User-Centered Security Applied to the Development of a Management Information System

M. Nohlberg[1] and J. Bäckström[2]

[1] School of Humanities and Informatics, University of Skövde, Skövde, Sweden
[2] Department of Computer and Information Science, University of Linköping,
Linköping, Sweden
e-mail: marcus@nohlberg.com

Abstract

The purpose of this study has been to do a user-centered security development of a prototype graphical interface for a management information system dealing with information security. The interface was perceived as successful by the test subjects and the sponsoring organization, Siguru. The major conclusion of the study is that managers use knowledge of information security mainly for financial and strategic matters which focus more on risk issues then security issues. To facilitate the need of management the study presents three heuristics for the design of management information security system interfaces:

1. Provide overview information very early in the program.
2. Do not overwhelm the user. Managers are not interested in the details of information security, but if they need details, they should be provided in a logical place.
3. Provide information in a way that is familiar to the manager. Provide contextual help for expressions that must be presented in a technical way.

Keywords

User-Centered Security, Management Information System, Usability.

1. Introduction

While security has been a concern almost since the beginning of the history of computers, it is during the last couple of years that the problem has been communicated to a broader audience than merely systems administrators and technicians. Security has been a major operational issue for a long time, and the costs have continued to rise, as have the number of incidents. In 1998, 32% of British companies suffered some kind of information security incident, and in 2004 that number had risen to 74 % of all companies and 94 % of the major companies (Department of Trade and Industry, 2004).

New laws and regulations such as Sarbanes-Oxley make managers more responsible for security. The widespread media coverage of viruses, DOS-attacks, computer crime etc. also adds to the attention paid to security. Business partners and stakeholders demand good information security if they are going to conduct business with a company (Rasmussen, 2002). This all makes security a business problem.

Many managers are neither technicians nor particularly knowledgeable in information security. Most of their knowledge comes distilled from a specialist who informs them about the current situation, as discussed by the authors in a previous paper (Nohlberg & Bäckström, 2007). Managers only receive second-hand information since they themselves are unable to get any kind of impartial data from the organization using the systems they have today. From the point of view of managers this makes security vastly different from, for instance, economical data that can be found from several sources in a company. The few security solutions that gives some general security information aimed towards users rather than specialists are often regarded as too complicated or too difficult to use, as is understood from the authors' professional experience and as discussed more in general by Furnell et al (2006). Hence, there is a need for an application that provides managers with an overview and understanding of information security that is aimed towards their specific needs and interests. This approach also fits well with the strive to avoid "The 10 deadly sins of information security", as argued by von Solms & von Solms (2004), where security is argued to be a corporate governance responsibility, as well as a business issue.

The purpose of this study was to construct a usable interface for information security-monitoring software with upper-level managers as target users. In order to construct a usable interface, it was important to get to know the users, their situation, their view on information security, and what kind of information they need.

This study was supported by the company Siguru, a small start-up company developing information security software, and is a part of the development process for the forthcoming product.

2. User-Centered Security

Almost as long as we have had computers and computer networks, there has been an ongoing work with development of programs to make them more secure. The focus of this work has been to generate powerful tools to protect our systems. The same attention has not paid to making the users understand the programs and making the same people understand the importance of a secure behavior when using computers and computer networks (Whitten & Tygar, 1998; Flechais & Sasse in Cranor & Garfinkel 2005; Dourish & Redmiles, 2002).

Since the mid-nineties there has been a growing interest among researchers in the information security-area who has called for a more user-centered approach to information security. There is a growing amount of articles on the subject (E.g. Simon & Zurko (1996); Holmström (1999); DePaula et al. (2005)).

The term “user-centered security” was coined by Simons & Zurko (1996) at the proceedings of the ACM-conference in 1996, and it can be seen as a key component of the movement for user centered development of information security applications. The term refers to “Security models, mechanisms, systems and software that have usability as a primary motivation or goal” (Simon & Zurko, 1996, page 27).

3. Design Principles for Development of Information Security Applications

The same basic principles of usability that apply to other applications apply to information security applications. A great foundation for all usability design is the design principles developed by Donald Norman (Norman, 2002). They describe a number of heuristics that is likely to enhance the usability of a product, i.e.:

∉ Feedback, giving the user some sort of information of what his or her action has lead to will make the user more aware of the status of the system.

∉ Visibility, it is easier to label a control that only has one function. The label of a control can be used by the user to remember the controls' function. If a control has many functions there is an immediate risk that the labeling will be ambiguous.

∉ Constraints, if the designer is able to constrain the number of actions that a user can carry out at a specific moment, the designer is also able to minimize the number of errors that the user can carry out at the same moment.

Other principles specifically considered in this project are described below.

According to Berson (in Carnor & Garfinkel, 2005), as little text as possible should be used to explain facts to the user. At the same time, it is important for the user to understand what is being communicated by the design, though the amount of text should be kept at a minimum. Every word, button and pixel should have a pedagogic ulterior motive (Berson in Carnor & Garfinkel, 2005).

The complexity of the interface should be kept as low as possible. It is also important *not* to design an application for all potential tasks that a user might be willing to undertake. The design should rather focus on the tasks that the user is most likely to undertake (Berson, 2005).

An interface which gives the users too much information, information at the wrong time or in an unsuitable way, will be perceived as confusing by the user. If the amount of information is too small, there is a risk that the user will not discover potential security threats (Long & Moskowitz, 2005; Berson, 2005).

Teach the user simple tricks. For instance, in the web browser Firefox, the address bar turns yellow when the user enters a site that uses SSL (a protocol for transmitting data safely over the Internet). The user knows that the current page is a secure site when he/she sees this, without having to interact with numerous dialogue boxes (Berson, 2005). Using simple tricks like this is mainly positive, though the designer has to continuously consider whether the user really needs this information about the program. A clue about when to use these tricks is when there is some change in the state of the program that the user needs to know about (Berson, in Cranor & Garfinkel, 2005).

4. Method

The first task was to learn what the potential users of the product would actually want to know about security. This was learned through a number of interviews and by scenario testing, described in more details in a previous paper (Nohlberg & Bäckström, 2007). The results showed in general a specific interest in knowing about security from a financial and strategic perspective, grouped in sections of security information, rather than an interest in detailed data. In fact, security was perceived by the managers mostly as financial risks.
An interview was made with representatives from the sponsoring company, Siguru, in order to get a broader understanding of the product the interface was supposed to be used with, its limits and possibilities. This formed the first guidelines on how the interface was supposed to be designed.

When the information from the interviews was collected, a “lo-fi” prototype was constructed on paper. The design of the prototype was created on the basis of the information from the interviews and information regarding the design of interfaces that was found in the literature survey. The “lo-fi” prototype was made by hand drawings on paper, in order to quickly generate a sketch of the interface while at the same time communicating to the subjects that this was an early prototype in hopes of making them more willing to give improvement suggestions.

User tests on the lo-fi prototype were made on potential target users. The first subject was in charge of the information security in a major governmental organization in Sweden. The second subject is the chairman of an information security company. The two subjects did not take part in the interviews. The user tests were recorded with a video camera. The tests consisted of six tasks and ten questions. The tasks were conducted first (except for the first question “What are your impressions of the first page”) and were then followed up by questions.

The user tests were analyzed through a task log. The purpose of the task log was to find out where the test persons experienced difficulties with the prototype, why they experienced these difficulties, and what could bee done to eliminate these difficulties (Hackos & Redish, 1998). Through this procedure, it was possible to find concrete improvements of the interface as well as investigate the test person’s mental model of how the system should work.

The “lo-fi” prototype was updated to a “hi-fi” prototype with the feedback from the interviews, the results, and the inferences from the “lo-fi” tests taken into consideration. The “hi-fi” prototype was interactive and built using Macromedia Flash. The prototype thus emulated a working interface and the tests were done on a computer, in contrast to the tests done on paper with the “lo-fi” prototype.

The “hi-fi” tests were carried out on three potential end product users. The users all had management positions within their company. The first two test persons are managers of a science park, while the third person is the MD of a mobile application company. The persons in the user tests for the “hi-fi” prototype had not taken part in the interviews nor the user tests on the “lo-fi” prototype. The user tests were recorded with a video camera.

The user tests consisted of five tasks and thirteen structured questions connected to the tasks that had been performed. The questions were then complemented with follow up questions depending on the answers of the interview subjects. The user tests were analyzed through a task.

The “hi-fi” prototype tests resulted in an updated design of the interface and a number of requirements for how the program should behave and how it should be implemented in the organization, as well as a set of design heuristics.

5. Results

In this section the three stages of development are presented, represented also by figures. These figures show only a small part of all the screens in the product, and are of course in higher resolution and color in the actual software. The data displayed in the figures are to visualize the software UI, and does not represent any actual organization. The features and functions behind the data are proprietary to Siguru, and thus not discussed further here. Where the decisions have been made with a basis in CHI literature, it is referenced, in other cases it is decisions made during the study with conclusions from the prototypes as a background.

The “lo-fi” prototype, as seen in figure 1, was constructed with support from theory and information gained through interviews. The major design decisions that were supported by theory and the interviews were:
Every piece of information is (in most cases) just one or two clicks away. This is made possible through the flap system and supports "recognition rather than recall" (Nielsen, 1994).

Three flaps were added, policy, education and inventory, in order to match the typical managers mental model of information security, which was found during the interviews and the scenario attached to the interviews (Nohlberg & Bäckström, 2007).

Information that was not regarded to be highly important for the novice users was hidden under the triangles to support Nielsen's principle of minimalist design (Nielsen, 1994). This was also done to minimize the amount of text and pictures, which would lead to reduced complexity and reduced clutter. Through this, the user primarily gets an overview of the current situation rather than details, which was one thing the interviewees said they wanted.

The language was adjusted to suit managers rather than technicians.

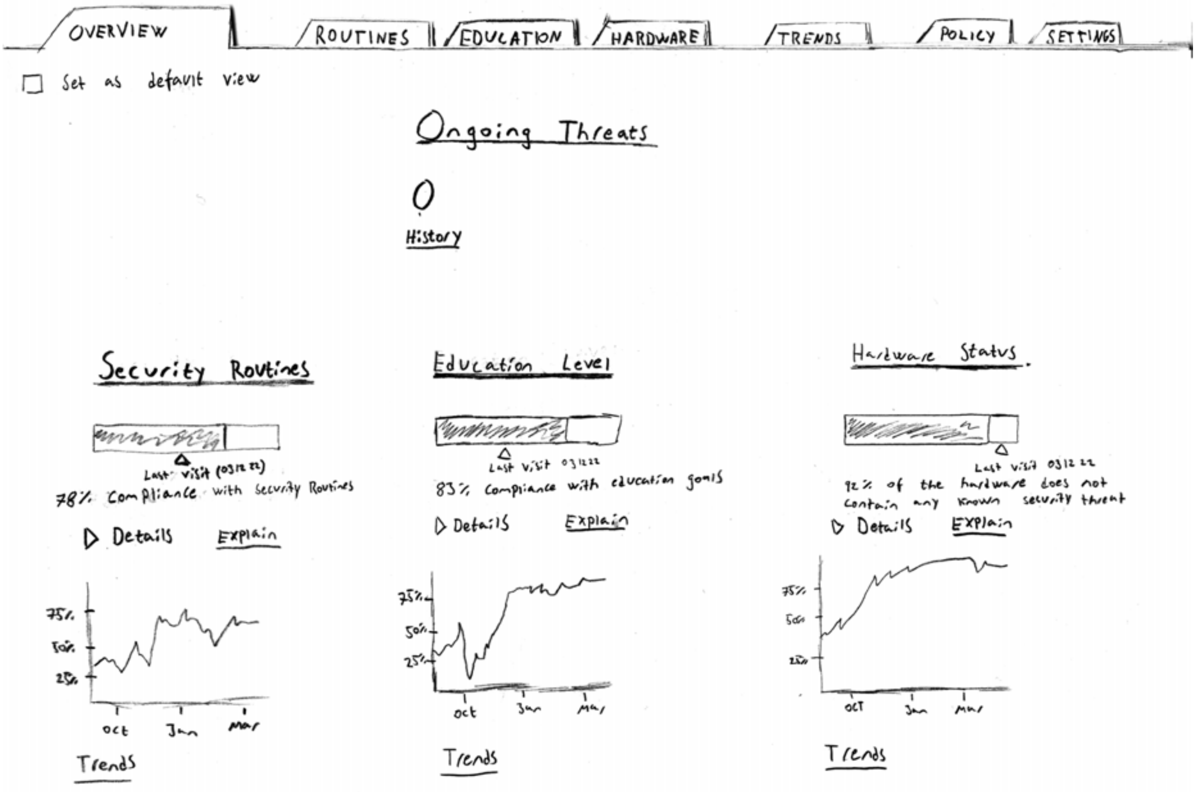


Figure 1: The "lo-fi" version of the overview page

The "lo-fi" prototype, as seen in figure 1, was developed on paper and tested. The major points of the feedback from the subjects where:

∉ The subjects preferred to have as little information as possible at the beginning, but also stressed that it was important to be able to access additional information in an easy way.

∉ The subjects want to be able to review why an incident happened and what can be learnt/improved from that. Because of that the history should include when and why the incident did happen, how much harm was done, what it cost, and other specific conditions at the time the incident happened.

∉ The subjects want to be able to see different threats that occurred at a certain time/period so that they can make strategic decisions based on this information. Therefore the history page should include an option that lets the user compare the threats during specific periods.

∉ It is important for managers to see the consequences of their investments in information security. Therefore a flap for money and resources was added to the “hi-fi” prototype.

∉ The subjects want to be able to see how severe a single threat/attack has been to the organization to make new decisions based on this information. Therefore the threats part of the inventory should include “consequences” of threats.

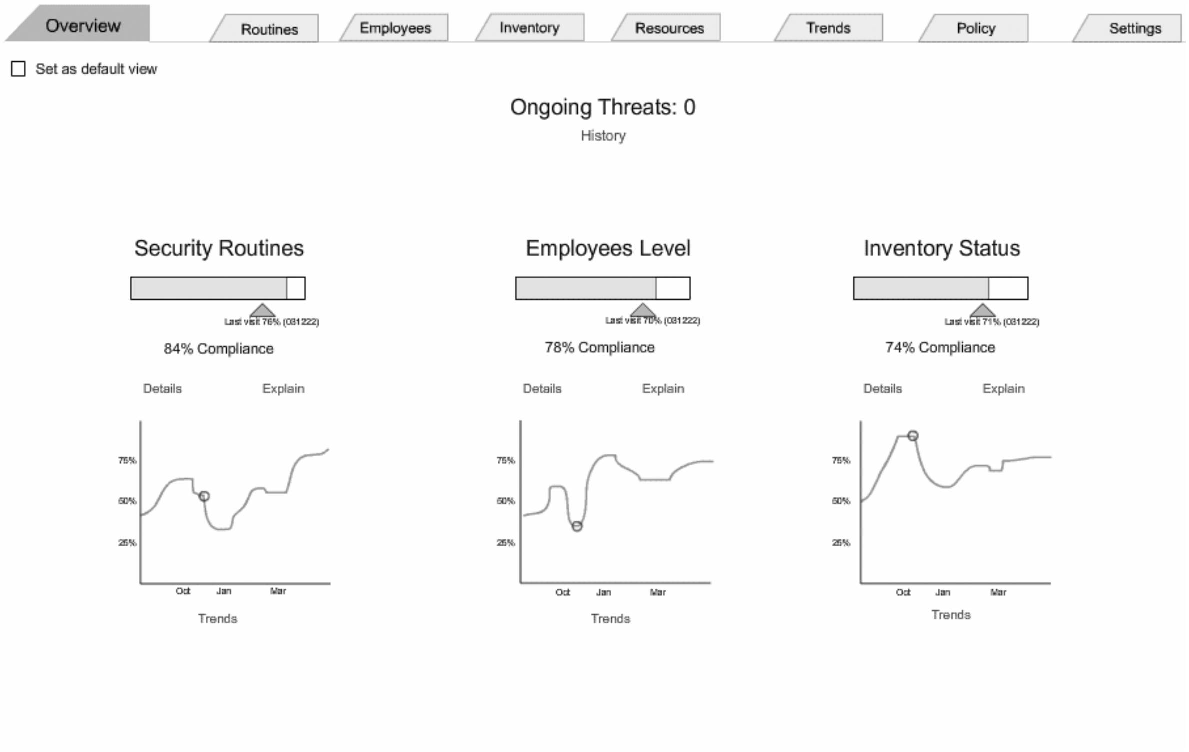


Figure 2: The “hi-fi” version of the overview page

The “hi-fi” prototype was developed further based on the results of the “lo-fi” tests and the interviews mentioned above; a screenshot can be seen in figure 2. The major points of feedback gained from the subjects were:

∉ A contextual help for each function that the users can access at any time will enhance the interaction with the system and provide guidance to the users when they need it.

∉ If the colors of the bars change depending on the status of the bar (e.g., if the value of a bar is critical, it should be red), then the users will easier interpret the value of the bar. Therefore if a value of a bar is acceptable, it should be in one color, if it is not acceptable it should be in another, and if it is close to not being acceptable it should be in a third color.

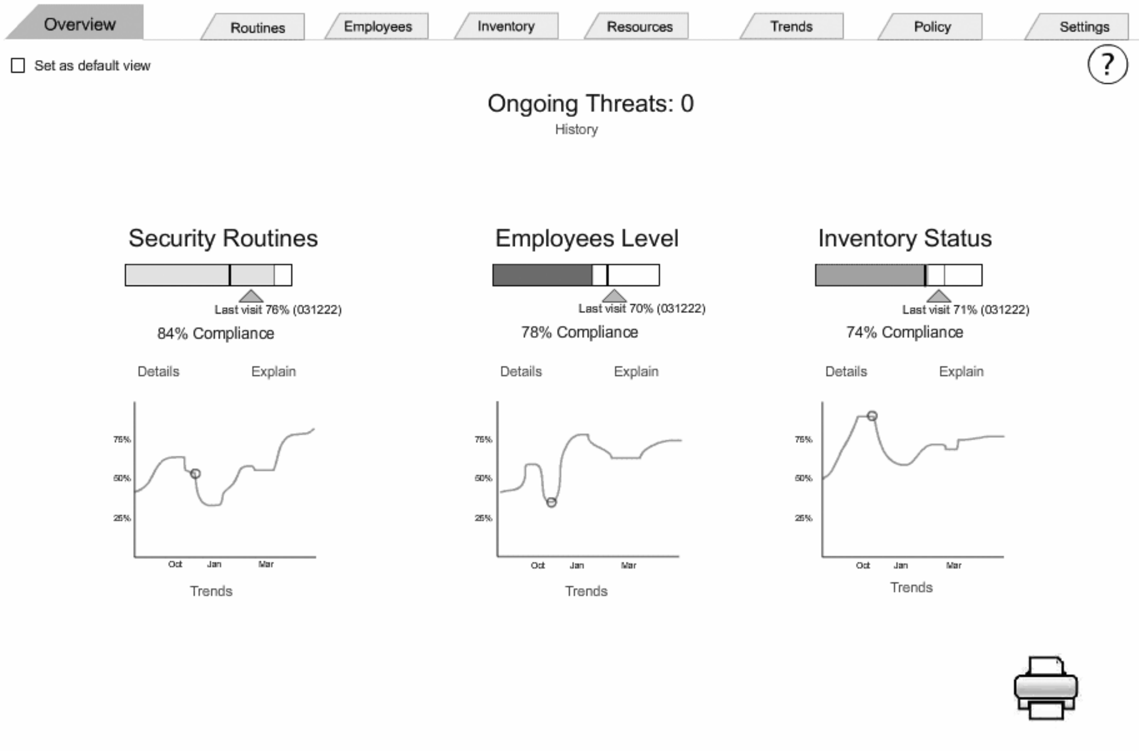
∉ When a user expands information that concerns a single subject, it should be made clear whether the information that he is expanding is connected to the information above or if it is new information. Therefore information that gives an overview of something should be made clearer and separate from information regarding one individual person

∉ According to the subjects it is important to be able to use the software to follow up the goals of the company, expenses etc. and thereby facilitate their ability to make strategic decisions. Therefore the trends graph should have an indication of how the different values relate to the reference values of the company. All the subjects stressed that it was very important that the program should support strategic and financial decisions, since that is a very important aspect of managers' responsibility.

∉ All subjects were satisfied with the amount of information that the interface presented.

∉ All subjects stressed that it was important to involve their subordinates in the system. By doing this they were likely to be more motivated to act in a secure way and at the same time they won't feel as monitored as they would feel if they were not involved.

All the subjects stressed that the information that was important to managers was information that gives an overview of the current situation rather than information that gives details about information security, and that the information should be presented using a vocabulary that managers can understand.



Ongoing Threats: 0

Security Routines — Last visit 76% (031222) — 84% Compliance

Employees Level — Last visit 70% (031222) — 78% Compliance

Inventory Status — Last visit 71% (031222) — 74% Compliance

Figure 3: The final version of the overview page

This input was used when developing a final version of the interface; a screenshot of the final version can be seen in figure 3 above.

6. Conclusions and Discussion

Managers are interested in security, but often find it hard to grasp the knowledge needed to fully understand and to make decisions about security. Therefore the information given to managers about security should be adapted to the specific needs of the target audience, rather than the technical possibilities or the requirements of technical personnel. This project has found several key characteristics of what managers' wants to know about security:

1. Managers are more interested in the overall status of the information security of the company than the details. This does not make managers uninterested in details, but they only want them when they need them, and they tend to group together areas of information security.
2. Managers consider information security on a more strategic and financial level than security specialists tend to do, focusing more on risks.
3. Managers do not only see security from the perspective of security, but also considers the possibility of making other gains, such as increased efficiency, minimized downtime etc.

In order to cater to the specific needs of managers, three design heuristics for user centered security design aimed at managers were developed during development of the interface. They were based on the works of Norman (2002) and further developed in this context:

1. Provide overview information very early in the program. The typical manager does not have the time or the knowledge to make this overview by himself/herself.
2. Do not overwhelm the user. Normally a manager is not interested in the details of the information security and/or does not have time to read this sort of information. If the manager wants the information, the manager is likely to find it.
3. Provide information in a way that is familiar to the manager. Use wordings that the user understands. Provide contextual help for expressions that must be presented in a technical way.

This project aimed towards developing an interface to display security related information to managers. The user centered process for creating the interface has been successful. The concept and the interface have been appreciated by both the subjects and the company, and are now going to be used as the basis for developing the actual "Siguru"-product.

From a managerial perspective, it is important to know where the educational and economic resources should be spent to secure proper information security in the entire organization. This kind of information security information systems might be able to prevent people from acting in an insecure way, since it will help managers to make the right investments, be they in technology, resources, or education.

In the future, the Siguru-software will also consist of an education module, to be used by each and every employee. This is believed to help the employees to educate themselves in security, as well as improve general awareness of security. With a management information system like the one proposed in this study as a foundation, security education can be transformed from a mere sidetrack to a critical process, the same way that information security might be transformed; by helping the decision makers understand, and be active in the process. Information security might finally be integrated in the normal decision processes of managers. That is the first step to get a really secure organization – when those making the decisions both care about security and understand it, and a good way to stop committing the 10 deadly sins of information security management (von Solms & von Solms, 2004).

7. Acknowledgment

The authors would like to thank the subjects for giving freely and willingly of their time. The authors would also like to thank colleagues and friends for support during the process, in particular Benkt Wangler, Stewart Kowalski, Thomas Ekström from The Logic Planet AB and Alexander Backlund.

References

Berson, J. (2005), *Zone Alarm: Creating Usable Security Products for Consumers*, in Lorrie, F.C. and Simson G., *Security and Usability,* O' Reilly Media, Sebastopol, CA.

Department of Trade and Industry (2004) "United Kingdom's Department of Trade and Industry's Information Security Breaches Survey 2004", www.pwc.com/uk/eng/ins-sol/publ/pwc_DTI-InfoSecutiry-Survey2004-Exec.pdf, (Accessed 10 May 2006)

DePaula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D., Ren, J., Rode, J. & Silva, F.R. (2005), "Two Experiences Designing for Effective Security", cups.cs.cmu.edu/soups/2005/2005proceedings/p25-depaula.pdf, (Accessed 15 November 2006)

Dourish, P. and Redmiles, D. (2002), *An approach to Usable Security Based on Event Monitoring and Visualization*, New Security Paradigms Workshop 02.

Furnell, S.M., Jusoh, A., Katsabas, D. and Dowland, P. (2006), *Considering the Usability of End-User Security Software*, Proceedings of 21st IFIP International Information Security Conference (IFIP SEC 2006), Karlstad, Sweden, 22–24 May 2006, pp. 307–316.

Flechais, I. and Sasse, A.M. (2005), *Usable Security,* in Lorrie, F.C. and Simson, G., *Security and Usability,* O' Reilly Media, Sebastopol, CA.

Hackos, J.T. and Redish, J.C. (1998), *User and Task Analysis for Interface Design,* John Wiley & Sons, Inc., New York, NY.

Holmström, U. (1999), "User-centered design of security software", www.hft.org/HFT99/paper99/Design/5_99.pdf, (Accessed 10 October 2006)

Long, C.A. and Moskowitz, C. (2005), *Simple Desktop Security with Chameleon*, in Lorrie, F.C. and Simson, G., *Security and Usability,* O' Reilly Media, Sebastopol, CA.

Nielsen, J. (1994), *Heuristic evaluation,* in Nielsen, J., and Mack, R.L., *Usability Inspection Methods,* John Wiley & Sons, New York, NY.

Nohlberg, M., Bäckström, J. (2007)*, Talking Security to Management: How to Do it.* Unpublished paper submitted for review.

Norman, D. (2002), *The Design of Everyday Things,* Basic Books, New York, NY.

Rasmussen M. (2002), "IT-Trends 2003: Information Security Standards, Regulations and Legislation"*,* images.telos.com/files/external/Giga_IT_Trends_2003.pdf, (Accessed 5 August 2006)

Simon, R.T and Zurko, M.E. (1996), *User-centered security,* Proceedings of the UCLA conference on New security paradigms workshops September 17 – 20, portal.acm.org/citation.cfm?id=304859, (Accessed 5 August 2006)

Von Solms, B., Von Solms, R. (2004), The 10 deadly sins of information security management, *Computers & Security* 23 (5), pp. 371 – 376.

Tygar, J.D & Whitten, A. (1998), "Usability of Security: A Case Study", reports-archive.adm.cs.cmu.edu/anon/1998/abstracts/98-155.html, (Accessed 2 August 2006)