Two Case Studies in Using Chatbots for Security Training

Stewart Kowalski[1], Katarina Pavlovska[1] , Mikael Goldstein[3]

[1] SecLab Department of Computer and Systems Sciences Stockholm University/Royal Institute of Technology Stockholm, Sweden

[2] migoli, Valhallavägen 130, 114 41 Stockholm, Sweden

stewart@fc.dsv.su.se

Abstract. This paper discusses the result of two case studies performed in a large international company to test the use of chatbots for internal security training. The first study targeted 26 end users in the company while the second study examined 80 security specialists. From a quantitative analytical perspective there does not appears to be any significant findings when chatbots are used for security training. However there does appear to be qualitative data that suggest that the attitudes of the respondents appear to be more positive to security when chatbots are used than with the current traditional e-learning security training courses at the company.

Keywords:, Security Awareness Training, Chatbots,

1. Introduction

At the first WISE conference in 1999 Kowalski et al [1] presented in the paper *The Manual is the Message* observations that employees in a company that received security policy and instruction via a paper based medium differed in attitude to security to those that received the same security policy and instruction via an internal webpage. Those that received the information via a paper medium appeared to have a better security attitude than those that received the same information via a web based medium.

In this paper were discuss two new case studies [2, 3] were the medium of communication is the independent variable and the knowledge, attitude and behavior the dependent variable. The paper is divided into five sections. After this short introduction we discuss the current state of security awareness training in corporations. In section two we review the technology of chatbots and how this technology was applied in the case studies. The design and result of these two case studies are presented in section four. We conclude with a general discussion on the potential of chatbots in security education.

2. Quick Overview of Security Awareness Training

The European Network and Information Security Agency ENISA report on current practices in security awareness initiatives in Europe points out that today most European companies have information security policies and instructions set on intranet sites. Most companies also have on-line instruction and 2/3 have some form of mandatory on-line training. [4]

There are those like Nielsen [5] that suggests that awareness and training for security are not an effective way to deal with the web based security problem and only good user design and solid security architecture is the answer. Srikwand and Jakobsson [6] point out often that in an effort to make security messages understandable to the common end user the message is simplified to such an extent that it loses its meaning. Jagatic et al [7] and Kumaragure et al [8] however have performed studies that showed in some case studies that when used in a correct context security awareness training can be effective.

To the authors knowledge no other case studies have been performed to see how chatbot technology can be used to enhance security awareness training.

3. Chatbot Technology

Weizenbaum created the first chatbot in the MIT Artificial Intelligence Lab and called it ELIZA. ELIZA imitated the "active listening" strategies of a touchy-feely 1960s Rogerian therapist [9]. A chatbot or chatterbot can be defined as a computer based program that imitates human (text-to-voice/text) conversation. There is a wide variety of chatbots in use today. They may be used for entertainment, marketing, education and a lists of various chatbots can be found at chatbot.org [10]. These bots can range anywhere from talking to William Shakespeare to speaking with ANNA at IKEA Inc. While some are designed so they are able to compete in a number of different chatbot competitions like the Loebner Prize [11] others are used as a tool for entertainment or for information retrieval. For example, chatbot Sofia [12] can assist in teaching mathematics, VPbot [13] imitates a patient that medical students can interview.

Some chatbots are used in e-business and as a way to communicate to customers. Rita (Real time Internet Technical Assistant) [14] is used in the ABN AMRO Bank to assist customers in doing financial tasks, such as a wire money transfer. In a company called GetAbby, Abby[15] is used to administer customer relationships. The chatbot uses voice recognition techniques during real time phone calls to track and save information from phone calls including customer name, address, and conversations. This allows the company to track customer calls in a cheaper and more efficient way. A chatbot named Anna [16] is used to interact with customers on Ikea's website. It guides and facilitates users in navigation of Ikea's site by allowing them to enter specific questions and then directing them to the appropriate place..

Chatbot Sofia [12] was part of an experiment conducted at the Harvard mathematics department in 2003. The experiment investigated the process of

teaching and learning mathematics with the help of a chatbot. Chatbot Sofia has an encyclopedic glossary of mathematics definitions and a general knowledge background, and is able to solve simple mathematical problems. The tool saves all the conversations which can later be analyzed in order to get more information on how students are learning, what questions they ask, and what mistakes they frequently make. It was concluded that Sofia contributes to a variety of teaching methods and builds an open source knowledge database for different parts of mathematics. In addition, by teaching Sofia and watching how it learns, students may gain a better understanding regarding the process of teaching mathematics. .

Computer Simulator in Educational Communication (CSIEC) [17] is a web-based human-computer communication system that uses natural language. This chatbot may be used as a chatting partner for learning the English language. It imitates human emotions and personalities. Moreover, conversations are not limited to any specific subject. The ideal user's input should be acoustic and then converted into text but so far only keyboard inputs are used since the speech recognition program still needs improvement-

It is important to note that when constructing such various chatbots, the goal of what the chatbot should do and the audience to whom the chatbot is for, should be considered and analyzed thoroughly. Tailoring the chatbot for the users and also addressing the appropriate questions/responses of a typical user will produce a more human-like effect. Allowing the chatbot to achieve such an effect may help to improve its overall intention as well as the user's experience of using the chatbot. .

4 Design and Result of the Two Case Studies

4.1 End User Case Study

In the first case study [2] selective sampling technique was used to divide the two groups. The selections criteria for the grouping were based on the geographical and operational organization of the company. All the five global sales regions were represented along with two of the three business units in the company were portionaly represented in the two groups. One group was exposed to chatbot (Sally) and e-learning and the other group to e-learning only. Both telephone interviews and email surveys were used to solicit responses from the two groups. The survey consisted of 35 questions which tested various aspects of knowledge, attitude and behavior to security issues. Space does not permit to include the full survey[1] in this paper.

Knowledge questions were concerned with the different information security classes at the company along with examples of typical document types and how they should be classified. Attitude questions covered such aspects as how important information security was over business goals an attitude questions concerning individual responsibilities for classification. Behavior questions ranged from asking how often they changed passwords to how to collect different access rights in the company.

Following the first survey all the respondents of the two groups were sent web links to a training package on Information Security (IS). One group was given an e-

[1] A full copy of the survey and a link to the chatbot can be requested by sending email to the author, stewart@dsv.su.se

learning package only while the other group was given an e-learning package with a voice and text chatbot (Sally). Figure 1 below shows the e-learning package with a chatbot. After about two months a second, identical survey was solicited to the respondents of the two groups.

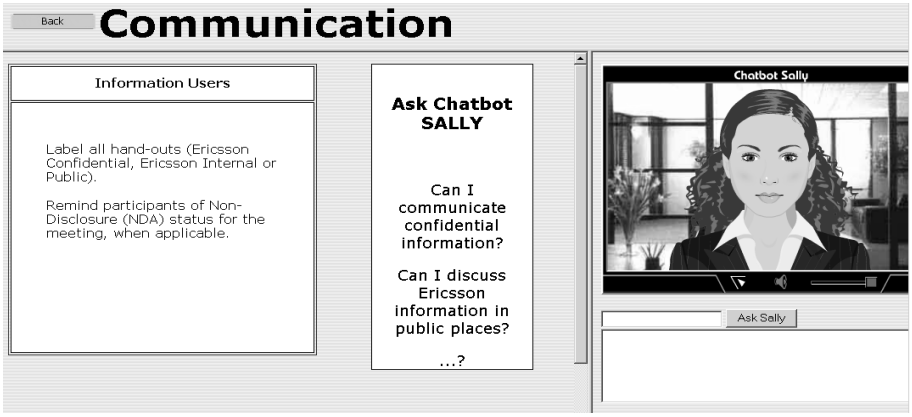

Fig. 1. E-learning package with security information on the left and with chatbot Sally on the right.

A Wilcoxon matched pair-single-ranks test was used to assess significance of the quantitative difference in Information Security related knowledge, attitude and behavior between the first and second intervention of the questions for the chatbot and non-chatbot group. There were no significant differences in respondents' responses between the first and second intervention in any of the two sample groups ($p \leq 0.05$, two- tailed test).

The experience of using the chatbot was measured qualitatively by asking the respondents how useful they thought the learning experience had been. As much as 70% of those that used the chatbot found it useful. Over 70% of the respondents agreed that the chatbot had a positive effect on their learning experience and that they would use the chatbot in the future.

To a large extent, the results of this chatbot case study are inconclusive. Quantitatively there does not appear to be any significant difference in knowledge, behavior and attitude improvement using a chatbot. However, the qualitative analysis does indicate positive attitudes by the chatbot users. The restrictive sample size of 16 users of the chatbot can be a contributing factor and the authors suggest that either a large scale analysis be done or a more clinic type of experimental design be used to validate the effects on chatbots on security awareness.

4.2 Security Specialist Case Study

The population consisted of 80 employees that took part in the Information Security Management System (ISMS) Lead Auditor training throughout 2007 [3]. The population was randomly divided into two groups; an experiment group (ISO Alan chatbot), containing 42 employees, and a control group, containing 38 employees.

The experiment group received an e-mail containing a web link to the e-learning package with the ISO Alan chatbot, see Figure 2 below.

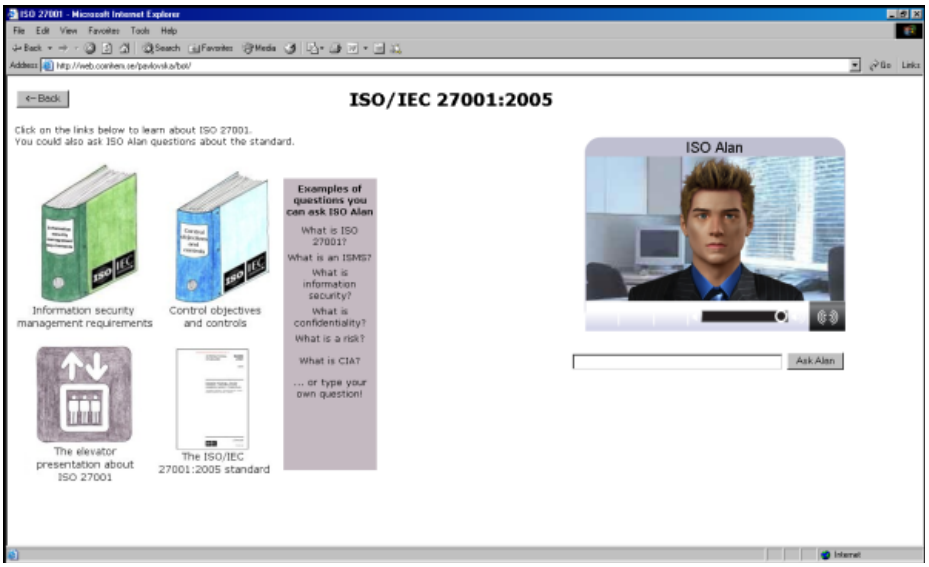

Fig. 2. ISO/IEC 27001:2005 ISO Alan Chatbot with e-learning package.

The employees in the experiment group were asked to spend some time with the e-learning package during the following two weeks. The e-mail also contained the information that when these two weeks had passed they would be asked to participate in a web survey about their feelings regarding their current knowledge of ISO 27001 and ISMS auditing. The control group only received an e-mail with the information about the web survey. Figure 3 shows all the steps of the experiment.

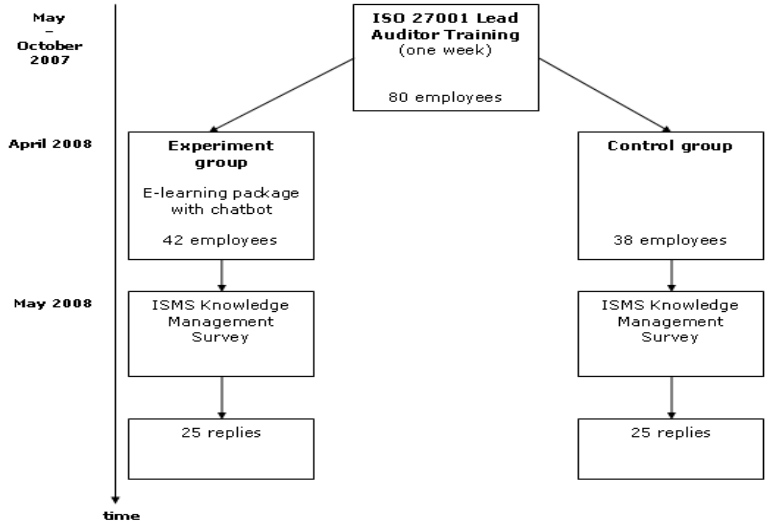

Fig. 3. ISO/IEC 27001:2005 ISO Alan Chatbot Case Design.

The results from the quantitative analysis show that there was no significant difference between the experiment group and the control group regarding knowledge and attitude. When asked however how useful they thought the learning experience had been, as many as 70% of those that used the Alan chatbot found it useful. Over 70% of respondents agreed that the chatbot had a positive effect on their learning experience and that they would use the chatbot in the future. A selection of comments is presented below;

> *ISO Alan chat is good, but his knowledge is a bit limited at present time, so when ISO Alan gets more knowledge it will be more useful. The left hand information packages were very good.*
>
> *Chatbot works quite well once you get used to the idea of simply using key words to get more information - sentences are not needed*
>
> *As far as I can conclude, the chatbot does not answer questions other than what is. If it is to provide an added value, it must be able to answer questions that would come from the target audience, such as how do I, who should be, etc.*

5. Discussion on Way Forward with Security Chatbots

The two cases studies do not provided clear data to validate or falsify the usefulness of using chatbots for security education and training. They do however give some qualitative indication that for particular group of users, chatbots can serve as a complement to computer based training and online awareness training. As Näckros [18] discovered in his work on game based instruction for IT security,

different learning styles of individuals prefer different methods of learning. As he points out the majority of computer based learning use sequential learning styles which are designed primarily on serialist learning style. However for those individuals who prefer a holistic approach a serial learning style is often ineffective. A chatbot permits a less serial learning style by design and allows respondents to move in a non-linear fashion in their discovery of knowledge. It is suggested by the authors that if further studies are done with chatbots employed in security training, the respondents should be first screened for their learning style to see if this can be used to predict their appreciation of a chatbot for learning about security issues.

One of the positive side effects of using a chatbot for security awareness training in the organization in the two case studies was a database of questions and issues that both the end user and the specialist ask about security. This database can be used as a knowledge base for future development in the organization. Methods used for developing, capturing, maintaining and sharing knowledge are usually called knowledge management. Ahmed et. al. [19] defines knowledge management as the combination of processes, technologies, strategies and culture an organization, used together to favor the learning in the organization. The potential of chatbots for security knowledge management in an organization is an area that author see as a potential of future research.

6. References

1. Kowalski, S., Nässla, H., Karlsson, J., Karlsson, V.: The Manual is the Message: An Experiment with Paper Based and Web Based IT Security Manuals. Proceedings of WISE1, Stockholm, 1999)
2. Kowalski, S., Mozuraite-Araby, R., Walentowicz, S.: Using Chatbots for Security Training of ICT Users , World Wide Research Forum 20th Conference Ottawa, Canada (April 2007).
3. Pavlovska[1], K.: Using Using chatbots to maintain knowledge about ISO/IEC 27001:2005 at Ericsson. Master's thesis, Department of Computer and Systems Sciences (2008)
4. European Network and Information Security Agency, Information Security Awareness Initiatives: Current Practice and the Measurement of Success (July 2007)
5 Nielsen, J.: User education is not the answer to security problems [online]. Accessed [Accessed: 2009]. Available at WWW: http://www.useit.com/alertbox/20041025.html
6 Srikwan, S., Jakobsson, M. 2007. Using cartoons to teach Internet Security [Accessed 2008]. Available at WWW: http://www.informatics.indiana.edu/markus/documents/security-education.pdf
7 Jagatic, TN., Johnson, M., Jakobsson, M., Menczer, F.: Social Phishing. Communications of the ACM. Vol. 50, Issue 10, pp. 96 – 100 (2007)
8 Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., Nunge, E.: Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. Conference on Human Factors in Computing Systems archive. Proceedings of the SIGCHI conference on Human factors in computing systems. San Jose, California, USA, pp. 905 – 914 (2007)
9 Weizenbaum, Jospeghy "ELIZA - A Computer Program For the Study of Natural Language Communication Between Man And Machine",Communication of the ACM 9 (1): 36-45 (1966)
10 Chatbot.org [Accessed on 24th April 2009] at URL http://www.chatbots.org/

11 Loebner Prize: http://www.loebner.net/Prizef/loebner-prize.html
12 Knill, O., Carlsson, J., Chi, A., and Lezama, M. (2004). An artificial intelligence experiment in college math education. [Accessed on 24th April 2009] ://www.math.harvard.edu/_knill.
13 Webber, G. M. (2005). Data representation and algorithms for biomedical informatics applications. PhD thesis, Harvard University.
14 Voth, D. (2005). Practical agents help out. IEEE Intelligent Systems, 20(2):4–6.
15 GetAbby http://www.getabby.com/lead_tracking.asp
16 ANNA [Accessed on 24th April 2009] at URL http://www.chatbots.org/chatterbot/anna_sweden
17 Jiyou, Jia.: CSIEC (Computer Simulator in Educational Communication): An Intelligent Web-Based Teaching System for Foreign Language Learning Advanced Learning Technologies. Proceedings of the IEEE International Conference, Issue 30, pp. 690 – 692 (2004)
18 Näckros, K.: Game Based Instruction within IT Security Education. Department of Computer and Systems Sciences, Stockholm University Royal Institute of Technology, Stockholm (2001)
19 Ahmed, Pervaiz, K., Kok, Lim, Kwang, Loh, Ann, Y. E.: Learning, Through Knowledge Management, Butterworth-Heinemann (2002)