available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Human and organizational factors in computer and information security: Pathways to vulnerabilities

Sara Kraemer[a,*], *Pascale Carayon*[b,1], *John Clem*[c,2]

[a] *Wisconsin Center for Education Research, University of Wisconsin-Madison, 1025 West Johnson Street, Madison, WI 53706, USA*
[b] *Center for Quality and Productivity Improvement, Department of Industrial and Systems Engineering, University of Wisconsin-Madison, 3126 Engineering Centers Building, 1515 Engineering Drive, Madison, WI 53706-1609, USA*
[c] *Information Design Assurance Red Team, Sandia National Laboratories, P.O. Box 5800, MS 0671, Albuquerque, NM 87185-0671, USA*

ARTICLE INFO

Article history:
Received 6 May 2008
Received in revised form
1 April 2009
Accepted 28 April 2009

Keywords:
Computer security
Red teams
Human and organizational factors
Design
Pathways
Vulnerabilities
Causal Network Analysis

ABSTRACT

The purpose of this study was to identify and describe how human and organizational factors may be related to technical computer and information security (CIS) vulnerabilities. A qualitative study of CIS experts was performed, which consisted of 2, 5-member focus groups sessions. The participants in the focus groups each produced a causal network analysis of human and organizational factors pathways to types of CIS vulnerabilities. Findings suggested that human and organizational factors play a significant role in the development of CIS vulnerabilities and emphasized the relationship complexities among human and organizational factors. The factors were categorized into 9 areas: external influences, human error, management, organization, performance and resource management, policy issues, technology, and training. Security practitioners and management should be aware of the multifarious roles of human and organizational factors and CIS vulnerabilities and that CIS vulnerabilities are not the sole result of a technological problem or programming mistake. The design and management of CIS systems need an integrative, multi-layered approach to improve CIS performance (suggestions for analysis provided).

1. Introduction

There is a high incidence of computer and information security vulnerabilities and its associated problems have costly ramifications. The 2008 Computer Security Institute/Federal Bureau of Investigation reports survey data from 522 computer security practitioners and senior executives from U.S. corporations, government agencies, financial institutions, medical institutions and universities (Richardson, 2008). The average loss per respondent was $288,618, caused by various types of computer security incidents. The survey also reported the vulnerability and attack trends within a 12-month time period, including: (1) 59% experienced an attack involving a virus, (2) 29% of organizations reported unauthorized use of computer systems, and (3) 44% reported insider abuse.

One of the largest problems in computer and information security (CIS) is the effective remediation of vulnerabilities and damages from attacks; however, organizations emphasize a technological approach to protect their assets (Besnard and Arief, 2004). Computer and information security has focused mainly on technological solutions to prevent vulnerabilities

[*] *Corresponding author*. Tel.: +1 608 265 5624; fax: +1 608 263 6448.
E-mail addresses: sbkraeme@wisc.edu (S. Kraemer), carayon@engr.wisc.edu (P. Carayon), jfclem@sandia.gov (J. Clem).
[1] Tel.: +1 608 263 2520; fax: +1 608 263 1425.
[2] Tel.: +1 505 844 9016.

0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.04.006

and attacks and have not yet fully adopted a sociotechnical approach that addresses human and organizational aspects of CIS (Dhillon and Backhouse, 2001). Human and organizational aspects have been found to be important in the effectiveness of other critical systems, such as safety and accident mitigation (Rasmussen, 1994; Reason, 1997).

This paper focuses mainly on human and organizational factors within the CIS system, but also acknowledges that technological factors are interlinked with these conceptualizations. Regardless of the strength of technical controls, if human and organizational factors affect their implementation and use, the effect on security can be severe (Bishop, 2002). In this regard, vulnerable computer and information security protection (e.g., weak passwords or poor usability) and malicious intentions may set the stage for computer and information security vulnerabilities. Vulnerabilities may be attributed to the outcomes of flawed organizational policies and individual practices whose origins are deeply rooted within early design assumptions or managerial decisions (Besnard and Arief, 2004).

1.1. *Research approach, questions, and paper overview*

This research utilized a macroergonomic approach to conceptualize CIS as a sociotechnical system (Hendrick and Kleiner, 2001). A macroergonomic approach considers both human and organizational factors of a sociotechnical system and refers to the design of the culture and structure of an organization, including the design of departmental boundaries, reward systems, supervisory and control systems, job design principles, performance expectations, employee involvement opportunities, labor or management contracts, and the social contract between the organization and its members (Pasmore, 1988). A macroergonomic approach was a qualified conceptual basis for this paper because it not only emphasizes the interactions of factors at various levels of CIS systems, but acknowledges contextual impact of specific types of settings on those interactions.

This paper aims to describe some of the human and organizational factors that contribute to CIS vulnerabilities and the relationships among those factors, from a macroergonomic perspective (Hendrick and Kleiner, 2001). Focus groups were conducted with red teams about their views of human and organizational factors and relationship to vulnerabilities in CIS systems. The following research questions are examined:

- What are the human and organizational factors that may contribute to CIS vulnerabilities?
- What are the relationships (i.e., pathways) among these factors and how do they contribute to types of CIS vulnerabilities?

This paper is organized into 4 main sections, beginning with a literature overview of human and organizational factors research in CIS from a multidisciplinary perspective. The Methodology section describes the qualitative research design. The study design consisted of 2 focus group sessions with red team members and used causal network analysis to identify and describe human and organizational pathways to CIS vulnerabilities. The Results section presents 2 causal network analyses and examples of specific human and organizational pathways to a CIS vulnerability category. The Discussion section integrates the human and organizational factors into 9 thematic categories: external influences, human error, management, performance management, resource management, policy issues, technology, and training. Limitations and future research are also discussed.

2. Literature overview of human and organizational factors in computer and information security

The role of human and organizational factors in CIS has been examined from a range of disciplinary perspectives. This list includes, though it is not exhaustive, research from the areas of cognitive engineering, computer science, human factors engineering, information systems, macroergonomics, management sciences, and systems dynamics. While these research tracks have examined various facets of human and organizational factors in CIS, researchers have called for more examination in these areas (Dhillon and Backhouse, 2001; Furnell, 2007; Schultz, 2005; Cresswell and Hassan, 2007). This overview will summarize some of the research across these disciplines.

Usability and users' role in CIS has been a substantial stream in this research, with a particular emphasis on usability of specific CIS methods, such as smart cards and biometric devices (Proctor et al., 2000), PGP 5.0 encryption software (Whitten and Tygar, 1998, 1999), and passwords (Adams and Sasse, 1999; Adams et al., 1997). Other usability studies have also included web browsers' basic security and identification indicators (Herzberg, 2009) and an analysis of desktop applications such as Word 2007 and Internet Explorer 7 (Furnell, 2007). This literature has identified a range of discrete interactions between users and specific CIS technologies, but has not examined how other influences, such as environmental or organizational considerations like time pressure or workload, can affect the performance of both the user and the CIS technology.

Another stream of research has examined users' perceptions and behaviors related to CIS. Stanton et al. (2005) conducted a survey study of 1167 end users in the financial, manufacturing, health, military, government, and telecommunications sectors on password-related behaviors as well as training and organizational awareness. They found significant correlations between good password-related behaviors and training and awareness. Albrechtsen (2007) conducted an interview study to explain users' experiences of information security by organizational factors. The study reported, among other findings, that organizational factors such as high workload create a conflict of interest between functionality and information security. Studies of security managers' and network administrators' perceptions of human and organizational factors have complemented these findings; these studies found that, among other factors, tasks and high workload were associated with weakened system states, human error, and overall system performance (Kraemer et al., 2006; Kraemer and Carayon, 2007).

Organizational factors in CIS research have included policies, culture, and management support. Studies involving policies have examined various dimensions, such as the effective uptake and dissemination of CIS policies (Fulford and Doherty, 2003), employees' behavior toward security compliance (Pahnila et al., 2007), and the importance of policy management and organizational procedures on the application and adoption of CIS policies (Karyda et al., 2005).

Culture in security systems has been found to be multidimensional, as well, including security governance, control, coordination, sound security processes (Ruighaver et al., 2007), top management support (Knapp et al., 2006), employee participation and training (Kraemer and Carayon, 2005), and employee awareness of security (Siponen, 2000). Other research have examined the interplay of human and organizational factors in CIS (Werlinger et al., 2009). Their analysis produced an integrated framework of human, organizational, and technological challenges associated with security management and emphasized the interplay among the various factors in the CIS system. The study found that in order to effectively address the range of CIS problems an approach that simultaneously addresses the factors is necessary. The stream of research in organizational factors have emphasized that effective CIS is indeed multi-dimensional and affects many facets of the CIS system. However, these areas of research have not yet explicitly linked factors to specific performance metrics, such as specific vulnerabilities or vulnerability types. In our current approach, we aimed to identify some potential interactions and pathways among factors that may have both indirect and direct effects on various vulnerability types.

Systems dynamics research has developed some models of human and organizational factors in CIS systems via causal loop diagramming, from the perspective of security managers (Sarriegi et al., 2005, 2006). In particular, these studies have explored security management from a dynamic and complex perspective, showing that the complex nature of these systems requires a modeling process capable of displaying the multifarious relationships among factors. Factors such as security management, culture, and lack of employee involvement, among others, were described as contributing to weakened security performance. This research used a similar approach to our study, but did not include an analysis of other organizational factors, such as lack of funding for CIS, inadequate staffing, lack of CIS policies and evaluation, among others identified in this current research, nor did it identify how human and organizational factors may impact CIS vulnerabilities.

This literature review has identified a range of human and organizational factors that may contribute to the performance of CIS systems. However, there are at least 2 areas yet to be fully addressed in the literature. The conceptualization of human and organizational factors in CIS and how they contribute to vulnerabilities is underdeveloped. There is also an underspecified knowledge base of the specific mechanisms and pathways of factors that may impact specific types of CIS system performance metrics. The contributions of this current research were to expand and refine the definitions of human and organizational factors in CIS, describe the nature of their relationships and mechanisms, and identify how they may affect the performance of CIS systems (*vis-à-vis* the impact on vulnerability categories).

3. Methodology

This study consisted of a qualitative research design. Qualitative techniques are often useful for gathering rich, detailed explanations of complex, intricate phenomena in order to reveal their context (Trochim, 2001).

3.1. *Sample*

Red teams were identified as a source of information to develop pathways of human and organizational factors to vulnerability categories. Red teaming is an advanced form of assessment used to identify weaknesses in a variety of CIS systems by simulating adversaries such as hackers. Red teams attacks and correction of system defects are beneficial for organizations' CIS systems in general (Computer Science and Telecommunications Board, 2002). The use of red teams is a mechanism for detecting system vulnerabilities and enhancing security. Red teams provide adversaries' perspectives of system weaknesses to CIS system defenders (Schudel and Wood, 2000).

This study conducted in collaboration with the Information Design Assurance Red Team™ (IDART™) program at Sandia National Laboratories in Albuquerque, New Mexico. The IDART program was identified as a qualified research partner for several reasons. The program has performed multiple types of critical assessments for a variety of organizations since its inception in 1997, including: targeted assessments for customers from the private sector, ranging from banking and finance, information technology, manufacturing and e-commerce, as well as the public sector, including the U.S. Departments of Defense, Energy, Interior, Homeland Security, and State. Their views of CIS systems are diverse and comprehensive, given the number and variety of assessments performed.

The IDART program differs from other red team programs in several ways. Their enterprise technology assessments generally employ both a system-of-systems approach and consider the system lifecycle. Many, if not most, red teams assess a system from within the constraints of 1 or 2 phases of the system lifecycle and do not employ a formal process to understand system-of-systems impacts. The red team program exists in a multi-program national security laboratory and it routinely assembles multi-disciplinary teams to assess complex and specialty systems, as opposed to teams that concentrate in a single domain or technology. Multiple red teaming approaches to red teaming in order to serve many customers that have different security concerns, while many red teams (e.g., some military red teams) have a single customer, a single environment in which they operate, and/or a single process that they follow. Besides performing assessments, red team members also work to refine, improve, and develop new methodologies, tools, and analysis techniques. Compared to other red teams, IDART spends more time on causal analyses of CIS vulnerabilities while other teams may concentrate more on reporting assessment results (e.g., number of rogue access points, number of unpatched systems). In sum, the IDART team frequently performs assessments from a systems viewpoint across the system lifecycle.

IDART has developed a formal methodology of assessment (Wood and Duggan, 1999). The program consists of core red

Table 1 – Sample characteristics.

Categories	Focus group 1 ($n = 5$)	Focus group 2 ($n = 5$)
Age/years: mean (range)	39.8 (26–51)	30.8 (26–49)
Gender	5 Males	4 Males, 1 Female
Experience/years: mean (range)	6.4 (2–14)	7.2 (3–14)
Member role	2 project leaders, 3 core members	2 project leaders, 3 core members
Summary of background	Computer science; information technology; system engineering, product support, system and network administration, networking, network security, Cisco systems, global enterprise networks and applications, programming, computer security design, implementation, operating, and testing	Computer science, nuclear weapons and materials research, distributed applications, UNIX systems, satellite sensor testing, process control systems, business administration, management, programming, quality assurance engineering, wireless security, intrusion detection, network security design, electrical engineering, red team experience outside of IDART™

team members, non-core red team members, and matrix members. Core red team members are system analysts who regularly participated in red team projects and whose full-time job is within the program. Non-core members are system analysts, who semi-regularly participated in red team projects and are not members of the program. Matrix members are analysts with specialized expertise and participated in projects that assessed specific systems. For example, a red team examination of biological and chemical agent detection system includes experts on biological and chemical warfare agents.

The sample consisted of 10 red team members. Two focus groups were conducted; each group consisted of 5 core red team members. A focus group of at most 6 people has been determined to be an appropriate number to gather detailed, rich information while still reaping the benefits of a group dynamics (Morgan, 1988; Stewart and Shamdasani, 1990). Furthermore, assessment project teams typically consist of 5 red team members.

While the sample was exclusively from a single red team program, a wide range of experiences and backgrounds were represented in the sample (Table 1). Each group consisted of 2 red team project leaders and 3 core red team members. Red team project leaders were core red team members who usually led team projects and were the most experienced members (i.e., 5–10 years of red teaming experience). The sample represented a diverse background and knowledge base in many areas of CIS and information technology. They also had experience in CIS related work and tasks as well as management experience. Lastly, the red team members had formal training in the fields of computer science, information technology, systems engineering, and electrical engineering.

3.2. Data collection

A relationship diagramming method was used to document and summarize possible pathway relationships among human and organizational factors and CIS vulnerabilities. The relationship diagram method consisted of arrows to show the possible cause-and-effect relationships among factors that influence problems (Mizuno, 1988). The relationship diagram method was chosen as a data collection tool for several reasons. The relationship diagram method simplified complicated problems into several major points, enabled issues to be examined from a broad perspective. Used in conjunction with the focus group technique, the relationship diagram method was used to capture and revise participants' ideas. However, since the relationship diagram method was unrestricted, the relationship diagrams differed between groups.

Each focus group session followed a data collection protocol. The red team members were presented with the open-ended question: "How are human and organizational factors related to CIS vulnerabilities?" and a set of probes that explored the nature of the factors and CIS vulnerabilities (see Appendix). Each session was 4 hours in length and took place in a private conference room at Sandia National Laboratories. The focus group discussions were audio-recorded and transcribed by a professional transcription service.

The participants developed their knowledge of the study's approach and constructs prior to the focus group sessions. Individual interviews were conducted with red team members prior to the sessions. The purpose of these interviews was to identify and describe human and organizational factors and CIS in general. During individual interviews, the red team members became familiar with terminology and concepts. The first author moderated the focus group sessions and conducted the individual interviews.

The beginning of each session was dedicated to summary review of the individual interviews. The moderator created several large posters that summarized the human and organizational factors identified in the individual interviews. The posters served as a primer for the brainstorming sessions. The red team members were tasked to generate a relationship diagram documenting the various human and organizational factors in CIS and their possible relationships to design, implementation, and configuration vulnerabilities (Howard and Longstaff, 1998; Howard and Meunier, 2002).

The relationship diagram process was used in conjunction with causal network analysis (Miles and Huberman, 1994). The causal network consisted of a relationship diagram of the most important independent factors (i.e., human and organizational factors) and dependent factors (i.e., CIS vulnerabilities) shown in boxes and of the relationships among them, depicted by arrows. The causal network technique was inductive, not an *a priori* framework. The plot of these relationships was directional and did not imply correlation. It was assumed that some factors exert an influence on others: Factor X brings Factor Y into being or makes Factor Y larger or smaller.

The causal network had associated analytic text (focus group discussions) that described the meaning of the factors and built a logical chain of evidence. A line was drawn between pairs of factors that may co-vary (factors appear consistently in the case) and may have some kind of relationship (more of 1 factor goes with less of another). A directional arrow was drawn between each factor that came first temporally and later factors that it appeared to influence. Influence meant that more or less of 1 factor determined the existence of another; the second factor might have been different had the first not been present. Meaning, a "mechanism" between the 2 factors may be involved.

After introducing the causal network technique, the red team members were given a stack of Post-it$_{(R)}$ notes and markers to write down various human and organizational factors. The red team members placed the Post-it notes on several large pieces of poster paper on the wall. On the right side of the poster paper were the categories of CIS vulnerabilities: design, implementation, and configuration. The red team members placed the Post-it notes on the paper and drew lines and arrows that indicated possible relationships among human and organizational factors and CIS vulnerabilities. Within an unbroken pathway, multiple channels usually led in different directions or arrived at the same place via a different route.

The focus group process used in this study was similar to IDART brainstorm process for creating system views and attack graphs for projects; however, the results were not interpreted as conclusive for several reasons. When red team members typically conduct brainstorming sessions, the red teams spend filter the graphs in multiple ways and assess the results on numerous criteria. In this sense, the results did not produce attack graphs. Rather, they composed scenarios of how vulnerabilities might be created in CIS systems from human and organizational factors. Also, the red team did not have multiple evaluations (post focus group session), such as a follow-up to the brainstorming session, which they would typically apply to brainstorm results.

Lastly, causal network analyses were the result of 2 focus group sessions that had some advanced preparation, including individual interviews on human and organizational factors in CIS, as well as the access to the study description and focus group guide prior to the focus group sessions. However, when a red team typically conducts a brainstorm session, the core assessment team briefs the team on the system mission, red team mission, and how the system works. In each of the focus group sessions, this information was not created nor provided.

3.3. *Data analysis*

A content analysis was performed on the discussions of each session. The content analysis presumed a defined coding structure to capture the critical content of the data (Ryan and Bernard, 2000). The coding structure consisted of "nodes" that represented each human and organizational factor in casual networks. The transcribed discussions provided the analytic content associated with each node. The first author performed the data analysis on the transcribed discussions, constructed node categories, defined the node structure, analyzed the meaning of responses in relation to the node structure, and placed passages of text in the node structure. QSR NVivo©, a qualitative software package, was used to code the content of the session.

The focus group discussions were analyzed separately; there was no cross-coding between group discussions. The first progression of thematic content analysis of the discussion was exhaustive. The second and third progressions of analysis were more selective and combed prior analyses for redundancies and over-differentiation.

A preliminary report of study findings was reviewed by 2 red team project leaders. The preliminary report consisted of a summary of the causal networks and description of each pathway leading to CIS vulnerabilities. The project leaders evaluated the causal network and human and organizational factors definitions for accuracy and precision. Overall, the 2 red team members created a total of 36 editorial comments. Of the 36 comments, 22 comments were related to rephrasing and clarification. The remaining 14 comments expanded the discussions on the relationships and definitions of human and organizational factors. The comments did not change the content or meaning of the causal networks. Rather, the reviewers' comments enriched the discussions with clarified examples and detailed definitions of human and organizational factors.

4. Results

In summary, the focus group participants identified a total of 66 human and organizational factors (21 human and organizational factors in focus group 1, 45 factors in focus group 2). The focus group participants identified a total of 50 pathways (37 pathways in focus group 1, 13 pathways in focus group 2).

The causal network analysis depicted various human and organizational factors pathways leading to CIS vulnerabilities: design, implementation, and configuration (Howard and Longstaff, 1998; Howard and Meunier, 2002). The participants of the first focus group determined that operational vulnerabilities was a fourth category in the vulnerability taxonomy. An operational vulnerability occurred when an process was undefined, missed, or performed out of order, and may have resulted in a security-related failure of the CIS system. The participants of the second focus group also determined that the operational vulnerability category was relevant to their analysis and added it to the taxonomy of CIS vulnerabilities.

4.1. *Focus group 1*

A total of 37 pathways that lead to various types of vulnerability categories and 93 relationships (i.e., the total number of connections between 2 factors) were identified. These included: 9 pathways to design vulnerabilities, 10 pathways to implementation vulnerabilities, 10 pathways to configuration vulnerabilities, and 8 pathways to operational vulnerabilities. See Fig. 1 for the causal network analysis of human and organizational factors and vulnerability categories.

4.1.1. *Examples of pathways*

This example represents 1 of the design vulnerability pathways depicted in causal network analysis. It represents a pathway to a design vulnerability (see Fig. 2). The description below is drawn from the content analysis performed on the participants' discussions in Focus group 1.

The type of data or project (1) drove the type of assets or information that is protected (e.g., high or low criticality), how much management supports CIS (2) and views its importance. The data or project type may have also been related to how much funding (4) was allocated to the CIS protection of those assets. Management support was also related to how security policies are developed. For example, low management support may have resulted in poorly specified CIS policy requirements (3). Funding availability (4) affected CIS staffing levels (5). The scheduling problems that emerged for CIS staff was also constrained by an overload of CIS policies (8), and the CIS system's interrelatedness to various system complexities (12). Complexity (12) referred to the intricacies of merging systems and was affected by the usability of CIS technologies (15). Inadequate staffing (5) and lack of CIS-related expertise of staff (10) may be related to biases for certain IT or CIS services, products, and technologies (9). These services, products, and technologies may be less secure than other products or services compared to the capabilities or features of other CIS technologies (15) and these products or services may not have adequate vendor support (16), such as not fixing bugs or providing proper documentation for technology features (13). A lack of CIS developer and staff expertise (10) directly affected the quality of requirement definition of the system (14). Poor or incorrect quality requirement definitions may lead to design vulnerabilities.

A second pathway example from this causal network analysis is 1 that affects both implementation and configuration vulnerabilities (see Fig. 3).

Refer to the previous design vulnerability pathway for a description of factors 1–5, 7–11, 13, 15, and 17. Vulnerabilities may have occurred when CIS systems and processes are not tested for functionality or vulnerabilities (20). Implementation vulnerabilities and configuration vulnerabilities may have been the result of testing that was not performed correctly or performed at all.

4.2. *Focus group 2*

A total of 9 pathways leading various types of vulnerability categories were reported in Focus group 2, which included: 2 design vulnerability pathways, 3 implementation vulnerability pathways, 2 configuration vulnerability pathways, and 2

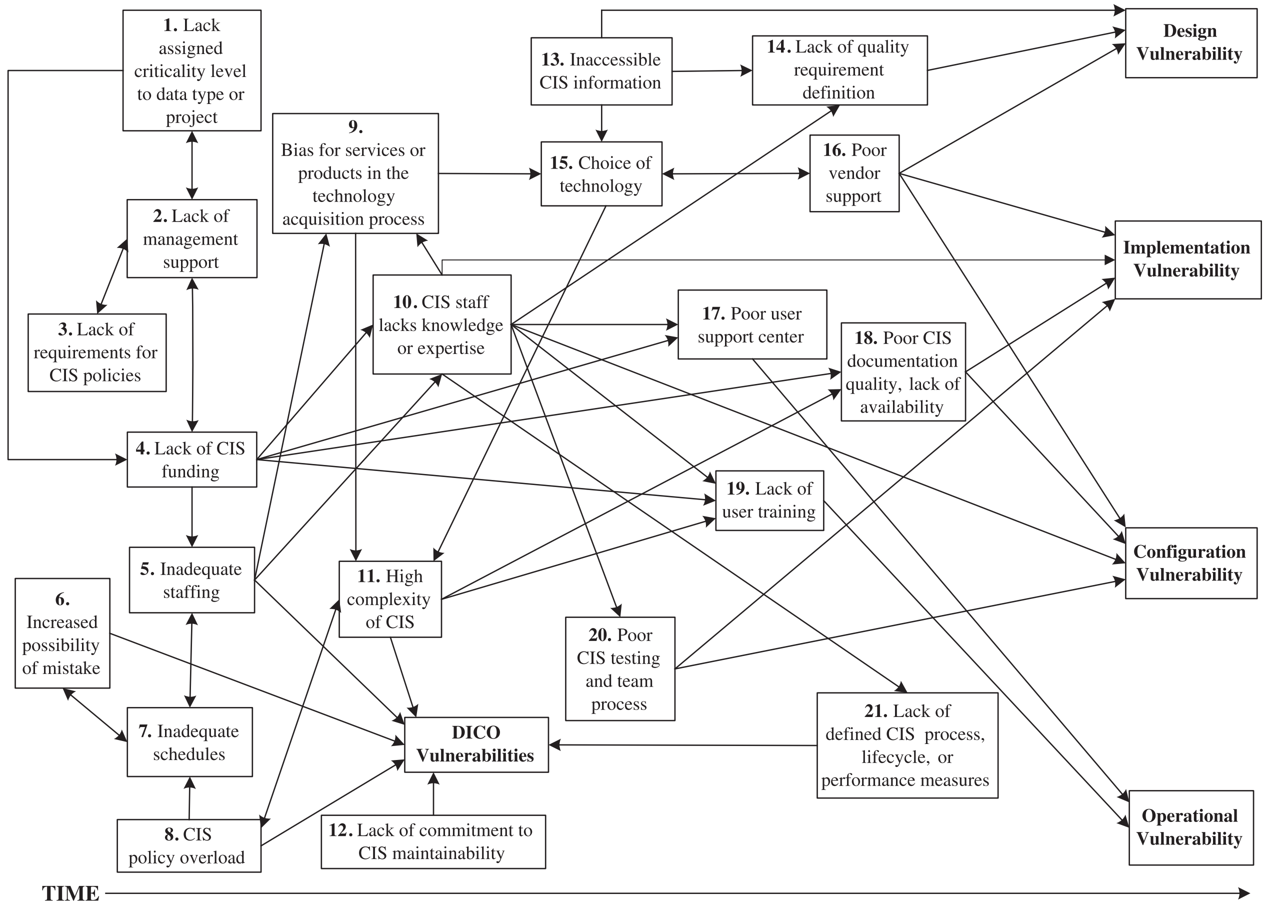
1. Lack assigned criticality level to data type or project
13. Inaccessible CIS information
14. Lack of quality requirement definition
Design Vulnerability
9. Bias for services or products in the technology acquisition process
15. Choice of technology
16. Poor vendor support
2. Lack of management support
Implementation Vulnerability
10. CIS staff lacks knowledge or expertise
17. Poor user support center
3. Lack of requirements for CIS policies
18. Poor CIS documentation quality, lack of availability
4. Lack of CIS funding
19. Lack of user training
5. Inadequate staffing
11. High complexity of CIS
Configuration Vulnerability
6. Increased possibility of mistake
20. Poor CIS testing and team process
7. Inadequate schedules
DICO Vulnerabilities
21. Lack of defined CIS process, lifecycle, or performance measures
8. CIS policy overload
12. Lack of commitment to CIS maintainability
Operational Vulnerability
TIME

Fig. 1 – Causal network analysis, focus group 1.

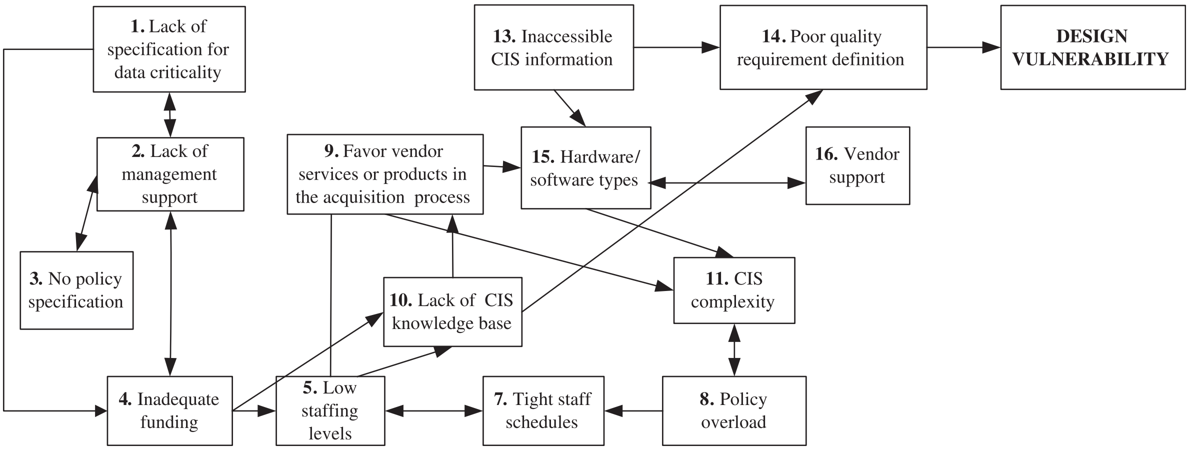
1. Lack of specification for data criticality
2. Lack of management support
3. No policy specification
4. Inadequate funding
5. Low staffing levels
7. Tight staff schedules
8. Policy overload
9. Favor vendor services or products in the acquisition process
10. Lack of CIS knowledge base
11. CIS complexity
13. Inaccessible CIS information
14. Poor quality requirement definition
15. Hardware/ software types
16. Vendor support
DESIGN VULNERABILITY

Fig. 2 – Example (1) of design vulnerability pathway (focus group 1).

operational vulnerability pathways. A total of 45 human and organizational factors were identified with 118 relationships (i.e., the total number of connections between 2 factors). A causal network analysis of human and organizational factors and vulnerability categories is depicted in Fig. 4. Special symbols in this figure represented a directional relationship between 2 factors and were not connected with a line and arrow. These symbols provided a "short-hand" for relationships and limited the number of lines depicted in the flowchart (see Fig. 5 for an example).

4.2.1. *Examples of pathways*

This example represents 1 of the design vulnerability pathways depicted in causal network analysis. It represents a pathway to a design vulnerability (see Fig. 6). The description below is drawn from the content analysis of focus group 2 discussions.

The importance of assets (4), or the assigned criticality of the protected asset, and available resources (e.g., funding, staffing) (5) contributed to creating a strong business case for CIS security (10). Without a strong business case for security, CIS became a low priority, relative to other aspects of the business (9) and management did not support CIS (12). The lack of buy-in and support by the management limited the organizations' ability to hire and retain competent and skilled CIS staff (14). The lack of appropriate staff contributed to the overall lack of time for completing CIS work (15). When changes to the CIS system occurred (e.g., merging a new CIS system or performing system upgrades), it was not done in the context of the overall CIS system (45). This resulted in an overall CIS system design vulnerability.

A second pathway example from this causal network analysis was 1 that affects both implementation and configuration vulnerabilities (see Fig. 7).

The description of factors 4, 5, 9, 10, and 12–15 was the same for the previous design vulnerability example. The implementer of a CIS mechanism or system forgot to implement a service (41), and this error resulted in an implementation vulnerability. This mistake may have been related to the implementer working under time constraints (39), single mechanism protection (40), and/or the lack of management process for the services protection (42).

5. Discussion

This research described numerous human and organizational factors and pathways that may contribute to the presence of

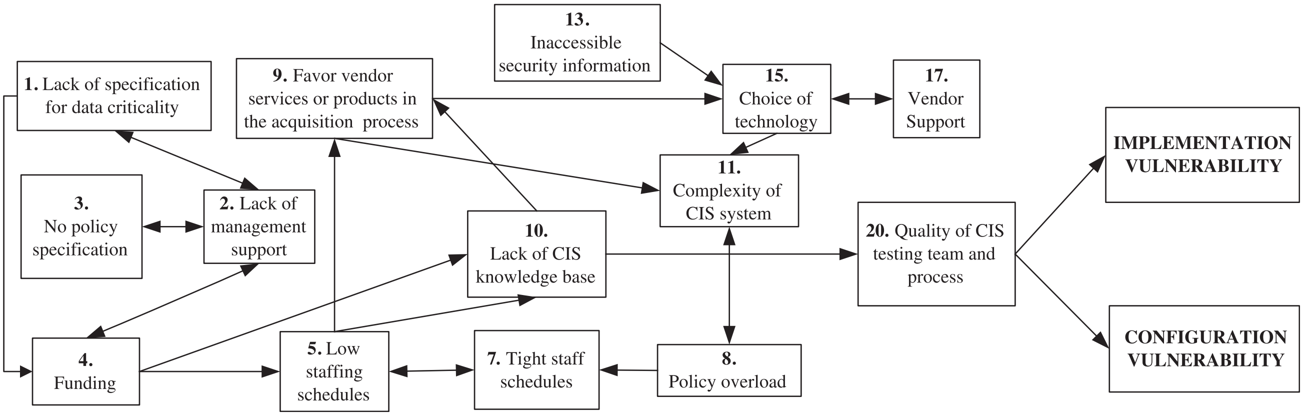
1. Lack of specification for data criticality
9. Favor vendor services or products in the acquisition process
13. Inaccessible security information
15. Choice of technology
17. Vendor Support
3. No policy specification
2. Lack of management support
11. Complexity of CIS system
10. Lack of CIS knowledge base
20. Quality of CIS testing team and process
IMPLEMENTATION VULNERABILITY
CONFIGURATION VULNERABILITY
4. Funding
5. Low staffing schedules
7. Tight staff schedules
8. Policy overload

Fig. 3 – Example (2) of implementation and configuration vulnerability pathways (focus group 1).

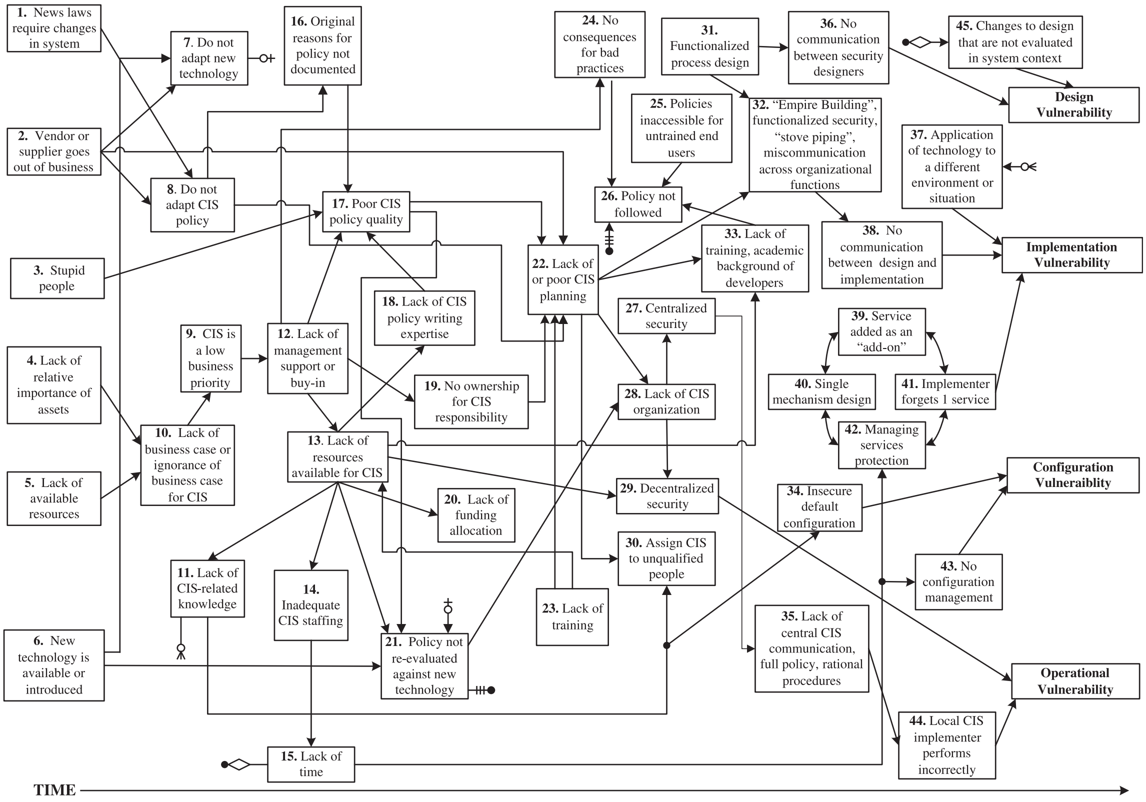
1. News laws require changes in system
2. Vendor or supplier goes out of business
3. Stupid people
4. Lack of relative importance of assets
5. Lack of available resources
6. New technology is available or introduced
7. Do not adapt new technology
8. Do not adapt CIS policy
9. CIS is a low business priority
10. Lack of business case or ignorance of business case for CIS
11. Lack of CIS-related knowledge
12. Lack of management support or buy-in
13. Lack of resources available for CIS
14. Inadequate CIS staffing
15. Lack of time
16. Original reasons for policy not documented
17. Poor CIS policy quality
18. Lack of CIS policy writing expertise
19. No ownership for CIS responsibility
20. Lack of funding allocation
21. Policy not re-evaluated against new technology
22. Lack of or poor CIS planning
23. Lack of training
24. No consequences for bad practices
25. Policies inaccessible for untrained end users
26. Policy not followed
27. Centralized security
28. Lack of CIS organization
29. Decentralized security
30. Assign CIS to unqualified people
31. Functionalized process design
32. "Empire Building", functionalized security, "stove piping", miscommunication across organizational functions
33. Lack of training, academic background of developers
34. Insecure default configuration
35. Lack of central CIS communication, full policy, rational procedures
36. No communication between security designers
37. Application of technology to a different environment or situation
38. No communication between design and implementation
39. Service added as an "add-on"
40. Single mechanism design
41. Implementer forgets 1 service
42. Managing services protection
43. No configuration management
44. Local CIS implementer performs incorrectly
45. Changes to design that are not evaluated in system context
Design Vulnerability
Implementation Vulnerability
Configuration Vulneraiblity
Operational Vulnerability
TIME

Fig. 4 – Causal network analysis, focus group 2.

CIS vulnerabilities. A qualitative study of the views of red team experts was conducted. A causal network analysis technique was used to capture their views of human and organizational factors and possible pathways to 4 types of CIS vulnerabilities: design implementation, configuration, and operational vulnerabilities.

The first focus group identified fewer factors and more pathways than the second focus group (21 factors and 37 pathways in focus group 1, 45 factors and 9 pathways in focus group 2). The number of pathways to vulnerability categories were evenly distributed within focus groups. In focus group 1, there were 9 design vulnerability pathways, 10 implementation vulnerability pathways, 10 configuration vulnerability pathways, and 8 operational vulnerability pathways. In focus group 2, there were 2 design vulnerability pathways, 3 implementation vulnerability pathways, 2 configuration vulnerability pathways, and 2 operational vulnerability pathways. The Limitations Section addresses the focus groups' differences in views.

Nine thematic categories emerged from an integrated summary of the findings: external influences, human error, management, organization of CIS, performance management, policy, resource management, technology, and training (see Table 2).

Human error and mistakes in particular may result in CIS vulnerabilities. Other research on human factors and CIS methods has highlighted the role of usability and good (i.e., error-free) security behaviors. Adams et al. (1997) conducted a web-based questionnaire survey of 139 respondents regarding their password-related behaviors. Infrequently used passwords were associated with more memory problems. Results also demonstrated significant correlations between ''desire to decrease security'' and ''frequent memory problems'', therefore justifying the need to examine human factors and usability of security methods, in order to maintain user support for security measures. Further, Kraemer and Carayon's (2007) study of network administrator and security managers' views of human error and human and organizational factors showed that human error may be related to organizational factors such as communication, security culture, and policy. Lastly, a study of the application of the Generic Error-Modeling System typology to analyze the extent of human error as a cause of privacy breaches found that mistakes in the information processing stage constitute the most cases of human error-related privacy breaches (Liginlal et al., 2009).

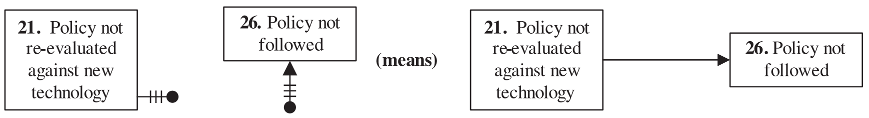
21. Policy not re-evaluated against new technology
26. Policy not followed
(means)
21. Policy not re-evaluated against new technology
26. Policy not followed

Fig. 5 – Example of special notation for relationships between factors.

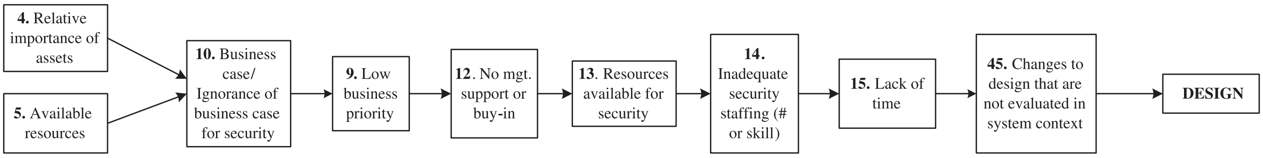
4. Relative importance of assets
5. Available resources
10. Business case/ Ignorance of business case for security
9. Low business priority
12. No mgt. support or buy-in
13. Resources available for security
14. Inadequate security staffing (# or skill)
15. Lack of time
45. Changes to design that are not evaluated in system context
DESIGN

Fig. 6 – Example (1) of design vulnerability pathway (focus group 2).

Within the theme of resource management, lack of CIS knowledge identified in both focus groups. The lack of CIS-related expertise and skills among staff and personnel decreases performance of the CIS system. Some research supports this claim. A qualitative analysis of semi-structured in-depth interviews with 30 users in 2 companies highlighted several human factors and organizational issues affecting password-related behaviors (Adams and Sasse, 1999), including the importance of compatibility between work practices and password procedures. For example, in 1 company, employees pointed out that individually-owned passwords were not compatible with group work. This study also highlighted the lack of security knowledge and information among users. Users were not necessarily opposed to security, but often unable to determine the security implications of their actions.

In the area of policy, there were a number of factors that could contribute to ineffective CIS policy including a lack of specification, lack of documentation, lack of internal capacity to create affective policies, and a lack of accountability or implementation mechanism to enforce the policy. A study of UK-based organizations investigated the uptake, content, dissemination, and impact of CIS policies and found some similar themes regarding the effectiveness of these policies (Fulford and Doherty, 2003). The study consisted of an exploratory questionnaire that sampled 208 senior CISS executives (response rate of 7.3%). The results of the analysis indicated that on average, 4 factors were perceived to be the most important: (1) visible commitment from management; (2) good understanding of security risks; (3) distribution of guidance on CIS policy; and (4) a good understanding of security requirements. These findings indicated that users' perceptions of CIS risks and requirements are important, but also identified that other factors affect the effectiveness of CIS policy, such as upper management support and shared knowledge of CIS.

Werlinger et al. (2009) expanded the conceptualization of the interplay of among human, organizational, and technological factors in a CIS system. They identified and described a way to understand the complexities of these relationships, for example, how the culture of an organization and decentralization of IT security can, in some instances, make security management more difficult. These conceptualizations validated and extended our findings of the various human and organizational pathways that may lead to CIS vulnerabilities.

The findings of this study are also consistent with the notion of latent organizational conditions that combine to create active system failures (Reason, 1997). Active systems failures in the CIS systems context include the occurrence human errors resulting in technical CIS vulnerabilities. Most approaches to vulnerability remediation only address active failures and have a direct, and usually short-lived, impact on CIS defenses. Current approaches to CIS systems apply stronger technical defenses at the contact points between people and systems in order to limit unsecure acts and subsequent vulnerabilities. But, as demonstrated in this study, such acts have a causal history that extends through many levels of the organization and system. Latent organizational conditions arise from decisions made by management, designers, policy writers, and network administrators. The latent conditions can have 2 kinds of adverse effects: they can translate into error-provoking conditions within the workplace (e.g., time pressure, understaffing, inadequate equipment, high workload) and they can create holes or vulnerabilities in the CIS system (e.g., untrustworthy update systems, lack of patch application, default passwords). Latent conditions may exist for a period of time before they combine with active failures and local triggers to create a CIS breach opportunity. Unlike active failures, whose specific forms may be difficult to foresee, latent conditions can be identified and remedied before a vulnerability surface or an attack occurs.

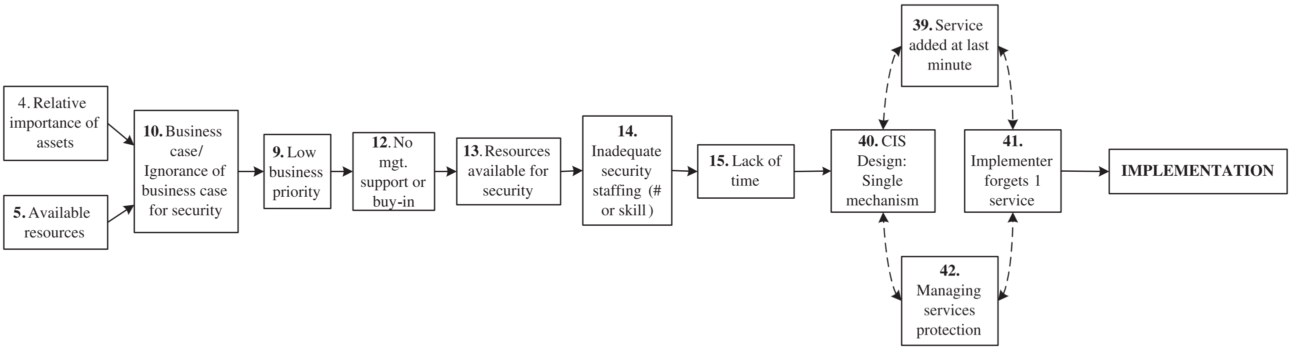
39. Service added at last minute
4. Relative importance of assets
5. Available resources
10. Business case/ Ignorance of business case for security
9. Low business priority
12. No mgt. support or buy-in
13. Resources available for security
14. Inadequate security staffing (# or skill)
15. Lack of time
40. CIS Design: Single mechanism
41. Implementer forgets 1 service
IMPLEMENTATION
42. Managing services protection

Fig. 7 – Example (2) of implementation vulnerability pathway (focus group 2).

Table 2 – Summary of human and organizational factors.

Themes	Human and organizational factors in CIS	
	Focus group 1	Focus group 2
External influences	None	New laws (e.g., HIPPA, Sarbanes Oxley) (1), vendors going out of business (2)
Human error	Mistakes (6)	Default configuration errors (34), implementer forgets a service (41), local implementer errors
Management	Lack of management support (2), lack of commitment to maintenance (12)	No upper management support (12)
Organization of CIS	Quality of CIS testing team and process (20)	Centralized security (27), lack of CIS organization (28), decentralized security (29), task allocation to unqualified staff (30), functionalized security (32), lack of central CIS communication (35)
Performance management	Lack of specification for data criticality (1), favor vendor services or products in the acquisition process (9), complexities of CIS system (11), inaccessible CIS information (13), vendor support (16), lack of user support (17), undefined CIS process, lifecycle, or performance measures (21)	Asset classification (4), CIS is a low business priority (9), lack of CIS business case (10), lack of CIS ownership, lack of CIS planning (22), functionalized process design (31), no communication among CIS designers (36), no communication between design and implementation (38), service "add on" (39), managing CIS services protection (42), no configuration management (43)
Policy	No policy specification (3), policy overload (8), poor quality of policy documentation (18)	Do not update CIS policy (8), policy purpose not documented (16), poor quality of CIS policy (17), lack of policy writing expertise (18), no policy evaluation (21), lack of policy accountability (24), policies are inaccessible for end users (25), policies are not followed (26),
Resource management	Inadequate funding (4), low staffing levels (5), tight staff schedules (7), lack of CIS knowledge base (10)	"Stupid People" – lack of CIS knowledge in user base (3), lack of CIS knowledge in staff (11), no resources for CIS (13), inadequate CIS staffing (14), lack of time (15), lack of policy writing expertise (18), lack of funding allocation (20)
Technology	Poor quality of requirement definitions (14), hardware/software types (15)	New technology implemented (5), do not adapt technology to system requirements (7), application of technology to a different environment (37), single mechanism design (40), changes in design are not evaluated in system context (45)
Training	No user training (19)	Lack of training (23), lack of training and education for developers (33)

5.1. *Limitations*

There are several limitations to this study. The sample of this study consists of 1 red team program. Interviewing other red team programs would be beneficial to understand the context of these issues with red teams that have different experiences or assessment methodologies. Further, at the time the study was conducted, the community of professional red teams was still relatively small compared to other areas of CIS assessment that are more developed, such as security audits and penetration testing.

The results of this study should not be taken as generalized facts, but rather the interpretations of some red team members' evaluations of CIS systems. The findings of this study may be transferable to certain organizations by comparing them to the context of this study. Theoretical generalization was the rational for transferability from this qualitative research study, since the basis lies in logic rather than probability (Seale, 1999). This logic inferred that the features present in a qualitative study will be related to a wider population not because the research case is representative, but because the analysis is unassailable (Mitchell, 1983). This was how a "theoretically" diverse sampling of expertise, experience, and background of red team members was justified with what may be considered a small sample size.

There may be several reasons for the differences between the conceptualizations of causal analysis networks. First, given the diversity of experiences in the sample, the variances in results could have manifested from the different compositions of each focus group. Second, the focus group design was semi-structured and exploratory. Group interviewing of this type may produce results that differ, especially across groups because the focus group approach is not prescriptive and fully-structured (Fontana and Frey, 2000). Lastly, when a red team typically conducts a brainstorm session, the core assessment team briefs the team on the system mission, red team mission, and how the system works. In each of the focus group sessions, this information was not created nor provided. The lack of pre-session briefings could also account for some of the differences between the approaches and results of the 2 focus groups.

5.2. Future research and implications

Future research may also build upon this analysis by incorporating more human and organizational factors in testing and refining the relationships among factors and CIS system performance. Researchers may add some of these constructs, such as lack of CIS funding or lack of assigned data criticality levels to CIS, into expanded models of organizational effectiveness and CIS performance.

Implications of this work suggests that human and organizational factors' roles in CIS are complex and make CIS systems particularly vulnerable in ways that technical remedies cannot fix. Possible methods to identify the relationships (or lack of) between and among human and organizational factors include large-scale social networking analysis, variance analysis, or macroergonomic assessment methods, such as the Macroergonomic Analysis and Design methodology (Robertson et al., 2002). A deeper analysis of factors and pathways may also benefit from more focus groups to further develop, refine, test, and validate the findings of this study.

Implications exist for security professionals and practitioners. Research findings suggested that human and organizational factors affect CIS performance in a multi-layered fashion and that CIS vulnerabilities are not always the result of a single mistake or configuration error. Rather, many latent organizational conditions, such as management support or decisions made by designers, combine to create scenarios where active failures (i.e., CIS vulnerabilities) may occur. Security practitioners and professionals should understand the impact of organizational factors on CIS, and that a systemized, CIS management program is necessary to address the latent organizational conditions that may contribute to CIS vulnerabilities or poor CIS performance.

Acknowledgements

This material is based upon work supported by the U.S. Army Research Laboratory and the U.S. Army Research Office under grant number DAAD19-01-1-0502 and by the College of Engineering at the University of Wisconsin-Madison.

Supplementary material

Supplementary data associated with this article can be found, in the online version, at doi:10.1016/j.cose.2009.04.006.

REFERENCES

Adams A, Sasse MA. Users are not the enemy. Communications of the ACM 1999;42(12):41–6.

Adams A, Sasse MA, Lunt P. Making passwords secure and usable. In: Thimbleby H, O'Conaill B, Thomas P, editors. People & computers XII, proceedings of HCI'97. Bristol: Springer; 1997. p. 1–19.

Albrechtsen E. A qualitative study of users' view on information security. Computers & Security 2007;26(4):276–89.

Besnard D, Arief B. Computer security impaired by legitimate users. Computers & Security 2004;23:253–64.

Bishop M. Computer security: art and science. Addison Wesley Professional; 2002.

Computer Science and Telecommunications Board-National Research Council. Cybersecurity today and tomorrow: pay now or pay later. , Washington, DC: National Academy Press; 2002.

Cresswell A, Hassan S. Organizational impacts of cyber security provisions: a sociotechnical framework. In: 40th Hawaii International Conference on Systems Sciences; 2007.

Dhillon G, Backhouse J. Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal 2001;11:127–53.

Fontana A, Frey JH. The interview: from structured questions to negotiated text. In: Denzin NK, Lincoln NK, editors. Handbook of qualitative research. Thousand Oaks: Sage Publications, Inc.; 2000. p. 645–72.

Fulford H, Doherty NF. The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management & Computer Security 2003;11(3):106–14.

Furnell S. Making security usable: are things improving? Computers & Security 2007;26(6):434–43.

Hendrick HW, Kleiner BM. Macroergonomics: an introduction to work system design. Santa Monica: Human Factors and Ergonomics Society; 2001.

Herzberg A. Why Johnny can't surf (safely)? Attacks and defenses for web users. Computers & Security 2009;28(1–2):63–71.

Howard JD, Longstaff TA. A common language for computer security incidents. Sandia National Laboratories; 1998.

Howard JD, Meunier P. Using a ''common language'' for computer security incident information. In: Bosworth S, Kabay ME, editors. Computer security handbook. New York: John Wiley & Sons; 2002. p. 3.1–3.22.

Karyda M, Kiountouzis E, Kokolakis S. Information systems security policies: a contextual perspective. Computers & Security 2005;24:246–60.

Knapp K, Marshall TE, Rainer RK, Ford FN. Information security: management's effect on culture and policy. Information Management & Computer Security 2006;14(1):24–36.

Kraemer S, Carayon P. Computer and information security culture: findings from two studies. In: Human Factors and Ergonomics Society, editor. Proceedings of the human factors and ergonomics society. Orlando, Florida; 2005. p. 1483–87.

Kraemer S, Carayon P. Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. Applied Ergonomics 2007;38(2):143–54.

Kraemer S, Carayon C, Clem JF. Characterizing violations in computer and information security systems. In: Proceedings of the 16th triennial congress of the international ergonomics association. Maastricht, The Netherlands; 2006.

Liginlal D, Sim I, Khansa L. How significant is human error as a cause of privacy breaches? An empirical stud and framework for error management. Computers & Security 2009;28:215–28.

Miles MB, Huberman AM. Qualitative data analysis: an expanded sourcebook. 2nd ed. Sage Publications; 1994.

Mitchell JC. Case and situational analysis. Sociological Review 1983;31(2):87–211.

Mizuno S, editor. Management for quality improvement: the seven new QC tools. Cambridge, Massachusetts: Productivity Press; 1988.

Morgan DL. Focus groups as qualitative research, vol. 16. Newbury Park: Sage Publications, Inc.; 1988.

Pahnila S, Siponen M, Mahmood A. Employees' behavior towards IS security policy compliance. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE; 2007.

Pasmore WA. Designing effective organizations: the sociotechnical systems perspective. John Wiley & Sons; 1988.

Proctor RW, Lien MC, Salvendy G, Schultz EE. A task analysis of usability in third-party authentication. Information Security Bulletin 2000:49–56.

Rasmussen J. Risk management, adaption, and design for safety. In: Brehmer B, Sahlin N-E, editors. Future risks and risk management. Dordrecht: Kluwer Academic Publishers; 1994. p. 1–36.

Reason J. Managing the risks of organizational accidents. Brookfield: Ashgate; 1997.

Richardson R. CSI/FBI computer crime and security survey. Computer Security Institute; 2008.

Robertson MM, Kleiner B, O'Neill MJ. Macroergonomic methods: assessing work system processes. In: Hendrick HW, Kleiner B, editors. Marcroergonomics: theory, methods, and applications. Mahweh, New Jersey: Lawrence Erlbaum Associates; 2002. p. 67–96.

Ruighaver AB, Maynard SB, Chang S. Organisational security culture: extending the end-user perspective. Computers & Security 2007;26(1):56–62.

Ryan GW, Bernard HR. Data management and analysis methods. In: Denzin NK, Lincoln YS, editors. Handbook of qualitative research. Thousand Oaks: Sage Publications, Inc.; 2000. p. 769–801.

Sarriegi JM, Torres JM, Santos J. Explaining security management evolution through the analysis of CIOs' mental models. In: 23rd international conference of the system dynamics society. Boston, Massachusetts; 2005.

Sarriegi JM, Santos J, Torres JM, Imizcoz D, Plandolit A. Modeling security management of information systems: analysis of a ongoing practical case. In: The 24th international conference of the system dynamics society. Nijmegen, The Netherlands; 2006.

Schudel G, Wood B. Modeling behavior of the cyber-terrorist. In: Conference proceedings: research on mitigating the insider threat to information systems-#2. Rand: Santa Monica, California; 2000.

Schultz E. The human factor in security. Computers & Security 2005;24(6):425–6.

Seale C. The quality of qualitative research. London: Sage Publications; 1999.

Siponen MT. A conceptual foundation for organizational information security awareness. Information Management & Computer Security 2000;8(1):31–41.

Stanton JM, Stam KR, Mastrangelo P, Jeffery J. Analysis of end user security behaviors. Computers & Security 2005;24:124–33.

Stewart DW, Shamdasani PN. Focus groups: theory and practice, vol. 20. London: Sage Publications; 1990.

Trochim WMK. The research methods knowledge base. 2nd ed. Cincinnati, OH: Atomic Dog Publishing; 2001.

Werlinger R, Hawkey K, Beznosov K. An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security 2009;17(1):4–49.

Whitten A, Tygar JD. Usability of security: a case study. Pittsburgh, PA: Carnegie Mellon University, School of Computer Science, Computer Science Department; 1998.

Whitten A, Tygar JD. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Proceedings of the 8th USENIX security symposium. Washington, DC; 1999.

Wood BJ. Duggan R. Red teaming of advanced information assurance concepts. In: DISCEX2000 DARPA information survivability conference. Hilton Head, South Carolina; 1999. p. SAND99–2590C.

Sara Kraemer is a researcher at the Wisconsin Center for Education Research in the School of Education at the University of Wisconsin-Madison. She received her Ph.D. in Industrial and Systems Engineering at the University of Wisconsin-Madison in 2006, where she completed research in human factors engineering and computer and information security. She was a National Research Council Fellow at Pacific Northwest National Laboratory in Seattle, Washington; her research focused on homeland security issues with a particular emphasis on the human factors aspects of radiation portal monitoring. In her current research, she is examining macroergonomic concepts of education (K-12) reform, including sociotechnical systems engineering for decision support at the district level as well as complex system improvement at the school-level.

Pascale Carayon is Procter & Gamble Bascom Professor in Total Quality in the Department of Industrial and Systems Engineering and the Director of the Center for Quality and Productivity Improvement (CQPI) at the University of Wisconsin-Madison. She received her Engineer diploma from the Ecole Centrale de Paris, France, in 1984 and her Ph.D. in Industrial Engineering from the University of Wisconsin-Madison in 1988. Her research areas include systems engineering, human factors and ergonomics, sociotechnical engineering and occupational health and safety, in particular in the domains of healthcare and patient safety, and computer and information security. Her research is funded by the National Science Foundation, the National Institutes for Health, the Agency for Healthcare Research and Quality, and other organizations and foundations. She is the North American editor for Applied Ergonomics, 1 of the top 3 journals in the human factors discipline. In July 2006, she was elected as the Secretary General of the International Ergonomics Association (IEA), and is the first woman to hold an officer position at the IEA. Dr. Carayon is a fellow of the Human Factors and Ergonomics Society.

John Clem holds degrees from of the University of Wisconsin-Milwaukee and Rocky Mountain College, and is a Principal Member of the Technical Staff at Sandia National Laboratories. Prior to joining the technical staff of SNL in 2002, John interned in Sandia's Center for Cyber Defenders Program where he worked on the development of an integrated network vulnerability scanning tool. As a core team member and Program Manager of Sandia's Information Design Assurance Red Team (IDART™), his work has included security assessments of critical infrastructure systems, global enterprise networks, leading-edge network security technologies, military defense systems, and R&D systems under development. Two recently concluded efforts address John's interest in providing decision makers with better information for evaluating security risks and trade-offs: the development of a new method to structure and optimize red team assessments, and a process to extend red team assessments with risk analysis. Currently John is a staff member in the Security Systems Analysis Department at Sandia, focusing on the cyber security of physical protection systems. John also serves as a red team instructor, frequently training qualified government, military, and commercial customers in the discipline of red teaming – authorized, adversary-based assessment for defensive purposes.