World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:8, 2014

Developing a Viral Artifact to Improve Employees' Security Behavior

Stefan Bauer, Josef Frysak

***Abstract*—**According to the scientific information management literature, the improper use of information technology (e.g. personal computers) by employees are one main cause for operational and information security loss events. Therefore, organizations implement information security awareness programs to increase employees' awareness to further prevention of loss events. However, in many cases these information security awareness programs consist of conventional delivery methods like posters, leaflets, or internal messages to make employees aware of information security policies. We assume that a viral information security awareness video might be more effective medium than conventional methods commonly used by organizations. The purpose of this research is to develop a viral video artifact to improve employee security behavior concerning information technology.

***Keywords*—**Information Security Awareness, Delivery Methods, Viral Videos, Employee Security Behavior.

I. Introduction

A multitude of risks threatens the operational business of organizations, which nowadays often grounds on insecure application of information technology and information systems. According to industry reports, the number of information security incidents increased in the last decade [1]. Operational risks faced by organizations may be triggered by systems, humans, processes or external causes. Previous research identified humans as major enablers for loss events, especially if humans use information technology to carry out their work [2]. Through undesirable behavior, employees can cause information security loopholes, which could be exploited by external perpetrators to take harmful actions against the organization (e.g. copy customer data). However, loss events may not only be caused by external individuals (e.g. hackers, social engineers), but may also originate from inside the organization (e.g. fraud, unintentional security violations) [3].

Organizations try to stem undesirable behavior of employees through technical and behavioral measures. Technical solutions, like data leak prevention software, provides a certain level of security, but sooner or later employees find ways to bypass such barriers [4]. Therefore organizations often implement information security awareness (ISA) programs to make the employees aware of existing risks. Usually organizations communicate the information security policy, in which compliant employee behavior is stated, through ISA delivery methods to their employees. Previous research discovered that organizations mainly use conventional delivery methods, like posters, leaflets and intranet articles, with low media richness to build ISAs [5]. Instead the authors recommend to use an innovative delivery method, which uses viral effects to effectively build information security awareness [6]. We assume that management should enforce horizontal communication about information security, instead of simply sending formal rules to single employees in form of intranet articles. The proposed research aims to provide design guidelines for viral videos as an innovative delivery method to enhance the employees' information security awareness.

The underlying research is structured in four parts: At first, a literature review about success factors of viral videos has been carried out to identify design rules for the success of viral videos. Preliminary results of the literature review can be found in Chapter 2 of this article. After the design phase, we plan to create a viral video about mobile device security, which is then tested at our research partner. We assume that some ISA delivery will be more effective to change employees' behavior toward more accurate adherence to the organizations information security policy. Therefore, the final goal of the research is to evaluate the changes in attitudes, subjective norms and the intention to behave according to the security policy induced by the viral video. Hence, a pre- and post- survey shall be conducted to measure the impact of the viral video.

II. Theoretical Background

Security officers of large organizations are concerned about the behavior of employees, because it seems that employees do not care about stated security standards [5]. Previous research discovered common examples for undesirable employee security behavior, like employees who do not lock their computer, use insecure passwords or make notes of passwords at visible places [7]. Further, undesirable employee behavior includes the case of careless use of mobile devices outside the company (USB sticks, laptops, mobile phones, tablets), which often leads to the threat of confidential information being leaked to outsiders [8].

In recent years, viral videos have already been used successfully in the context of electronic business and marketing [9]. But all in all, the attributes of success or failure of a video becoming viral are rather unknown [10]. A video is a powerful method to create a strong mental impression and helps the audience to easily remember the key messages [11]. A video clip can spread very fast and arise the intended

S. Bauer is with the Vienna University of Economics and Business, A-1020 Austria (phone: +43-1-31336-5202; e-mail: Stefan.bauer@wu.ac.at).
J. Frysak is with the Vienna University of Economics and Business, A-1020 Austria (e-mail: josef.frysak@wu.ac.at).

awareness, but might also totally miss the intended goals [10].

The primary ambition of a successful viral campaign is to create horizontal and vertical communication between employees, which enforces them to recommend their colleagues to behave desirably, as illustrated in the video [12]. Co-worker behavior and recommendations are important factors for information security behavior in organizations, which is why we assume that an ISA program with viral videos would be reasonable to improve the social norms of companies [13].

Previous research identified several success factors for viral campaigns [10]-[12]. An important ingredient of a viral video is an element of surprise, which could be identified in every successful viral video analyzed by [12]. Moreover, successful viral campaigns take advantage of emotions to trigger involvement of employees [12]-[14]. The majority of people frequently forward e-mails to friends, family and colleagues, and share emotions indirectly [14].

Further, it is important that the viral message captures the imagination of the employee, which implicates that the content of the video has to be of relevance to the employee. Moreover, viral videos need to be targeted on a problematic practical area. Hence, the planned viral video for this research will deal with mobile device security, as mobile devices are actually risk factors for organizations, because they are frequently connected to the organizations information system and thus deserve closer attention [15].

There are several possibilities how viral campaigns can be classified [12]. There are six specific types of viral campaigns. Based on experience we assume that a joy-based campaign with surprising elements is proper for the ISA context. For designing the video, it is essential to show undesirable employee behavior, resulting in loss events and risks concerning mobile devices at it's the beginning and presenting the appropriate best practice behavior in a humorous manner afterwards. We further intend to integrate the employees of our research partners into the viral videos to enhance their involvement and to make the actors ambassadors of the videos. The final goal for practitioners is to motivate the employees to avoid behaviors demonstrated in the first part and behave as illustrated in the second part of the video. The methodology 4behindour planned research paper is to develop and verify our design guidelines through design science. This ensures that our design guidelines provide a scientific proven approach for viral videos to increase awareness of the employees concerning information security.

TABLE I
DESIGN GUIDELINES

Preliminary Design Guidelines	Intended effect
1. Implement an element of surprise.	Attention of the employee
2. Implement content, which enables emotions to trigger involvement of the employees.	Involvement of the employee
3. Implement content, which is relevant for the employees.	Involvement of the employee
4. Attention should target on a problematic practical area.	Relevance /attention /involvement of the employees
5. Use employees as actors and make them to ambassadors of the videos.	Involvement of the employees

The behavior of an individual concerning information security can be analyzed through the theory of planned behavior (TPB) [13]. The TPB is a scientific proven theoretical framework to predict and explain human behavior in a security context [16]. In the actual research model the TPB is extended by the factors security awareness and perceived security program. All added factors originate from previous research [17]. The research model is used as a theoretical framework to evaluate the effects of the viral video, because the empirical research is structured as an intervention study, with a pre- and post-online survey.

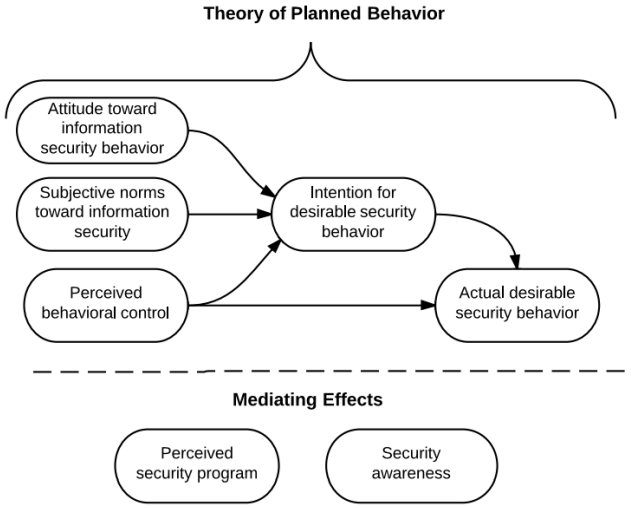

Fig. 1 Research Model

The description of the final goal raises several research questions worth being examined in detail by the proposed research. Based on the literature review and first research stages, we formulated three preliminary research questions for further research stages:

1) Are the proposed design guidelines for viral videos suitable for the development of a viral artifact in the information security context?
2) Do viral videos constitute a proper ISA delivery method to change subjective norms and attitudes of employees?
3) Are viral videos better suited to improve employees' security behavior compared to conventional ISA delivery methods?

A viral video enhances horizontal communication about

information security. Hence, we assume that an information security awareness delivery method like viral videos improve social norms and attitudes toward information security of the employees. Further, we assume that security awareness and the perception of security awareness program will benefit from the viral video campaign.

III. Research Methodology

The underlying project plan is the first step of our ambitious research project. Fig. 2 illustrates the research methodology. The idea for this research project was developed during an expert interview with an operational risk trainer at our research partner. After the idea was born, the existing scientific literature was screened for information security awareness delivery methods and design requirements for viral videos, and the online video platforms were searched for innovative viral videos in the research context. A list with best practice examples can be found in the appendix of this research application. The literature review was carried out according to the methodology of Webster and Watson[18]. The scientific papers were selected through a keyword based research in the most important academic databases. The resulting articles were screened manually for relevance regarding the research context.

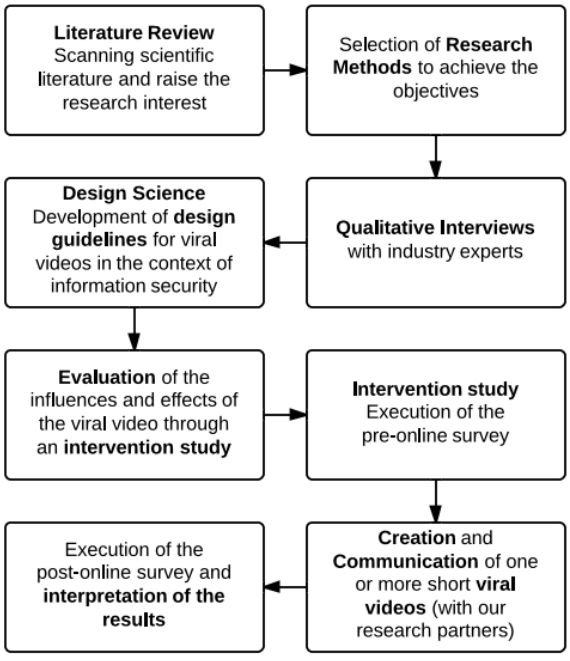

Fig. 2 Research Methodology

After summarizing the literature, the selection of most suitable research methods followed. We decided to use design science, with a quantitative intervention study in the evaluation phase, to carry out the research. Before the design science stage began, two expert interviews with professionals were conducted to gain knowledge on the topic. Both interviewees have been professionals from the banking industry, which already planned to create information security awareness videos. The interviews were very helpful to get an idea how the video can be produced and to identify influence factors in practice. After the interviews, we searched for a young professional movie producer, interested in the underlying project. A one-man motion picture production company was found through university contacts. Our research partner, the movie producer and the applicant already have had several meetings to discuss the content of the video and the progress of the project.

In the next phase, we used design science to provide recommendations on how to design an effective ISA viral video strategy. Design science research is defined as "a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence"[19]. The goal of any DSR project is the creation of an artifact [19]. An artifact is defined as something artificial that is constructed by humans and appears either in the form of a construct, model, method or instantiation. In this case, the viral video is the artifact and together with our research partners, we plan to design multiple iterations of prototypes before the final viral video is sufficiently sophisticated to be distributed among the employees. In order to design practically relevant artifacts, DSR is strongly focusing on evaluation of artifacts[20]. Therefore, the overall research goal is to measure the impact of viral videos on the employees' information security behavior compared to other awareness delivery methods.

The upcoming phases contain the creation and communication of the viral video and the evaluation phase. Basing on a quantitative approach, the evaluation phase consists of a pre- and post-online survey to measure the constructs of the TPB (attitude, social norms, perceived behavioral control, intended behavior and actual behavior), security awareness and the perceived security awareness program. The chosen latent variables originate from previous research [17]. An online questionnaire will be carried out before and after the intervention (viral video). The questionnaire has already been developed. Fig. 3 represents the evaluation phase, which is conducted with one group, for which the intervention is provided and another group without intervention. The design of research of the intervention study is planned according to the study of Albrechtson and Hovden [21], in which a security awareness comic was applied as intervention.

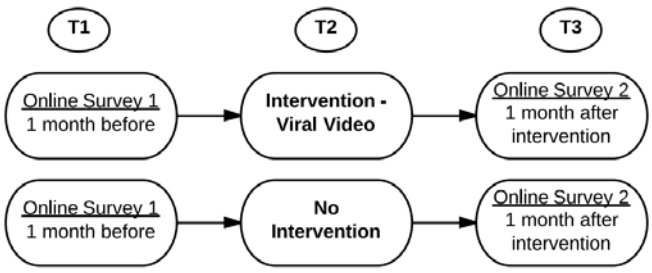

Fig. 3 Evaluation phase: Intervention study design

Our research partner supports the study by publishing an article in the employee newspaper and by distributing links of the online survey via their internal email system. Currently they have access to 1200 employees; nevertheless, the non-response bias is estimated to be quite high. To achieve a return rate of at least 20%, the employees get an incentive for answering the questionnaire. We planned to raffle off four tickets for a gourmet theatre in Vienna for each survey (pre- and post-survey). With this incentive we suggest the amount of probable subjects to be sufficient, as the PLS based structural equation modelling approach requires at least 100 cases to return significant results [22].

IV. Conclusion

ISA programs are intended to make employees aware of potential information security risks. Compared to conventional methods, viral videos are an innovative method to deliver information security awareness in an effective and efficient way. Viral videos could not be limited to an organizational context; also common computer users could be educated through short spots by national agencies. One limitation of the proposed research is the observation of (positive) long term effects produced by the viral video. As the study is restricted to single, disjoint questionnaires, only the short term effects can be analyzed.

References

[1] ORX, "Operational Risk Loss Report 2012," Operational Risk eXchange Association2013.
[2] S. Jahner and H. Krcmar, "Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk Management," in *Americas Conference on Information Systems (11th AMCIS)*, Omaha, NE, 2005.
[3] M. Warkentin and R. Willison, "Behavioral and policy issues in information systems security: the insider threat," *European Journal of Information Systems*, vol. 18, pp. 101-105, 2009.
[4] A. J.-T. Chang and Q.-J. Yeh, "On security preparations against possible IS threats across industries," *Information Management & Computer Security*, vol. 14, pp. 343-360, 2006.
[5] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study," in *AIS SIGSEC Workshop on Information Security & Privacy (WISP2013)*, Milano, 2013.
[6] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Computers & Education*, vol. 52, pp. 92-100, 2009.
[7] M. Siponen and A. Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly*, vol. 34, pp. 487-502, 2010.
[8] M. Warkentin, D. Straub, and K. Malimage, "Featured Talk: Measuring Secure Behavior: A Research Commentary," presented at the Annual Symposium of Information Assurance & Secure Knowledge Management, Albany, NY, 2012.
[9] R. Ferguson, "Word of mouth and viral marketing: taking the temperature of the hottest trends in marketing," *Journal of Consumer Marketing*, vol. 25, pp. 179-182, 2008.
[10] K. Nelson-Field, E. Riebe, and K. Newstead, "The emotions that drive viral video," *Australasian Marketing Journal (AMJ)*, vol. 21, pp. 205-211, 2013.
[11] R. D. Waters and P. M. Jones, "Using Video to Build an Organization's Identity and Brand: A Content Analysis of Nonprofit Organizations' YouTube Videos," *Journal of Nonprofit & Public Sector Marketing*, vol. 23, pp. 248-268, 2011.
[12] A. Dobele, A. Lindgreen, M. Beverland, J. Vanhamme, and R. van Wijk, "Why pass on viral messages? Because they connect emotionally," *Business Horizons*, vol. 50, pp. 291-304, 2007.
[13] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, vol. 31, pp. 83-95, 2012.
[14] R. E. Guadagno, D. M. Rempala, S. Murphy, and B. M. Okdie, "What makes a video go viral? An analysis of emotional contagion and Internet memes," *Computers in Human Behavior*, vol. 29, pp. 2312-2319, 2013.
[15] S.-P. Oriyano and R. Shimonski, "Mobile Attacks," *Client-Side Attacks and Defense*, pp. 223-241, 2012.
[16] T. Sommestad and J. Hallberg, "A review of the theory of planned behaviour in the context of information security policy compliance," in *International Information Security and Privacy Conference*, 2013.
[17] S. Bauer and E. W. N. Bernroider, "An Analysis of the Combined Influences of Neutralization and Planned Behavior on Desirable Information Security Behavior," presented at the 13th Annual Security Conference, Las Vegas, 2014.
[18] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, vol. 26, pp. xiii-xxiii, 2002.
[19] A. Hevner and S. Chatterjee, *Design Research in Information Systems*: Springer, 2010.
[20] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, pp. 45-78, 2007.
[21] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Computers & Security*, vol. 29, pp. 432-445, 2010.
[22] M. Sarstedt, C. M. Ringle, and J. F. Hair, "PLS-SEM: Indeed a Silver Bullet," *The Journal of Marketing Theory and Practice*, vol. 19, pp. 139-152, 2011.