INFORMATION SECURITY SURVIVAL KIT: LIFE-LONG END-USER PREVENTION TRAINING FOR SMALL TO MEDIUM-SIZED BUSINESSES

L. Roger Yin, University of Wisconsin-Whitewater, USA, yinl@uww.edu
Blake Penn, University of Wisconsin-Whitewater, USA, pennb@uww.edu
Daniel T. Norris, University of South Carolina, USA, dnorris@sc.edu

ABSTRACT

Small and medium-sized businesses are the organizations most frequently hit with viruses, hacking, malware, and unwanted e-mail. They are also the nation's front-line defense when it comes to these information security issues. Unfortunately, these same organizations are the ones least likely to be able to afford the time, expense, and expertise necessary to combat these growing threats. It is the contention of the researchers that an Information Security Survival Kit can be constructed which will address these issues - primarily through the vehicle of end-user education. This Kit will enable small and medium-sized business to protect themselves from these threats in an efficient and affordable manner.

Keywords: information security, life-long learning, end-user education, cyber trust

INTRODUCTION

Ever since the terrorist attacks in September 11, 2001, there has been a growing concern among corporations and government agencies to come up with new approaches to measure an organization's information security risks and posture. The Department of Homeland Security (DHS) was established to coordinate the anti-terrorism efforts, including the prevention of cyber-attacks, as a national priority. For fiscal year 2004, DHS acquires $37 billion dollars as its operational budget, and such number might continue to increase. In guiding such efforts, a national task force on information security and assurance explains and defines the theories and processes that will help an organization protect its proprietary information including

- The need to assess the current level of risk.
- The need to determine what can impact the risk.
- The need to determine how risk can be reduced or mitigated.

Those needs have turned into an increasing demand globally in both private and public sectors for IT and IS professionals with information security and assurance knowledge and expertise.

While the U.S. national infrastructure of information security and assurance has been pushed to the forefront, the plan seems to overlook the necessary preparation of the vulnerable "weakest link," the end-users, or "information consumers." With ever-present risks of viscous attacks on the borderless Internet, end-users in small and medium-size businesses are brutally exposed to increasing number of spam, phishing, spyware, malware, viruses, and fraud that have severely impacted these end users in the areas of privacy, productivity, efficiency, and the sense of trust that would have made e-commerce a viable way to conduct business for these end-users sooner.

Though there have been anecdotal instructions and low-cost or even free software to "cure" the affected computers, these cures are random and discreet at best. Currently, the only viable options existing for small and medium-sized businesses to mitigate the risk of information security risk are professional consulting advice and commercial information security products. Information security professionals are cost prohibitive for small to medium-sized businesses to employee as FTEs due to their extensive and specialized training and skills. Only medium-large and large organizations both have the funding and division of labor necessary to support these specialists (with the exception of small and medium-sized consulting and service firms). Information security consulting services are expensive and are usually cost prohibitive to the small and medium business market, as well. Finally, only the most rudimentary security controls, such as anti-virus software are economically viable for small and medium-sized businesses. More expensive and robust information security controls, such as network firewalls, intrusion detection and prevention systems, and policy enforcement and endpoint security management systems are simply out of their financial reach. In addition, even capable and technology-savvy employees at these firms lack the time and effort to perform the necessary research to keep current with information security threats and countermeasures.

In fact, Internet fraud complaints have risen dramatically from 1,152 in 1997 to 37,183 in 2003 [5]. This form of high-tech coercion is performed by "social engineers, a new generation of hackers"[12, p. 57]. Unlike Charles Dickens' time, these nefarious denizens are after the new up-market commodity which is information. Protecting information costs U.S. corporations millions annually [7, 10] and those costs are expected to skyrocket over the next decade [6]. Corporate computing systems are only one target. Consumer watchdog organizations have identified many other situations where engineered social deception has resulted in significant personal losses such as online auction fraud, e-mail scams, and identity theft [8]. Whether the target is large corporate databanks or personal bank accounts, information security is only as good as the weakest link, which typically, is the end-user [3, 11].

In a sea of information out on the Internet, it is overwhelming for ordinary, unsophisticated end-users of computers to sort out what is "necessary" and "adequate" that they need to know what might threaten their privacy and business integrity. Therefore, it is proposed that a thoughtfully designed "Information Security Survival Kit" is to be developed based on extensive research in information security (including the human deception elements), technological solutions, and multimedia-based e-learning for general end-users in small to medium-sized businesses.

RESEARCH DESIGN AND PROCEDURE

This applied action research project will be based on both quantitative data gathered from pretest/posttests of end user knowledge on information security, and qualitative data collected from questionnaires, interviews, and "blogs" or critical reflections and feedback of the participants. This will be the second phase of the project. Tentatively, the participants will be 30-40 end users in small to medium-sized businesses in Wisconsin.

Before the research procedure and cycle could begin, however, the instrument, an "Information Security Survival Kit" will be developed and distributed, which will be the Phase 1 of the project. The project evaluation and future improvement will then be the third phase.

Phase 1: Developing the Instrument (Constructing the Survival Kit)

In the first stage of the project period, an Information Security Survival Kit will be created based on minimalist training design approach [2, 1]. No new software will be created from scratch. Rather, the Kit will focus on helping end users deal with information security problems surrounding them by providing practical instructions on using what software under what circumstances in "plain language." This Survival Kit will include the following:

- A pretest in the form of a questionnaire that the participant needs to fill out first and send back to the researchers. The examples of the prior knowledge being tested are
    - What is "spyware?" How would you know your computer is affected by it?
    - On a Web browser (e.g., Internet Explorer) screen, how do you identify the data transaction on that session is secured and encrypted?
- An instructional "jumpstart" book or booklet outlines the four major information security treats mentioned above and preventive actions against each one. Examples are
    - What anti-virus software best suit your need? Where do you find and get it?
    - What are the Top 10 human errors in electronic information security?
- A series of interactive training DVD titles with scenarios and case studies to depict and explain different ways to avoid vicious attacks as well as setting up a defense system with cost-effective computing hardware and software solutions. Here is an example:
    - Episode B: Playing detective against spoof mail – located the geographical origin of the spoofer and Web hosting services provider used.
    - Episode D: Terrorists and identify theft – what happen to those stolen credit card and bank account information?
- An accompanying Website providing most current and updated information regarding end-user information security prevention, including updates on cyber laws and regulations. This Website could also provide moderated threaded discussion forums for participants to share their personal experiences and support each other along with the academic and industry experts who are willing to contribute. As Wenger [9] may point out, this is to build a virtual community of practice and construct a new body of knowledge where each member of the community could share with and learn from each other through telling life stories.

The Information Security Survival Kit will serve to (a) educate end users to information security concepts and best practices and (b) provide tools and references to assist in following best information security practices. The educational components will include text, hypertext, and audio-visual material. The aim of this material will be to make end users at small and medium-sized businesses better net citizens by training them in the proper and secure way to operate their computing resources in the course of their day-to-day business.

This educational material will include, but will not be limited to topics such as operating system and patch management, systems updates, anti-virus products and methods, phishing and e-mail abuse, user and file-system management and best practices, firewalls and perimeter security, cyber security laws and regulations, system auditing and accountability, employee information security awareness, business continuity planning and disaster recovery, and information security policy formulation and enforcement.

The tools and resources in the Kit will include, but will not be limited to, shareware and freeware computer security software, information security reference material, and hyperlinks to both the project web site and other useful information security resources. These tools and resources will aid in enabling the user to follow the best practices covered in the education portion of the kit.

Phase 2: Utilization of the Instrument and Data Collection

Using the customer databases maintained by Global Business Resource Center and Small Business Development Center at University of Wisconsin-Whitewater, the project coordinators will identify 30-40 small to medium-sized business owners in southern Wisconsin who are interested in this project and distribute the Information Security Survival Kit to them. The participants will agree that in order to receive optimal benefit including technical support and customized advice on information security for their businesses, they will contribute to the Web-based virtual discussions at least once a week and provide feedback on the usability of the Information Security Survival Kit during the first month of using the Kt. They will also fill out an online questionnaire as a posttest designed to assess their learning gain in the end of Phase 2. Telephone interviews and on-site visits with the participants may also be conducted to provide the researchers rich and thick description on their learning experiences.

After the first month of Phase 2 is completed, the data collected from Web discussion forum, interviews, and questionnaires will be sorted and analyzed.

Phase 3: Evaluation and Study Results

Once data are collected and analyzed, the project coordinators will interpret the results and write up the findings. Evaluation method on the successfulness of the project design and the Information Security Survival Kit will be elaborated in the 4th section of this proposal below.

LINK TO ECONOMIC IMPACT

According to the British research firm, mi2g, financial losses in the year 2004 for malware alone have been estimated to be as high as $166 billion dollars [4, WWW]. These figures do not reflect other, non-malware related, financial losses due to lax information security (such as hacker attacks – including social engineering), which brings the total cost even higher. Most successful malware attacks (about 60 per cent) successfully target small businesses. In comparison, only about 2.5 per cent of malware attacks disrupt large enterprises, government agencies, etc.

These statistics demonstrate the vivid business need for small businesses to protect themselves against the growing threat of malware and hacker attacks. The very same statistics also show us that without mitigating these threats, enormous financial harm can be done – especially to small businesses that are ill-equipped to deal with the financial fallout of cyber attacks and malware. Most small businesses do not have the in-house expertise or the resources to engage outside consulting experts to deal with growing cyber threats. Lack of education is also a significant issue, with most small business owners and employees being unaware of the numerous and varied threats they face when using their computers and networks.

The average amount of information security consulting time to adequately begin to educate and fix many common information security problems can be conservatively estimated at 80 man-hours. At a reasonable market rate of $200 per hour, this expense adds up to $16,000 per small business. This amount might be very reasonable for a medium-to-large sized business, but will likely be cost prohibitive to small businesses. We propose the Information Security Survival Kit as an alternative to small businesses to cost-prohibitive consulting services. For example, if the kit were deployed to 20 small businesses, it will add up to an immediate aggregate direct savings of $320,000. In addition to the direct savings (from not having to hire outside consulting), much more money will also be saved by avoiding costly malware and hacker attacks (including social engineering attacks) at these small businesses. An added benefit is that by securing these small businesses, they cannot be used as a launching point for attacks on other systems (and one compromised system can potentially attack thousands or millions of additional hosts). Therefore, the aggregate cost savings, both direct and indirect, could very conservatively be estimated to be in the range of millions of dollars in Wisconsin alone.

The Information Security Survival Kit will initially be distributed free of charge, or for a small nominal fee or subscription charge for research purposes. After the research has been undertaken, however, there exists the potential for the Kit and supporting materials to be offered commercially. Several options for commercialization exist, including licensing of the Kit itself, offering a subscription service for businesses to have access to the Kit and the website supporting it, and creation of an educational outreach class or program to supplement and expound upon the material contained in the Kit. The content of the Kit and the results of the research could also be incorporated into a textbook or other commercial publication. If the research goes exceedingly well, the efforts of the projects could also be leveraged to create a service business that would address the information security needs of small to medium-sized businesses in a cost effective manner.

EVALUATION METHOD

The primary purpose of this project is to create an Information Security Survival Kit for computing end-users in small to medium-sized businesses that is useful, usable, scalable, and ultimately gain the most from the advancement of electronic commerce with minimum pain and loss suffered from the pitfalls of information security. The expected outcomes for the project are explained in the following:

Usefulness

For measuring how useful the Survival Kit is, the participants will answer questions – in forms of questionnaires and interviews – on their knowledge and experience on various information security treats, solutions, and their competency or proficiency in resolving and preventing such problems. Specific examples and success stories explaining their “know-how” in problem-solving will be collected. The learning gain and perceived usefulness will be assessed by comparing the data collected in the beginning and the end of the implementation time period.

Usability

To identify how usable or user-friendly the Information Security Survival Kit is for the participants, they will answer questions – in forms of questionnaires and interviews – related to the design elements of the instrument, including but not limited to, user interface, ease of navigation, consistency, accuracy, timeliness, technical explanation, content flow, and programmatic errors, etc. Feedback and comments gathered with the usability testing will be essential for product improvement.

Scalability

To assess how scalable and wide-spread this Survival Kit could reach out to more computing end-users, the participants will answer questions in the end of Phase 2 on how likely they will recommend this Information Security Survival Kit to their family and friends living outside of southern Wisconsin or in different businesses. If the majority of the participants suggests that, based on their own experience, this product could benefit more end-users, there may be a high probability that the user population of this Survival Kit could be scaled up to more needed people.

To sum up, the relationship among outcome, method, and timeline is outlined in Table 1.

Table 1. Outcomes, Methods and Timeline for the Security Survival Kit

Outcome	Method	Timeline
Usefulness • Participants are able to gain practical knowledge in understanding, resolving, and preventing information security threats.	• Pretest	Nov., 2005
	• Posttest	April, 2006
	• Questionnaires • Thinking-aloud protocol (authentic story-telling in discussion forums) • Interviews	Nov., 2005 – April, 2006

Usability
• Participants find this Kit to be user-friendly in helping them learn how to deal with information security threats.
	• Testing
	  o Thinking-aloud protocol
	• Inspection
	  o Features
	  o Heuristics
	• Inquiry
	  o Questionnaires
	  o Interviews
		Nov., 2005 – April, 2006

Scalability • Participants would recommend this Kit to other people in similar nature.	• Exit Questionnaire • Exit Interview	May-June, 2006

CONCLUSION

If the results of this pilot study prove to be fruitful and meaningful, the project researchers intend to expand the end-user group beyond the region and type of businesses, and reach out to students and teachers in schools and universities as well. It is also possible that this Kit is to be translated into Spanish, French, Chinese, Japanese, or any other languages to make it a world-wide endeavor. Future extramural funding support for the project expansion may come from the CyberTrust grant of National Science Foundation and private funding sources. We believe that it is imperative to prepare and educate the citizens not only how to protect themselves from cyber crimes, but also why they should not commit any cyber crimes – and the time to begin the education is now.

REFERENCES

1. Carroll, J.M. & Rosson, M.B. (1987). The paradox of the active user. In J.M. Carroll (ed.), *Interface thoughts: Cognitive aspects of human-computer interaction*. Cambridge: MIT Press/Bradford Books.
2. Carroll, J.M. (1990). *The Nurenberg Funnel: Designing Minimalist Instruction for Practical Computer Skill*. Cambridge, MA: The MIT Press.
3. Erlanger, L. (2004). The weakest link, *PC Magazine*, *23*, pp. 58: ZDNet.
4. Jaques, R. (2005). Cost of malware soars to $166bn in 2004. Retrieved Feb 01, 2005 from http://www.vnunet.com/news/1160924
5. National Fraud Information Center. (2004). Internet scams: January-december 2003:National Consumer League.
6. Nicolett, M., & Kavanagh, K. M. (2004). It security management market and technology evolution. Retrieved 11/16/04, 2004
7. Panettieri, J. C. (2003). Security, *CFO*, *19*, pp. 33: CFO Publishing Corporation.
8. Rusch, J. J. (1999). The "social engineering" of internet fraud, *INET99 The Internet Global Summit*.San Jose, CA: Internet Society.
9. Wenger, E.(1998). *Community of practice: learning, meaning, and identity.* Cambridge, U.K.: Cambridge University Press
10. Winkler, I. S., & Dealy, B. (1995). *Information security technology?Don't rely on it: A case study in social engineering.* Paper presented at the Fifth USENIX UNIX Security Symposium, Salt Lake City, Utah.
11. Yin. L. R. & Prostakova, A. (2003). Top Ten Human Errors in Electronic Information Security. *Business Education Forum*. *58*(1), 51-53.
12. Yin, R. L. (2004). The new hacker: The social engineer. *Business Education Forum*, *59*(1), 57-59.