of persona characteristics becoming overly diluted or deviating from the data they were based on.

4.3. *Step 3 - Analysis*

With the personas designed and validated, Company X agreed relevant awareness needs and learning styles applying to each persona could be analysed. However, the lite-personas offered less applicable detail in comparison to the full personas, suggesting they may be better incorporated into outputs and communications. The full personas were therefore used to elicit relevant needs, points and observations indicating learning styles and level of detail required. This was achieved by considering how each persona would act or respond in a given business scenario. Their motivations, attitudes and understanding could then be analysed to identify any weaknesses towards security. The personas did, however, demonstrate a good level of understanding or existing awareness, and that some mechanisms were already successfully used within Company X.

During analysis, this information was further considered in the context of the company, its culture, current processes and procedures, workloads and the type of clients they work with, and how the theme of Social Engineering applies. Also of consideration were the Cyber Security Essentials (Gov.UK, 2015) and ISO 27001 (British Standards Institution, 2016) accreditations in place with the risks, needs and requirements for maintaining these. ISO 27001 audits were frequently carried out. Therefore, practising security was essential to the business given their types of clients, ranging from small businesses to government organisations, whereby security clearances were required for applicable employees. This was also reflected within interviews and observations, where certain information could not be discussed or revealed.

Findings from interviews and observations determined Company X operated primarily in one location with a secondary London office. The culture was fast-flowing, energetic, technology orientated and generally security minded. A positive ethos was evident with a desire to continually improve, being the best at what they do. Security needs were balanced, for example, with internet or Wi-Fi connections, where employees need web access for business and personal purposes to social media or streaming services, using varied systems or devices. Technological controls were, however, in place to integrate security seamlessly, many of which were beyond the users knowledge or control, supported by a number of relevant policies and procedures addressing human interactions.

The calibre of new and existing employees covering varied age ranges and backgrounds, appeared to be maintained to a high standard. New employees were given a detailed and well-presented company handbook, and follow a staggered induction programme to introduce the new starter to company life, expectations, policies and procedures, including general security awareness. Company stand-up meetings take place on a weekly basis for general updates, and other team meetings may be carried out when required. People matter to the business, so there was a good support structure in place and usage of the internal online system as the central portal for information was encouraged.

As with some employees, persona three occasionally travels to meet clients. External security awareness is a consideration for the business, as secure external access to systems for permitted employees was important for business operations. Clients and other visitors may also arrive at Company X for meetings, so there were layered security procedures and awareness on how this should be managed, along with procedures for discussing information with third-parties.

Most employees observed had a good level of understanding towards technological subjects and terminology. However, despite all three personas appearing technically minded, albeit at differing levels, some consideration should still be given towards less technical areas of the business or new starters.

The next stage of analysis reconsidered each of the persona needs from the context of the business overview. This established the most relevant approach towards design and implementation of awareness content tailored to business and audience needs. For example, workloads were high and time management was maximised where possible to meet business, client and security needs.

To be most effective, it was identified methods should therefore cause least interruption to daily activities, be interactive or participatory, and incorporated into existing team meetings. This could include the Social Engineering card game considered in Step 1, quizzes, short video clips, topic briefs, or guidelines, preferably bite-size and to-the-point with user-friendly language. This would likely suit all persona needs. However, for persona three, there was an appetite towards deeper and broader content for certain topics, and the use of industry-based social media security updates for threat awareness.

Awareness needs may be further supported by displaying relevant awareness posters, utilising the internal online system implementing awareness material, alerts and on-going news. Use of desktop backgrounds and screensavers was discussed with Company X. However, based on their usability experience, for desk-based employees background images are often obscured and overlooked, and screensavers become annoying after continual display over time. It was therefore concluded these may be counter-productive and would not be incorporated.

If budget permits, awareness styled novelty or promotional items maximising use of the lite-persona identities within the designs could provide opportunities for company branded take-away items. This was, however, out of scope for testing, as was the development and introduction of a system-based awareness tool. It was acknowledged such a system could offer a number of benefits incorporating refresher training and awareness exercises integrating the personas, and be supported by record keeping functionality. This would likely help reinforce awareness needs, thus preventing or reducing the likelihood and impact of security-based risks, and was a likely consideration for the future.

A cost-benefit-analysis may wish to be considered to examine advantages and disadvantages of developing a system in-house compared to that of existing third-party systems or

services. As with many awareness approaches, this may be difficult to quantify financially. However, when compared with the potential of costs, losses and reputational damage resulting from a data breach, the on-going system costs for an awareness tool or other recommended activities may be minimal in the long-term by comparison.

4.4. *Step 4 - Design and development*

After concluding the analysis in Step 3, recommended primary awareness communications were selected. These included the Social Engineering card game, short topic briefs, quizzes, factsheets, and short video clips, incorporated into existing team meetings. Secondary communications included relevant awareness posters, use of the internal online system to publish ongoing updates, short guidelines, booklets or factsheets, integrating personas where possible.

The thematic needs of Social Engineering awareness were considered against business-specific persona needs and behaviours. Findings indicated applicable topics should include visitor and ID badge requirements, prevention of unauthorised access to systems or buildings, shoulder surfing, reverse Social Engineering, insider targeting, and types of Phishing. Web users would benefit from awareness of online attacks such as waterholing and pop-up windows, and risks towards themselves or the business when using social media – and what to do in the event of these occurring.

In all cases, there should however be an acceptance towards areas of human factors that may be vulnerable and could therefore be improved upon. For example, persona one would specifically benefit from awareness of Voice of Authority or Third-party authorisation attacks. Persona three would benefit from awareness of preventing in-person Social Engineering attacks whilst working externally.

A number of these relevant topics were addressed by the Social Engineering card game. This provides for interactive and participatory awareness building towards risks of Social Engineering, where the purpose is to explore attack scenarios and approaches applicable to Company X. When designing the game board, it is suggested this should duplicate the actual business layout to benefit from its familiarity towards locations of systems, devices or other attack vectors. However, in agreement with Company X to reduce security risk towards the business, a generic floor plan was instead created with some basic similarities, meaning it was still fit-for-purpose meeting the needs of Company X.

Within the game, each player would carry out an attack on one of the personas using the cards selected. The persona would be allocated their workstation within the game board. The attacker has to determine whether they are an insider or outsider, and how they would gain access to the building, systems or data relevant to the persona. As a group, the likelihood of applicability and success of the attack type is discussed, then concludes a score for the player, before moving on to the next player.

Secondary communications may incorporate posters from online awareness resources, a selection of which were printed and discussed with Company X. These covered Social Engineering topics ranging from simple and to-the-point, detailed, graphical, movie style and comical cat posters. When considering the personas and culture, Company X determined the comical cat posters would likely be most accepted.

Continuing to support the theme, quizzes could offer fun bite-sized awareness. One option was to use free and reputable online quizzes (GetSafeOnline, 2016; OpenDNS, 2016) or a downloadable Phishing e-learning module (TheSecurityAwarenessCompany, 2015), used individually or as a fun group or team meeting awareness building exercise. An introduction to the team meeting and the theme of Social Engineering could utilise short videos, such as an interview with insights from professional Social Engineer Jenny Radcliffe, who touches on many key points relevant to businesses and Social Engineering (Infosecurity Europe, 2015).

Company X determined future iterations of the cycle could include awareness videos made with in-house technology, or demonstrations could be arranged to show the ease of system exploits. Internal Phishing campaigns could be developed, or a Social Engineer Penetration test could be arranged. However, before activities of this nature would be implemented, it was confirmed considerable discussions should take place to identify advantages and disadvantages of such a test. For example, where this may create a risk of distrust between the business and its employees. The focus therefore prioritised the implementation approach agreed with Company X based on the personas.

4.5. *Step 5 - Implement*

As time required for full implementation and review would fall outside of the testing time-frame with Company X, it was agreed a primary and secondary communication method would be tested. Testing of the secondary supports validation of the targeted awareness material and design based on persona needs. Aspects of this are considered when testing the primary method that supports validation towards incorporating personas within awareness output.

Two simulated team meetings were used whereby the card game and a review of preselected awareness posters could be tested. Each meeting lasted up to an hour, with the first group consisting of four employees from more technical roles. The second group had three employees from less technical roles, supported by the security manager with the game-play. Both groups were introduced to the purpose of the meeting, the design and use of personas, and how they applied to company awareness, the game and floor plan.

The more technical group were able to understand game terminology, scenarios and principles with ease. Much discussion time was spent debating in technical terms how attacks may be improved at the company using particular approaches or technology. The less technical group were slower by comparison to understand the game, and were appreciative of the manager support helping describe attack scenarios and principles by relating them to the business using analogies. This promoted further discussion where they identified techniques that may be used in the public domain. Both groups engaged in fun discussions throughout each round of the game, demonstrating to some degree the game was creating awareness through discussion based on the game content. In both cases, the floor plan became almost redundant and instead

relied on discussion and visualisation to walk-through attacks within the company.

The concept of using personas to identify and tailor awareness needs and their integration into the game output was generally understood. However, for game-play, group members did not have time to fully absorb the persona templates, and were more distracted by the need to understand the concept of the game and Social Engineering. Participants found the use of personas as victims was useful, as most group members could imagine working with them or having similarities to other employees. For example, both groups identified persona one was susceptible to Voice of Authority attacks. Interestingly, this part validated findings of Step 4 where this was previously identified.

Some group members felt a focus on how they themselves may be a victim would have been more useful. That said, throughout the game, there were constant reflections on how the scenarios may apply to themselves, colleagues or even their family. Therefore, it could be argued this need was still met, thus promoting awareness.

After game completion, group members individually provided feedback towards the game and its integration with personas. The remainder of the session then turned focus towards the preselected awareness posters. Ten posters were sourced online and two posters were created to represent a theme that was basic and to-the-point. Group members individually reviewed the posters, considering which posters they believed would be appealing and effective in raising awareness within the company culture. This offered a sense of empowerment and participation towards internal awareness activities. The findings of the game and poster reviews are discussed in Section 4.6.

4.6. *Step 6 - Review*

Given the project time-frame and other business priorities, it was not possible to obtain a baseline metric towards measuring the effectiveness of the awareness cycle. Furthermore, at the conclusion of the activities, it was not appropriate to apply and review manual or automated feedback mechanisms suggested in previous sections. These were considered long-term measures that would be reviewed after the completion of the cycle that would end outside of the time-frame working with Company X.

However, in addition to the verbal feedback from management and staff regarding the integration of personas, two opportunities were used to offer feedback towards the effectiveness of the awareness activities. Following this feedback process assisted in validating certain parts of the process. A game review form was used to gain feedback towards the Social Engineering card game that integrated personas assisting in raising awareness of Social Engineering techniques. A poster review form and guide sheet was used to gain feedback towards the likely appeal and effectiveness of the awareness posters, previously selected based on the personas.

Poster findings demonstrated a varied appeal in both groups, as individuals had differing likes and dislikes towards the ascetics, wording or overall appeal and use in the company culture. This suggested that regardless of the gender, age or technical expertise, each person had different tastes, meaning a range of posters should be considered. Feedback indicated which posters were likely to have a positive impact, although the long-term impact would need to be considered at a later stage, considering whether they would be overlooked after the 90-day cycle. Interestingly, the cute comical cat posters were considered fun and humorous, which suited the culture, although other posters could still be an option. This finding in particular validates where Company X determined in Step 4, based on the personas the comical cat posters would likely be accepted.

Game findings suggested it was well received and did promote awareness. The more technical group members felt they were more familiar with the topic and gained the least awareness, although once the game-play was understood, the less technical group gained the most security awareness.

When combining these findings together, we found that participants were at first unsure or unaware of the persona concept. They were more used to stereotypes found online or in magazines. Once they understood these were instead archetypes based on real data from their colleagues, they were able to appreciate the benefits better. This was evident throughout the game where participants could identify with them as other employees. At an employee level, the personas were more visible within the output, but gave less focus towards the awareness being based on personas. Whereas, at management level, the benefits of using personas as a means for identifying human factor security risks was accepted as an approach towards tailoring awareness, although integrating them within output was secondary.

5. Discussion

The aim of our work was to develop a user-centred approach integrating the use of personas to identify business-specific human factors and security risk to be addressed within awareness activities. To enable the integration of personas with awareness activities, a persona-centred on-going Information Security awareness solution was proposed. This aimed to reduce or mitigate related Information Security risks through business tailored security awareness output.

However, to test these concepts, the project required a case-study business for data elicitation to build personas based on their employees, and tailor subsequent activities to its business needs. Despite approaching companies in good time, some difficulties were experienced in securing a company to work with. Although candidates provided positive feedback, the reality was, companies were unable to support the project. Either with time constraints, provide any type of supervisory support, resource or budget, regardless that much of the project would be delivered at no cost, compared to the use of external consultant services. From a different perspective, this demonstrates the reality businesses face when considering, planning or implementing such a programme, when other priorities, budgets and resource are already stretched.

Company X kindly offered their assistance to test and validate our work. However, as there was insufficient time for Company X to plan or build this project into weekly activities, some limitations would apply. Working with Company X enabled testing of many features from the proposed methodology, providing the business a means for implementing on-going

awareness. Company X were consulted at each stage of the process, considering research findings leading to the general approach and application of the persona-centred methodology, creating a cycle of activities tailored to business and persona needs.

Considering threats to validity described by Yin (2013), e.g. Internal, External, Construct and Reliability validity, we first consider the notion that personas can be used as a tool to elicit behaviours and characteristics from a given audience. Once developed from empirical data, personas were specifically validated with Company X who agreed their appropriateness. The elicitation of human factor security risks from the personas leading to tailored output was part validated with Company X at selection stage, and again from participant feedback at implementation and testing. Data quality from persona findings is likely to be subject to the ability and understanding of those applying the process and resources available. Business type and context may impact on external validity with differing results, yet will still provide empirical data.

To assist the integration of personas into an awareness process, we identified consistent process steps from other common frameworks and approaches to create a structured persona-centred methodology. This also helps with construct validity by defining the problem space and steps to address it, and reliability validity to ensure process repetition. The full validity of the process was more difficult to confirm due to shortened time-scales for testing. Elements described that were tested enabled a useful and structured means of applying the personas in each step. For example, once elicited, tailored awareness needs could then be matched to the business context with optimal communication methods using available resource.

Although full testing of the process as an on-going cycle could not completed, feedback gained from activities tested suggested an approach using personas has potential benefits towards addressing security related human factors. Communication methods of a card game and posters generally worked for Company X. In combination, this helped raise most individuals awareness, albeit at differing levels, and had positive effects on creating participatory discussion promoting a security minded culture.

6. Conclusion

We presented the development and application of a persona-centred on-going Information Security awareness solution for the workplace. Specifically, we tested the concept of designing for the user by integrating personas. This HCI approach is used to bridge the gap between standard awareness approaches by incorporating business-specific human factor security risks, leading to tailored security awareness output. A review of related work, personas, approaches and frameworks was undertaken to understand how such an approach could be combined. From this, a persona-centred methodology was devised and largely tested with a case-study business.

Personas were constructed based on empirical data relevant to the business, providing a useful means to identify audience awareness needs, communicated with a predefined security theme for the programme cycle. However, the personas generated were generally based on more technical roles. Collection of data from less technical roles providing a balanced spread of the business audience would be more appropriate when fully applying this methodology in a real-world scenario.

Individual persona roles could also be used to identify needs at a team or department level, or for other related purposes. For example, application to security risk assessment, or related control and procedure modifications. Despite test environment limitations, personas appeared to offer a good level of value towards the design process, demonstrating potential for their overall effectiveness as a persona-centred tool for addressing human factors in security awareness.

In both workload and analysis, work conducted with personas took time to produce and validate, yet provided a useful and relevant method for tailoring security awareness needs. It was, however, unclear how effective selected activities would be over time towards changing and improving behaviours. Further consideration may need to be given towards embedding personas into the business and awareness programme output, such as promotional take-away items.

Having carefully and methodically considered appropriate steps and tasks for the persona-centred methodology, application of the process with Company X appeared to work well and offered value towards an area they wished to improve upon. Although Company X were already very security minded, the test subjects appeared to benefit from activities that could, for example, be participative and incorporated into a team meeting, providing an indication the application of the methodology was positive.

By continuing to embed this process into business-as-usual activities, it is likely this process could be adapted to suit business needs, whilst providing the flexibility to evolve. This also gave Company X ideas of how other updates may be delivered. The inclusion of a system-based tool for computer based training and awareness was considered a future advantage for extending awareness.

Further work relating to the programme's long-term effectiveness of improving behaviours, reducing risks and embedding security into an unconscious routine, would also be of interest to validate its long-term effects. To further enhance its validity, this process may also be trialled in a smaller less security orientated business, or indeed as part of a larger national organisation to observe any differences in the approach required. That said, the process is presented at a level whereby the steps could be followed in most scenarios, or integrated with other risk or awareness approaches, retaining the main feature or novelty of our approach using personas; archetypes based on real business users, needs and behaviours, as a means for identifying workplace security awareness needs.

REFERENCES

Atzeni A, Cameroni C, Faily S, Lyle J, Fléchais I. Here's Johnny: A methodology for developing attacker personas, in: Availability, Reliability and Security (ARES), 2011 Sixth International Conference, IEEE; 2011, pp. 722–27.

Bada M, Sasse A, Nurse JRC. Cyber security awareness campaigns: Why do they fail to change behaviour?, International Conference on Cyber Security for Sustainable Society 2015 Conference paper; 2015. 118–31.

Beckers K, Pape S. 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; 2016, pp. 16–25.
Beyer M, Ahmed S, Doerlemann K, Arnell S, Parkin S, Sasse AM, et al., Awareness is only the first step: A framework for progressive engagement of staff in cyber security, techreport, Hewlett Packard Enterprise; 2015. Available from: https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf. [Accessed 22 February 2016].
British Standards Institution, BS ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements [Electronic version]; 2016.
Cooper A. The inmates are running the asylum. Macmillan Publishing Company Inc; 1999.
Cooper A, Reimann R, Cronin D, Noessel C. About face: the essentials of interaction design. John Wiley & Sons; 2014.
Denning T, Lerner A, Shostack A, Kohno T. Control-alt-hack: the design and evaluation of a card game for computer security awareness and education, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security, ACM; 2013, pp. 915–28.
Dominguez CMF, Ramaswamy M, Martinez EM, Cleal MG. A framework for information security awareness programs. Issues Inf Syst 2010;11(1):402–9.
ENISA, Users guide: How to raise information security awareness; 2006. Available from: http://www.iwar.org.uk/comsec/resources/ENISA/infosec-awareness.pdf. [Accessed 1 February 2016].
Faily S, Fléchais I. Barry is not the weakest link: Eliciting secure system requirements with personas, in: Proceedings of the 24th BCS Interaction Specialist Group Conference, British Computer Society; 2010a, pp. 124–32.
Faily S, Fléchais I. The secret lives of assumptions: Developing and refining assumption personas for secure system design, in: International Conference on Human-Centred Software Engineering, Springer; 2010b, pp. 111–8.
GetSafeOnline, Get safe online safety test, GetSafeOnline; 2016. Available from: https://www.getsafeonline.org/quiz/. [Accessed 22 March 2016].
Gov.UK, Cyber essentials scheme: overview. Department for Business, Energy & Industrial Strategy, Gov UK; 2015. Available from: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview. [Accessed 1 February 2016].
Gundu T, Flowerday S. Ignorance to awareness: towards an information security awareness process. SAIEE Afr Res J 2013;104(2):69–79.
Herskovitz S, Crystal M. The essential brand persona: storytelling and branding. J Bus Strategy 2010;31(3):21–8.
Hinson G. Raising security awareness through marketing: Seven steps to promote your information security brand, IsecT; 2013. Available from: http://www.noticebored.com/Raising_security_awareness_through_marketing.pdf. [Accessed 10 September 2015].
Hochleitner C, Graf C, Tscheligi M. Do you enjoy getting gifts?: Keeping personas alive through marketing materials, in: CHI'13 Extended Abstracts on Human Factors in Computing Systems, ACM; 2013, pp. 2355–8.
Infosecurity Europe, Jenny Radcliffe Interview, Youtube; 2015. Available from: https://www.youtube.com/watch?v=_WhD3vMeLe8. [Accessed 22 March 2016].
Madsen S, Nielsen L. Exploring persona-scenarios-using storytelling to create design ideas. In: Human work interaction design: usability in social, cultural and organizational contexts. Springer; 2010. p. 57–66.
Manke S, Winkler I. The habits of highly successful security awareness programs: A cross-company comparison, Tech. rep., Secure Mentem and Internet Security Advisors Group, USA; 2012. Available from: http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf. [Accessed 25 January 2016].
Mann I. Hacking the human: social engineering techniques and security countermeasures. Gower Publishing, Ltd.; 2012.
Mannerud TA. The security awareness cycle, Tom A Mannerud; 2014. Available from: http://www.mannerud.org/2014/10/04/the-security-awareness-cycle/. [Accessed 22 January 2016].
Maqousi A, Balikhina T, Mackay M. An effective method for information security awareness raising initiatives. Int J Comput Scie Inf Technol 2013;5(2):63.
Nielsen L. Personas-user focused design, vol. 15. Springer Science & Business Media; 2012.
Nielsen L. The Encyclopedia of human-computer interaction. 2nd ed. Aarhus, Denmark: The Interaction Design Foundationn; 2015 [Chapter 30]. Available from: https://www.interaction-design.org/encyclopedia/personas.html. [Accessed 10 February 2016].
Norman DA. Emotion design: why we love (or hate) everyday things. Basic Books; 2004.
OpenDNS, Phishing quiz, OpenDNS; 2016. Available from: https://www.opendns.com/phishing-quiz/. [Accessed 22 March 2016].
PricewaterhouseCoopers LLP, 2015 Information Ssecurity breaches survey, PricewaterhouseCoopers LLP; 2015. Available from: http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html. [Accessed 1 August 2015].
Pruitt J, Grudin J. Personas: practice and theory, in: Proceedings of the 2003 conference on Designing for user experiences, ACM; 2003, pp. 1–15.
Roer K. The security culture framework, The Security Culture Framework; 2015. Available from: https://securityculturefframework.net/. [Accessed 12 August 2015].
Roper CA, Grau JJ, Fischer LF. Security education, awareness, and training: from theory to practice. Butterworth-Heinemann; 2006.
Stewart G. Personas for security awareness. ISSA Int J 2014;12(1).
TheSecurityAwarenessCompany, Phishing ILM, TheSecurityAwarenessCompany; 2015. Available from: http://free.thesecurityawarenesscompany.com/downloads/phishing-ilm/. [Accessed 9 April 2016].
Wilson M, Hash J. Building an information technology security awareness and training program, NIST Special publication 800; 2003. 50. Available from: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. [Accessed 1 February 2016].
Yin RK. Case study research: design and methods. Sage publications; 2013.

Duncan Ki-Aries is a Cyber Security PhD Research student in the Department of Computing & Informatics at Bournemouth University. His PhD research is specifically looking at Risk Assessment in Complex Systems of Systems (SoS), which incorporates a number of research areas of interest, such as System of Systems Engineering (SoSE), Interoperability, Risk Management, Security, Awareness, Trust, Privacy, Usability, and Human Factors.

Dr Shamal Faily is a Senior Lecturer in the Department of Computing & Informatics at Bournemouth University. His research explores how security can be designed into software systems. In particular, he aims to understand how interaction design techniques and software tools can be used to build and maintain systems that are not only secure, but also usable within different contexts of use. As such, Shamal's research interests are at the intersection of Cyber Security, Software Engineering, and Human-Computer Interaction (HCI).