PROJECT DESCRIPTION

Study Objectives

Computer and information security (CIS) is usually approached from a technology-centric viewpoint. Remedies for CIS vulnerabilities and breaches tend to focus on technical mechanisms, e.g., stronger firewalls and implementation of encryption. However, the potential weakness of technical solutions and the danger of focusing solely on technical solutions have been highlighted by many. Schneier (2000) states: "Computer security is difficult (maybe even impossible), but imagine for a moment that we've achieved it… Unfortunately, this still isn't enough. For this miraculous computer system to do anything useful, it is going to have to interact with users in some way, at some time, for some reason. And this interaction is the biggest security risk of them all. People often represent the ***weakest link*** in the security chain and are chronically responsible for the failure of security systems." A similar message was provided by Mitnick and Simon (2002): "A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business. The company is still totally vulnerable... the human factor is truly security's ***weakest link***." These two quotes describe the 'weak link' of the human factor; however, it is important to understand that the 'weak link' is actually the one who designs, maintains and uses computer and information systems. Therefore, it is important to design CIS systems and processes that consider the needs, characteristics, strengths and limitations of those people, i.e. to adopt an approach based on the discipline of human factors engineering. Such an approach can help understand behaviors of end users and network administrators, and the factors that affect their behaviors and are amenable to some type of intervention or change.

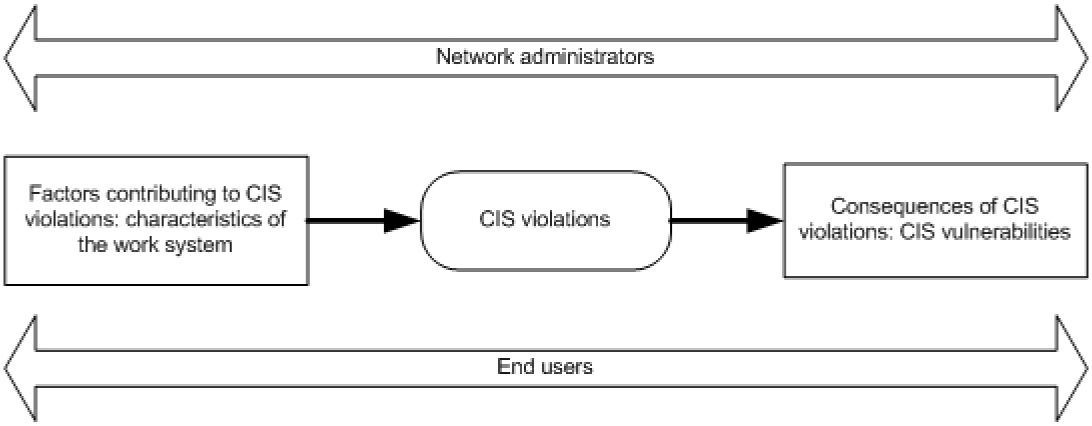
The technical CIS remedies are often designed and implemented with little consideration for the needs and characteristics of the end users, network administrators and CIS managers. This lack of consideration for human factors may create situations where people have to circumvent the CIS mechanisms and procedures in order to perform their job. Some anecdotal evidence exists to show that CIS can be compromised as the results of actions by the designers and users of the computer and information system. Therefore, understanding the role of the 'legitimate users' is of critical importance. This study will focus on (non-malicious) violations committed by end users and network administrators.

CIS incidents are often related to actions by 'insiders', i.e. network administrators and end users (Gordon, Loeb, Lucyshyn, & Richardson, 2005). Some of these actions may represent violations of rules, policies, instructions or procedures related to CIS. We propose to examine violations in CIS committed by two groups of people: (1) network administrators, and (2) end users. We will used a mixed-methods research approach that combines qualitative (interviews and focus groups) and quantitative (survey) research in order to understand CIS violations, their consequences and the factors contributing to violations, and to develop solutions to deal with CIS violations.

Definition and research model

Violations are defined as deliberate deviations from those practices (i.e. written rules, policies, instructions or procedures) believed necessary to maintain safe or secure operations (Reason, Manstead, Stradling, Baxter, & Campbell, 1990). The literature on violations emphasizes the role of the social and organizational context, where behavior is governed by operating procedures, codes of practice, rules and regulations (Lawton, 1998; Reason et al., 1990). This approach emphasizes factors in the work system of end users that can contribute to violations. Figure 1 presents the model of CIS violations used in the proposed research.

Figure 1 – Model of CIS violations


Network administrators
Factors contributing to CIS violations: characteristics of the work system
CIS violations
Consequences of CIS violations: CIS vulnerabilities
End users

CIS violations are committed by end users and network administrators that deliberately do not follow rules, policies, instructions or procedures. Sometimes, CIS policies are not written down, but are understood (or should be understood) by everyone, such as not giving known hackers/criminals accounts on the system. In some cases, there are policies that are written down for appearances of government regulators, but that are just not followed or that the organization does not expect to be followed. There are hierarchies of policies from the parent organization down to the lower-level organization that a user is supposed to follow. However, local practices may deviate from the parent's organization because of the preferences of the leader of the local organization, possibly in violation of the parent organization’s policy. These examples of CIS policies show that the specificity of CIS will need to be considered in our research on violations. Whereas the definition of violations is widely accepted in various applications (e.g., industrial safety, driver behavior), it may need to be further refined and maybe modified for the CIS domain. This will be explored in the first phase of the proposed research.

Our model of CIS violations emphasizes the role of various *work system characteristics as contributing to CIS violations*. Many times end users are simply unaware of the consequences of the violation. Adherence to security policy may involve degradation in performance or functionality. The end user may honestly believe that the rule is unnecessary or unduly hampers operations and therefore makes a decision on their own behalf or on behalf of their team. Many users have experienced policies that are overly conservative or ill-conceived and may therefore be less willing to comply with security policies. Many end users and network administrators do not directly pay the consequences of a failure resulting from their violation. There may not be time or staff to comply with the policy (for example, install all patches to all systems as soon as they come out can just be prohibitive). These are some of the possible reasons why CIS violations occur; they represent the following elements of the work system (Carayon & Smith, 2000; Smith & Carayon-Sainfort, 1989): the person (e.g., lack of knowledge), task and organizational factors (e.g., lack of resources to comply with policy). Our research will explore systematically the reasons or factors contributing to CIS violations, including all elements of the work system (the person, task, physical environment, tools and technologies, and the organization). This research can then help identify solutions for improving CIS-related behaviors of end users and network administrators (i.e. reducing the occurrence of violations or mitigating their impact on CIS vulnerabilities).

Background and Literature Review

Violations in safety

The cognitive and social sciences have developed various taxonomies for the classification of human error in safety (Rasmussen, 1982; Reason, 1990). Human error is the failure of planned actions to achieve their intended consequences (Reason, 1990). A closely related concept is *violations*, or deliberate (though not necessarily reprehensible) deviations from those practices believed to maintain safe or secure operations (Reason et al., 1990). Violations need to be described in their social and organizational context (Reason et al., 1990). Various elements in the work environment may propagate the occurrence of violations, such as time pressure or a large number of tasks to perform.

Reason (1990) offered a preliminary classification of violations. Violations vary according to intentionality and outcome: acts of sabotage/terrorism and deliberate actions that may or may not result in a negative outcome. Further, there are three major categories of deliberate violations: routine, optimizing, and situational (Reason, Parker, & Free, 1994). Routine violations are “corner-cutting” or short cuts, optimizing violations reflect actions unrelated to the functionality of the task (e.g., job of high speed driving), and situational violations are seen as essential to get the job done in a particular work situation. For example, Hobbs and Williamson (2002) surveyed 1,359 aviation mechanics on workplace accidents and incidents. They found that violations are strongly associated with quality incidents, but are not necessarily precursors of accidents. Violations may set the scene for an accident because they increase the probability of error. For example, the omission of a functional check at the completion of maintenance work may not in itself lead to a problem, but could permit an earlier lapse to go undetected. The taxonomy of Reason et al. (2004) will serve as a basis for our taxonomic framework of CIS violations and factors contributing to CIS.

Violations in safety research have also been explored in automobile driving. Parker and colleagues (1995) surveyed 1,656 drivers and using the Driver Behavior Questionnaire, examined the relationship between driving behavior and involvement in accidents. The results revealed that violations, or behaviors that involved deliberate deviations from safe driving practice, were predictive of accident liability. This survey study further emphasized the point that violations lead to accidents. In our proposed research, we contend that unsecure behaviors, such as violations, can be predictive of vulnerabilities and security breaches.

Further, the healthcare field has begun to explore caregivers’ violations of protocols (Parker & Lawton, 2000). A survey study describing medical practice was administered to 315 nurses, doctors, and midwives and 350 members of the general public in the UK. The study examined two factors manipulated within nine scenarios of surgery, anesthetics, and obstetrics. The first factor, behavior, was described as an improvisation (no rule availability), the violation of clinical protocol, or compliance with a clinical protocol. The second factor, patient outcome, was described as good, bad, or poor. Both samples of healthcare providers and the general public were asked to evaluate the nine scenarios with regard to the inappropriateness of the behavior, the likelihood that they would take further action (i.e. reporting by healthcare provider and complaining by the public) and responsibility of the outcome (e.g., the healthcare professional, the patient, the protocol itself, the hospital). Results showed that the violation of protocols and bad outcomes were judged most harshly. Irrespective of outcome, violations were evaluated more negatively. The authors warned against over-reliance on procedures (or protocols) as a form of organizational defense against accidents or claims. Procedures may stifle innovation and make people less able to function in novel situations. A study of policies and procedures in computer security should therefore capture the range of (positive or negative) consequences of violating those policies and procedures.

Lawton (1998) examined violations of safety rules by railway workers. A pilot study of 11 shunters and pilot drivers identified perceived risk and frequency of 40 rules concerning general safety on and around the track and rules prescribing safe shunting. The results of the pilot study were used to generate a list of 12 violations that were examined subsequently in a questionnaire survey of 36 shunters. The survey respondents were asked to identify the top (up to five) motives for each of the 12 violations. The most frequently cited motives were: quicker way of working (39%), inexperienced shunter (38%), time pressure (37%), and high workload (30%). Other motives included characteristics of the shunter (e.g., lazy, skilled), characteristics of the rule (e.g., impossible to work according to the rule), characteristics of the tools and technologies, lack of management commitment to safety, and physical fatigue. Lawton performed a cluster analysis to classify the violations with respect to the reasons given for noncompliance. The cluster analysis approach developed by Lawton to examine safety violations will be used in our study to examine CIS violations of network administrators and end users.

Violations in CIS

Violations committed by the ‘legitimate users’ can affect the state of CIS. The CSI/FBI survey of 453 respondents from U.S. corporations, government agencies, financial institutions, medical institutions, and universities, revealed that those organizations experienced incidents from the *inside*: (1) 46% reported 1-5 incidents; (2) 7% reported 6-10 incidents; and (3) 3% reported 10 or more incidents (Gordon et al., 2005). Some of these incidents could involve violations committed by network administrators and end users.

In 2004, an attacker named “Stakkato” launched a successful Internet attack of Cisco Systems, the US Military, NASA, and research laboratories (Markoff & Bergman, 2005). The attack executed an organized system for automating the theft of computer log-ins and passwords. One part of the overall attack was exploiting a vulnerability that resulted from unpatched SSH software version. In this instance, a network administrator or IT professional may have intentionally decided to not patch or upgrade the system to eliminate SSH vulnerability. In network administration, applying patches and upgrading systems are part of many tasks that include the design, implementation, and maintenance of CIS systems. However, network administrators may have to take “short cuts” (i.e. perform violations such as not applying patches) in order to compensate for factors in their work environment. For example, network administrators tend to have a high workload, which can inhibit them from monitoring and maintaining the patches for their CIS systems (Kraemer, Carayon, & Clem, 2006; Kraemer &

Carayon, forthcoming). High workload is usually associated with other organizational constraints, such as understaffing, no upper management support, or lack of prioritization. For some of these reasons, network administrators may perform violations, or take short cuts, in order to accomplish most of their tasks. However, things will be missed, such as patching vulnerable software, as was exemplified in the Stakkato example.

Besnard and Arief (2004) have described users' "trade-offs" to commit violations from a cognitive approach. They propose that user decisions regarding security in the workplace can be interpreted in terms of an intuitive cost-benefit trade-off. For example, logins and passwords require the user to recall and use. Given the mandated complexity of passwords and the number of passwords to recall, users may use storage features (i.e. cookies) or write them down, given their judgment of the importance of the data protected. This cognitive 'trade-off' analysis is only one of many explanations for CIS violations. The research on violations in other domains has highlighted a number of other motives or reasons for violations, such as high workload and time pressure, lack of knowledge and lack of management commitment to safety/security.

Stanton and colleagues (2005) conducted an empirical analysis of end user security behaviors by interviewing 110 IT professionals, managers, and regular employees. Interview data were used to create a two-factor, six-category taxonomy of intentionality (i.e. malicious, neutral, beneficial) and technical expertise (i.e. high, low). In this taxonomy, violations exist on the neutral/high or neutral/low dimensions, where behaviors have no clear intentions to do harm to the organization's IT or resources. An example of a violation from someone with a high level of expertise and neutral intention would be a network administrator configuring a wireless access gateway that inadvertently allows wireless access to the company's network by people passing in cars. An example of violation from someone with a low level of expertise and neutral intention would be an end user choosing a weak password that is easy to remember, such as their name. Stanton and colleagues also conducted a follow-up survey of 1,167 end users in the financial, manufacturing, health, military, government, and telecommunications industries on password-related behaviors (e.g., frequency of changing the password, sharing passwords with others) as well as training and organizational awareness (e.g., organization provides training programs to promote CIS awareness). They found significant correlations between good password-related behaviors and training and awareness.

Although these expert opinions and studies observe the role of violations by CIS end users, network administrators, and managers, they have not fully taken into account how the work system or environment contributes to the behavior or decisions. In addition, this research has not examined CIS violations in a systematic basis. Further research is needed to identify all possible CIS violations, their causes and their consequences.

Preliminary research

Researchers at the Center for Quality and Productivity Improvement (CQPI) of the University of Wisconsin-Madison have conducted preliminary research on human errors and violations in computer and information security (Funding provided by Department of Defense on "Modeling and Simulation for Critical Infrastructure Protection"; #DAAD19-01-1-0502, PI: Stephen Robinson, UW-Madison). This research has been performed in collaboration with the UW E-

Business Institute, the Computer Sciences Laboratory at the UW-Madison and Sandia IDART program.

Kraemer and Carayon (forthcoming) studied how various work system elements propagate human error and violations and consequently create or promote CIS vulnerabilities. They interviewed 10 network administrators and 10 CIS managers to obtain descriptions of the types of violations committed by end users and network administrators. For example, network administrators intentionally introduce holes in firewalls so that outsiders who are collaborating on projects can have access to their networks. They may do this because they lack a set procedures or rules that have been agreed upon by the user groups, or they may be so overworked and pressed for time that allowing holes in the firewalls is the quickest and easiest way to complete their tasks.

Kraemer, Carayon, and Clem (2006) conducted a study of red team members' views of CIS violations of end users and network administrators and related work system factors. They interviewed 14 red team members from Sandia National Laboratories' Information Design and Assurance (IDART) program. The interviews yielded a preliminary taxonomy of CIS violations and related work system factors. Overall, red team members commented on *routine* CIS violations of end users (9 of 23 total comments) and network administrators (14 of 23 total comments) and work system factors associated with those routine CIS violations (44 total comments). The work system factors associated with end user routine violations were: lack of CIS understanding (3 of 15 comments), individual beliefs related to CIS (11 of 15 comments) and incorrect technology (1 of 15 comments). The work system factors associated with network administrator routine violations were: poor CIS policy (2 of 29 comments), individual beliefs related to CIS (9 of 29 comments), lack of prioritization of work tasks (14 of 29 comments), and other various task related factors (4 of 29 comments). An example of an end user routine violation would be writing down a password that is difficult to remember because they lack the understanding of the importance of keeping it memorized and other work tasks take precedence over memorization of passwords. An example of a network administrator routine violation would be creating one password to serve multiple machines because they are overwhelmed with their CIS and non-CIS related duties. This short cut allows them to complete their work more efficiently.

The major weakness of our preliminary research is the lack of data gathered from the end users themselves. We have captured network administrators' and red team members' views about errors and violations committed by end users (Kraemer et al., 2006; Kraemer & Carayon, forthcoming). In the proposed research, we will capture the views of the end users in order to verify, expand, and specify the various work system factors associated with CIS violations of end users. The views of the end users are essential in creating a valid taxonomy of factors and work system solutions.

Significance

The proposed research effort will take advantage of the expertise in computer and information security of Sami Saydjari, president of the Cyber Defense Agency (CDA). This will ensure that the research developed is anchored in the 'reality' of computer and information security problems. In addition, the direct involvement of CDA in the proposed research will help facilitate the dissemination of the research results. We will also collaborate with Professor Veeramani and the UW E-Business Institute in the research and dissemination efforts.

Our research will have the following specific contributions:

- We will define CIS violations committed by end users and network administrators.
- We will create scenarios and case studies to show the linkages between CIS violations and CIS vulnerabilities and breaches.
- We will develop a survey to assess the organizational risk for CIS violations and to identify the factors contributing to CIS violations.
- We will identify a list of solutions for preventing CIS violations and reducing their negative consequences.

These specific contributions are anchored in the disciplines of human factors engineering, computer sciences and industrial and systems engineering, and will lead to further scientific progress in each of these disciplines. For instance, an examination of the program of the Human Factors and Ergonomics Society annual conferences in 2003-2005 shows no contribution related to the area of cybersecurity, except for our papers on a human factors vulnerability analysis of computer and information security (Kraemer & Carayon, 2003), red team performance (Kraemer, Carayon, & Duggan, 2004) and computer security culture (Kraemer & Carayon, 2005). Our proposed research program should trigger interest on the part of the human factors engineering discipline for researching and studying CIS. We can serve as an example of the involvement of human factors engineering in research on CIS. In addition, there are unique characteristics of CIS that can lead to further scientific development of human factors engineering concepts, models and theories.

We will also disseminate our research to the computer security discipline in order to help them understand the important role of human and organizational factors in CIS. We will submit a paper to the USENIX Security Symposium. Somesh Jha, assistant professor of computer sciences at the University of Wisconsin-Madison, is a member of the program committee for the 15th USENIX Security Symposium. We have recently consulted with him regarding a paper on human and organizational factors in CIS that we intend to submit to this conference. His advice was very important to help us improve our paper. We will consult with Professor Jha and Sami Saydjari about future submissions to the USENIX Security Symposium or other computer security conference.

The proposed research can provide significant information to companies interested in (re)designing their organizational systems and processes in order to prevent the occurrence of CIS violations. Creating more rules, policies and procedures may not be the ‘right’ answer to improving CIS. According to Reason et al. (1998), “one of the effects of continually tightening up safe working practices is to increase the likelihood of deliberate deviations from these practices: in other words, encourage violations”. Our research can highlight the organizational and work system factors that contribute to CIS violations, and allow the discovery of solutions that do not solely rely on rules, policies and procedures and that improve the design and implementation of CIS rules, policies and procedures.

Methodology

Our proposed research is described in Table 1. The research activities are listed in the order in which they will be performed, as each activity produces information useful to the next research activity. This mixed-methods approach begins with qualitative research (focus groups and interviews) aimed at identifying the list of possible CIS violations, continues with quantitative research (survey) to identify the most frequent and risky CIS violations, and ends with qualitative research (focus groups) to create a list of possible solutions and approaches dealing with CIS violations.

Table 1 – Proposed research activities

Research activity	Participants	Purpose	Outcomes
Focus groups	- network administrators - CIS managers - CIS experts	To identify CIS violations and their consequences	List of CIS violations and consequences
Interviews	- network administrators - end users	To identify factors contributing to CIS violations	List of factors contributing to CIS violations Draft questionnaire on CIS violations
Survey	- network administrators - end users	To quantify the risk of CIS violations	Identification of most frequent and most risky CIS violations and their contributing factors
Focus groups	- CIS managers - CIS experts	To identify approaches for preventing or reducing the impact of CIS violations	List of solutions for CIS violations

Focus groups – Identification of CIS violations and their consequences

Our preliminary research has identified some CIS violations and their consequences. We propose to build on this preliminary research by gathering additional data from network administrators, CIS managers and CIS experts. These three groups of people have the CIS technical knowledge and expertise to help us identify CIS violations and the consequences of CIS violations. Some of these violations may result in security vulnerabilities or weaknesses in operating system application code, or configuration that makes it possible for threats to exploit the system (or underlying network) thereby creating negative impact or damage (Taylor, 2004). Thus, creating the basis of a “universal vulnerability”, a state in a computing system(s) that allows the attacker to: (1) execute commands as another user; (2) access data that is contrary to the specified access restrictions for that data; (3) pose as another entity; and (4) conduct a denial of service (The Mitre Corporation, 2006). On the other hand, some of violations may not result in security vulnerabilities or weakness, and may actually represent innovative ways of dealing with novel situations. This phase of our research will help clarify the relationship between CIS violations and CIS vulnerabilities, i.e. the consequences of CIS violations.

Study procedures. We will conduct 3 focus groups, one with each of the 3 groups (network administrators, CIS managers and CIS experts). Each focus group will last 2 hours and will be comprised of about 5 participants. The participants will be recruited with the help of Professor Veeramani, director of the UW E-Business Institute, and Sami Saydjari, president of the Cyber Defense Agency (CDA). At the beginning of the focus group, the definition of CIS violations will be explained and examples of CIS violations will be described (these examples will come from our preliminary research). The discussion in the focus groups will be organized around the following questions:

- What are the different violations committed by network administrators and end users that contribute to security vulnerabilities and breaches in computer and information systems?
- What is the impact of the violations, as measured by the extent of the security vulnerability or breach?

These questions are similar to the questions we have used in our preliminary research on errors in CIS. Our preliminary data collected from Sandia red team members provide information only on “routine violations”, i.e. “corner-cutting” or short-cuts taken in order to accomplish work tasks. We will facilitate the focus groups’ discussion in order to capture all categories of violations: routine, optimizing and situational (Reason et al., 1994).

The focus groups will be led by two members of the research team: one researcher will be the main facilitator of the discussion whereas the second researcher will ensure that all topics have been addressed throughout the discussion. The focus groups will be audio recorded, and the tapes will be transcribed electronically for further qualitative data analysis.

Data analysis. A content analysis of the focus groups data will be performed using the qualitative software package, QSR NVivo©. Requirements for data quality in qualitative research will be met through the following activities:

- Three researchers will read all of the data, and together define a preliminary node structure. A node structure is comprised of nodes (i.e. categories) and sub-nodes (i.e. sub-categories). The taxonomy of violations developed by Reason and colleagues (1998) will also be used to develop the preliminary node structure of CIS violations.
- One researcher will perform the content analysis by reading each transcript in its entirety while making marginal notes to assist in developing coding categories. The researcher will look for key words or phrases that appeared to be distinctive and occur in subsequent passages. These phrases will be the titles of the subnodes.
- A definition will be assigned to each node and sub-node.
- The coding strategy consists of two elements: (1) comments will be coded once in analysis and (2) comments will be coded at the most specific node. We will create a mutually exclusive taxonomy of violations; therefore, we will not adopt a cross-coding strategy.
- After the coding all of the transcripts, the same researcher will re-read the content of all the nodes and sub-nodes to check for inconsistencies, redundancies or impreciseness.
- In order to check for inter-rater reliability, two researchers will each code a focus group transcript, using the node structure and definitions provided by the first researcher. Inconsistencies will be identified and reconciled within the node structure.
- The first researcher will apply the changes to the node structure, check the content of all of nodes, and make any necessary changes resulting from the inter-reliability test.

- The comments and nodes will be quantified by aggregating the number of comments at the most specific nodes.

The outcome of the data analysis will be an exhaustive list of CIS violations (possibly categorized by type of violation: routine, optimizing and situational) and consequences associated with each category of violation. Because violations occur with respect to a specific CIS policy, rule or procedure, the full enumeration of all CIS violations may not be possible. The focus of our analysis will be on the development of 'generic' categories of CIS violations, such as violation regarding policy for password quality.

Interviews – Identification of factors contributing to CIS violations

Our preliminary research has identified some of the reasons for CIS violations. For instance, network administrators are often overburdened with too many tasks, lack of prioritization of tasks, and understaffing (Kraemer et al., 2006; Kraemer & Carayon, forthcoming). Further, end users may take short cuts when they have a lack of understanding of the importance of CIS. We propose to expand on this research effort by conducting individual interviews with network administrators and end users. We will use the list of CIS violations produced at the previous stage in the interviews.

Study procedures. A total of 15 interviews with network administrators and 15 interviews with end users will be conducted. Each interview will last about 1 hour and will be audio recorded. Interview data will be transcribed electronically. At the beginning of the interview, the list of CIS violations and consequences that came out of the first step will be presented to the interviewee. The interviewee will be asked to think about instances when CIS violations have happened (for instance, s/he has committed a violation or someone else has committed a violation) and to describe the circumstances surrounding those violations. This approach is similar to the critical incident technique (Flanagan, 1954). A few examples of factors contributing to CIS violations will be provided (these examples will come from our preliminary research); this will help 'frame' the discussion so that the interviewee understands that the focus is on the work system factors as contributors to CIS violations.

Data analysis. A content analysis of the interview data will be performed using QSR NVivo©. The same data analysis process described above will be used for this phase of the research. The outcome of this data analysis will be a list of factors contributing to CIS violations. These factors will be organized into categories. The categorization scheme could be based on the work system model developed by Carayon and Smith (Carayon & Smith, 2000; Smith & Carayon-Sainfort, 1989). We have successfully used this model to describe human errors in CIS and the factors contributing to human errors (Kraemer & Carayon, 2006). It is very likely that we will develop two different categorization schemes for network administrators and end users.

We will also use the interview data to draft a questionnaire on CIS violations. The questionnaire will be structured as follows:

- Demographics and background information, including job category
- List of CIS violations and questions on self-reported frequency
- List of factors contributing to CIS violations and questions on self-reported frequency.

We will use the approach used by Lawton (1998) in a study of safety violations and accidents among railway workers. She came up with a list of 12 safety violations (e.g., "The shunter works without wearing the high visibility clothing provided”) and a list of 14 reasons for violation (e.g., “This is a quicker way of working”). She then asked 36 shunters to indicate from the list of 14 reasons up to five which were most likely to encourage the shunter to commit each of the 12 violations. Our questionnaire will be formatted in a similar way: we will ask network administrators and end users to identify the most frequent contributing factors for each of the CIS violations.

Three network administrators and three end users who participated in the interviews will be asked to participate in the pilot study of the draft questionnaire. The pilot study will examine the following issues:

- Clarity of the questions
- Completeness of the survey
- Duration of the survey.

It is possible that the questionnaire will be slightly different for network administrators and end users. Our preliminary research shows that different work system factors can contribute to CIS violations: the Sandia red team members mention lack of CIS understanding as a factor explaining CIS violations by end users, but not by network administrators, and mention lack of prioritization of tasks as a factor for network administrators, but not for end users.

Survey of network administrators and end users

A survey of network administrators and end users will be conducted in order to quantify the extent to which (self-reported) CIS violations occur and the factors contributing to CIS violations. The survey will also examine the relationship between CIS violations and contributing factors, therefore allowing the identification of key contributors to CIS violations.

Study procedures. A web survey will be conducted to gather information on CIS violations from network administrators and end users. Companies and professional organizations will be approached for participation in the survey. The companies will be recruited with the help of Professor Veeramani, director of the UW E-Business Institute; the professional organizations will be approached with the help of Sami Saydjari, president of the Cyber Defense Agency (CDA). We will target companies in a variety of industries in order to achieve external validity of our results. Those companies will help us recruit their employees for the end user survey; the professional organizations will help us recruit their members for the network administrator survey.

We used the PASS 2000 (Power Analysis and Sample Size) software in order to determine the sample size. A power of .80 and an alpha value of .05 were used in the analyses. In order to detect a correlation of .30 (e.g., between the presence of a CIS violation and the presence of a contributing factor), we need a sample size of 160 participants. Given a response rate of 60%, we should recruit 260 network administrators and 260 end users.

Data analysis. The survey data analysis will consist of the following steps:

1. data cleaning and verification
2. descriptive statistics on demographics and background information
3. descriptive statistics on CIS violations and factors contributing to CIS violations

4. correlation analysis between (1) CIS violations and (2) factors contributing to CIS violations. We will first perform a bivariate correlation analysis, and then a canonical correlation analysis to examine the multivariate relation between the two groups of variables.
5. cluster analysis of violations to classify the violations according to the reasons given for their occurrence. A cluster analysis similar to the one performed by Lawton (1998) will be done.

An additional data analysis step may be necessary to reduce the number of variables (depending on the number of CIS violations and contributing factors that emerge from the previous step of the research). If necessary, factor analysis will be conducted to identify underlying constructs.

Data analysis will be performed separately for the network administrators and the end users. In addition, the questions that are similar for both groups (end users and network administrators) will be analyzed simultaneously and compared between the two groups. This comparative analysis will produce information useful to identify the factors specific to each group. For instance, high workload and poor prioritization of tasks may be important contributors to CIS violations by network administrators, but not by end users. Therefore, a strategy for preventing CIS violations by network administrators may focus on improving their workload and workload management.

Focus groups – Identification of solutions for CIS violations

The survey data will be presented to two groups of CIS managers and experts. The focus of the discussion will be on solutions for preventing CIS violations or reducing the impact of CIS violations.

Study procedures. CIS managers and experts who participated in the first set of focus groups will be asked to participate in a second focus group. The procedure used in the first set of focus groups will be applied in this second set of focus groups. At the beginning of the focus group, a summary of the survey data will be presented. The discussion in the focus groups will be organized around the following questions:

- What are possible solutions for preventing CIS violations?
- What are possible solutions that would mitigate the consequences of CIS violations?
- What are the barriers to implementing those solutions? How can those barriers be overcome?

The discussion in the focus groups will be closely connected to the findings of our research; emphasis will be put on solutions that deal with the causes of CIS violations identified in the previous steps of the research.

Data analysis. The data analysis will be organized to produce a table comprised of rows (CIS violations) and columns (solutions for preventing or mitigate the consequences of CIS violations). The cells in the table will indicate the relationship between the CIS violations and the solutions: preventing (P) CIS violations or mitigating (M) the consequences of CIS violations. For each solution or group of solutions, a list of barriers and methods for overcoming the barriers will be defined.

Timeline

ACTIVITIES	**YEAR 1**				**YEAR 2**			
Focus groups – Identifying CIS violations and their consequences								
Focus group with network administrators	X							
Focus group with CIS managers	X							
Focus group with CIS experts	X							
Data analysis		X						
List of CIS violations and their consequences		X						
Interviews – Identification of factors contributing to CIS violations								
Interviews with network administrators			X	X				
Interviews with end users			X	X				
Data analysis					X			
Create draft survey					X			
Survey of network administrators and end users								
Pilot testing of survey					X			
Web survey of network administrators						X		
Web survey of end users						X		
Data analysis							X	
Focus groups – Identification of solutions for CIS violations								
Focus group with CIS managers							X	
Focus group with CIS experts							X	
Data analysis								X
Dissemination								
Workshop for companies		X	X	X	X	X		
Presentation at conferences				X				X
Reports				X				X
Research meetings	X			X		X		X

Broader Impacts

The proposed project will involve the participation of students in the research process. This will promote their development of analytical training and learning, including the acquisition of valuable skills such as learning statistical software, conducting literature search (information literacy) and project management. In addition, because of the inter-disciplinary nature of the proposed research, students will be exposed to various disciplines (i.e. industrial and systems engineering-ISyE, human factors engineering, computer sciences and computer security). Students will have the unique opportunity to learn about and experience inter-disciplinary research. Before the semester starts, an email announcement will be sent to undergraduate students in the ISyE department to participate in the research project: the students will be able to take 3 credits to count toward the ISyE technical elective requirement.

As a female faculty in engineering, the PI plays a major role in encouraging traditionally underrepresented groups to enroll in graduate education in engineering. Every effort will be made to recruit women and underrepresented minority students to work on this project. In the ISyE department at the University of Wisconsin-Madison, the graduate student population is about 33% female and 2% black and Hispanic. The College of Engineering of the University of Wisconsin-Madison has systems and programs in place that can help the PI recruit women and underrepresented minority students (GERS fellowships for underrepresented graduate students; SURE program that allows underrepresented undergraduate students to work on a research project during the summer). The PI has an excellent track record in advising women and minority graduate students. Eight students have completed their PhD under the supervision of the PI: 7 were women and two of the women were African-American. Currently, the PI advises 3 Ph.D. students (2 of them are women), and 2 MS students (1 woman, 1 man). In the fall'2006, an American Indian woman will begin a Ph.D. in ISyE with the PI.

Several links between the research and teaching activities will be organized, in particular with the following ISyE courses taught by the PI and the co-PI: ISyE549-Human Factors Engineering (optional course with yearly enrollment of about 30 students), ISyE653-Job Design (junior design course with yearly enrollment of 40-60 students), ISyE671-E-Business: Technologies, Strategies and Applications (optional course with yearly enrollment of about 30 students) and ISyE672-E-Business Transformation: Design, Analysis and Justification (optional course with yearly enrollment of about 30 students). Data from the proposed research will be used as examples in those courses; for instance, examples of CIS violations and the role of organizational factors as contributing to CIS violations will be used when discussing job design theories in ISyE653. The results of this research will also be shared with a group of computer security researchers at the University of Wisconsin-Madison; this group has a group email address that reaches out to all researchers and staff interested in computer security. The group meets on a regular basis to discuss computer security research. We will also create a website for the project that will be used to disseminate findings of our research.

To actively promote the discoveries associated with this research effort and to address educational activities, we propose to offer a workshop to companies. The workshop will be team-taught by the PI (Carayon), and the post-doctoral fellow (Kraemer). The workshop will be designed at the beginning of the second year of the project, and will be offered during the summer at the end of the second year of the project. The objective of the workshop is to provide information on human factors in CIS to companies. Sami Saydjari, president of the Cyber Defense Agency, will be invited as a speaker at the workshop. The workshop will be organized in cooperation with Professor Veeramani and the E-Business Institute of the University of Wisconsin-Madison. We also plan to offer a mini-tutorial on our research at an appropriate conference, such as the International Human-Computer Interaction conference or the SIGCHI conference.

The following table describes our publication plan.

Table 2 – Publication plan

Title	Authors* (lead author in CAPS)	Where?	When?
Model of CIS violations (based on this proposal)	CARAYON, Hoonakker, Kraemer, Saydjari	Computers & Security	To be submitted by middle of Year 1
CIS violations and their impact on CIS (results of first set of focus groups)	KRAEMER, Carayon, Hoonakker, Saydjari, Veeramani	Information Systems Journal or Information Management & Computer Security or IBM Systems Journal	To be submitted by end of Year 1
CIS violations and contributing factors (results from interviews)	KRAEMER, Carayon, Hoonakker, Saydjari	Applied Ergonomics or Human Factors or Safety Science	By end of Year 1

CIS policies from the viewpoint of computer security experts and practitioners (using data from focus groups and interviews)	SAYDJARI, Carayon, Kraemer, Hoonakker	IEEE Security and Privacy Journal	By end of Year 1
Development of a survey on CIS violations	CARAYON, Kraemer, Hoonakker	Annual Conference of the Human Factors and Ergonomics Society	At the beginning of Year 2
How network administrators and end users compromise CIS?	KRAEMER, Carayon, Hoonakker, Saydjari, Veeramani	USENIX Security Symposium	At the beginning of Year 2
CIS violations by network administrators and end users (results of survey)	HOONAKKER, Kraemer, Carayon, Saydjari, Veeramani	Communications of the ACM	At the end of Year 2
Preventing CIS violations (results of the second set of focus groups)	CARAYON, Kraemer, Hoonakker, Saydjari, Veeramani	Computers & Security	At the end of Year 2
What can companies do to improve the design and implementation of CIS policies?	VEERAMANI, Carayon, Kraemer	Infosecurity Today or Computers & Security	At the end of Year 2

* The authors will also include graduate and undergraduate students who participate in the research project.

NSF Prior Support

Paths to Retention and Turnover in the IT Workforce: Understanding the Relationships Between Gender, Minority Status, Job and Organizational Factors NSF Grant #EIA-0120092 (PI: P. Carayon) [2001-2004]

The aims of this study were to identify: (1) what job, organizational and quality of working life (QWL) factors influence turnover intention within the current IT workforce and (2) in what way gender and minority status play a role in the relationships between job and organizational factors, QWL and intention to turnover. The study included four activities: (1) a pilot study and pre-test to develop and test a survey instrument, (2) a web survey to collect data on job, organizational, QWL factors and turnover intention, (3) secondary analysis of a database to examine differences between men and women in IT and non-IT jobs, and (4) a range of dissemination activities. The results of the pilot study are reported in a paper to be published in Behaviour and Information Technology ("Evaluating causes and consequences of turnover intention among IT users: The development of a questionnaire survey"). A total of 814 IT workers from five companies and an organization for female scientists and engineers working in the ITWF participated in the main web survey (response rate: 56%). Our results show very little differences between men and women, and majority and minority IT workers with regard to QWL and intention to turnover. On the other hand, we found differences between men and women regarding the job and organizational factors that affect QWL and turnover intention. For instance, supervisory support is an important predictor of turnover intention among female IT workers, but not among male IT workers. A total of 24 publications have been written on this project: 15 papers published in conference proceedings, 5 book chapters, 2 journal articles (one to be published, one submitted) and 2 reports. We will soon submit one article to MIS-Quarterly and one article to Communications of the ACM. A total of 5 graduate students participated in this project: one Hispanic woman, one Hispanic man, two white women and one white man.

REFERENCES

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 23*, 253-264.

Carayon, P., & Smith, M. J. (2000). Work organization and ergonomics. *Applied Ergonomics, 31*, 649-662.

Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin, 51*(4), 327-358.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *CSI/FBI Computer Crime and Security Survey*: Computer Security Institute.

Hobbs, A., & Williamson, A. (2002). Unsafe acts and unsafe outcomes in aircraft maintenance. *Ergonomics, 45*(12), 866-882.

Kraemer, S., Carayon, C., & Clem, J. F. (2006). Characterizing violations in computer and information security systems. In *Proceedings of the 16th Triennial Congress of the International Ergonomics Association*. Maastricht, the Netherlands.

Kraemer, S., & Carayon, P. (2003). A human factors vulnerability evaluation method for computer and information security. In The Human Factors and Ergonomics Society (Ed.), *Proceedings of the Human Factors and Ergonomics Society 47th Annual Meeting*. Santa Monica, CA: The Human Factors and Ergonomics Society.

Kraemer, S., & Carayon, P. (2005). Computer and information security culture: Findings from two studies. In The Human Factors and Ergonomics Society (Ed.), *Proceedings of the Annual Meeting of the Human Factors and Ergonomics Society*. Santa Monica, CA: The Human Factors and Ergonomics Society.

Kraemer, S., & Carayon, P. (2006). A human factors model of human error in computer and information security. *Applied Ergonomics, accepted with revision*.

Kraemer, S., & Carayon, P. (forthcoming). A human factors model of human error and violations in computer and information security. *Applied Ergonomics*.

Kraemer, S., Carayon, P., & Duggan, R. (2004). Red team performance for improved computer and information security. In The Human Factors and Ergonomics Society (Ed.), *Proceedings of the Annual Meeting of the Human Factors and Ergonomics Society* (pp. 1605-1609). Santa Monica, CA: The Human Factors and Ergonomics Society.

Lawton, R. (1998). Not working to rule: Understanding procedural violations at work. *Safety Science, 28*, 77-95.

Markoff, J., & Bergman, L. (2005, May 10). Intruder Attack on Computer Net is Called Broad*. The New York Times*.

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception-Controlling the Human Element of Security*. Indianapolis, IA: Wiley Publishing.

Parker, D., & Lawton, R. (2000). Judging the use of clinical protocols by fellow professionals. *Social Science & Medicine, 51*, 669-677.

Parker, D., Reason, J., Manstead, A. R., & Stradling, S. G. (1995). Driving errors, driving violations and accident involvement. *Ergonomics, 38*(5), 1036-1048.

Rasmussen, J. (1982). Human errors: A taxonomy for describing human malfunction in industrial installations. *Journal of Occupational Accidents, 4*, 311-333.

Reason, J. (1990). *Human Error*: New York: Cambridge University Press.

Reason, J. (2004). Beyond the organisational accident: The need for "error wisdom" on the frontline. *Quality and Safety in Health Care, 13*(Suppl II), ii28-ii33.

Reason, J., Manstead, A., Stradling, S., Baxter, J., & Campbell, K. (1990). Errors and violations on the roads: A real distinction? *Ergonomics, 33*(10/11), 1315-1332.

Reason, J., Parker, D., & Free, R. (1994). *Bending the Rules: The Varieties, Origins and Management of Safety Violations*. Leiden: Faculty of Social Sciences, University of Leiden.

Reason, J., Parker, D., & Lawton, R. (1998). Organizational controls and safety: The varieties of rule-related behavior. *Journal of Occupational and Organizational Psychology, 71*, 289-304.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, Inc.

Smith, M. J., & Carayon-Sainfort, P. (1989). A balance theory of job design for stress reduction. *International Journal of Industrial Ergonomics, 4*, 67-79.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jeffery, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*, 124-133.

Taylor, L. (2004). Vulnerabilities and threats 101. *Intranet Journal*.

The Mitre Corporation. (2006). *Common Vulnerabilities and Exposures*. Retrieved 02/11/2006, from http://cve.mitre.org