An Adversarial Viewpoint of Human and Organizational Factors in Computer and Information Security: Final Report

University of Wisconsin-Madison & Information Design Assurance Red Team (IDART™), Sandia National Laboratories

August 2006

Sara Kraemer and Pascale Carayon
Center for Quality and Productivity Improvement
University of Wisconsin-Madison
610 Walnut Street 575 WARF
Madison, WI 53726

John Clem
IDART™
Sandia National Laboratories
PO Box, 5800, MS-0671
Albuquerque, NM 87185-0671

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.

For more information:
Dr. Pascale Carayon, Director of the Center for Quality and Productivity Improvement
Tel: +1-608-265-0503
Fax: +1-608-263-1425
carayon@engr.wisc.edu

RESEARCH TEAM

Sara Kraemer & Pascale Carayon
Center for Quality and Productivity Improvement
University of Wisconsin-Madison
610 Walnut Street 575 WARF
Madison, WI 53726
Tel: 1-608-263-2520
Fax: 1-608-263-1425
Email: carayon@engr.wisc.edu

John Clem
IDART™
Sandia National Laboratories
PO Box, 5800, MS-0671
Albuquerque, NM 87185-0671
Tel: 1-505-844-9016
Fax: 1-505-845-7065
Email: jfclem@sandia.gov

ABSTRACT

This report presents a multi-dimensional examination of the human and organizational factors that affect computer and information security (CIS) and explains how human and organizational factors contribute to CIS vulnerabilities, namely, the various pathways and mechanisms leading to a technical CIS vulnerability. Human factors in CIS, such as password memorability or usability of encryption methods, in addition to organizational factors in CIS, such as implementation and monitoring of security policies or procedures are analyzed.

Research was conducted using an "adversarial" approach. A red team, a group of security analysts who model hacker behavior in order breach CIS systems in a sanctioned environment, was used as the source of information. A case study of a single red team program (The Information Design Assurance Red Team (IDART™) program at Sandia National Laboratories in Albuquerque, New Mexico) that crafted "an adversarial viewpoint" of human and organizational factors in CIS was conducted using a qualitative research approach. Data collection methods included interviews, focus groups, and review of red team reports.

Fourteen red team members in individual interviews reported 589 total comments on human and organizational factors consistent with the work system categories (Carayon and Smith, 2000; Smith and Carayon-Sainfort, 1989). The work system categories consist of: organization (372 comments), individual (124 comments), task (46 comments), technology (40 comments), and environment (7 comments).

Two focus groups of five red team members each constructed the various mechanisms and pathways of human and organizational factors related to CIS vulnerabilities: design, implementation, configuration (Howard and Longstaff, 1998; Howard and Meunier, 2002) and operational vulnerabilities. Both focus groups emphasized organizational factors, such as management commitment, resources, funding, and CIS policy, contributing to CIS vulnerabilities.

This study created a work systems framework that characterizes the complex and multivarious nature of CIS systems. This framework serves as a novel contribution to the fields of human factors engineering and computer science, as it provides a systems approach to CIS that incorporates human and organizational factors. This contribution furthers the understanding and etiology of CIS system vulnerabilities, which will allow system defenders to build more secure computer and information systems to remediate CIS breaches and attacks.

TABLE OF CONTENTS

1. INTRODUCTION

The security community has largely focused on the technical causes of computer and information security (CIS) breaches or vulnerabilities. It has been argued that the human factor that is associated with the use and design of security is largely ignored by this community (Sasse, Brostoff, & Weirich, 2001). The poor implementation of security can seriously impact an organization's productivity, reputation, and the well-being of its employees. The implication is that while the human side of computer security is almost always exploited, such as a user error, the blame is not of the users but rather the factors of the work systems in which they work. Even with a strong, technology-centered approach, many exploits can and will be facilitated by user behavior (Besnard & Arief, 2004; Carayon & Kraemer, 2002; Schein, 1984) or faulty operational, management, or organizational factors (Computer Science and Telecommunications Board-National Research Council, 2002). This point has been further emphasized by Cobb, Cobb, & Kaybay (2002), in that information systems security has both technical and non-technical aspects, of which the primary non-technical factor is human behavior that may defeat many technical security measures. Research into the non-technical security aspects of CIS is critical because CIS systems are typically technology-centered systems where user security considerations are not jointly considered in their design and use.

Human factors issues in CIS are being recognized as important concepts for addressing CIS attacks and breaches. Weak CIS protection (e.g., poor passwords or inadequate encryption methods) and malicious intentions set the stage for CIS attacks, but it is argued that successful attacks are the outcomes of flawed policies and/or practices whose origins are deeply rooted within early design assumptions or managerial decisions (Besnard & Arief, 2004). The etiology and causal factors for CIS breaches and vulnerabilities are still unknown. This is partly due to the complexity of the problem (e.g., multiple risk factors) and the lack of studies examining the problem from this perspective.

In order to investigate human and organizational factors and CIS, the Center for Quality and Productivity Improvement at the University of Wisconsin-Madison has collaborated with Sandia National Laboratories' Information Design Assurance Red Team (IDART™) program. The purpose of this study is to characterize the various human and organizational factors associated with CIS and describe the various pathways and mechanisms that result in specific types of CIS vulnerabilities.

This research examines the "non-technical" aspects (i.e. human and organizational factors) of computer and information security (CIS). The adversarial viewpoint of these factors is important and unique. Systems defenders need to take human and organizational factors into account as they plan their defenses against attacks. Their defensive strategies depend on not only understanding how to harden technical security vulnerabilities, but also how to develop a holistic system that considers how human behavior interacts with the technical CIS system.

2. RESEARCH OBJECTIVES

The focus of this study is to study human and organizational factors that of CIS, from an adversarial perspective. CIS adversaries include attackers who attempt to exploit technical or non-technical system faults (i.e. CIS vulnerabilities and human and organizational factors). The adversarial viewpoint of "non-technical" factors (i.e. human and organizational factors) is an important perspective to capture because: (1) there is extremely limited research examining the non-technical aspects of CIS; (2) there is no research examining non-technical aspects of CIS from the viewpoint of an attacker; and (3) the adversarial viewpoint of vulnerabilities, both technical and non-technical, is critical to CIS system designers' and defenders' knowledge base.

2.1 Specific Research Objectives

2.1.1 Research Question #1

What are the human and organizational factors of CIS from an adversarial perspective?

This research question used the theoretical foundations of *work system theory* (Carayon & Smith, 2000; Smith & Carayon-Sainfort, 1989). The work system has five distinct elements that interact with each other: the *individual* (e.g., end user, network administrator, security manager); *technology* (e.g., passwords, firewalls, smart cards); *organization* (e.g., security department, security policy, security culture); *task* (e.g., applying patches, opening attachments, creating passwords); and *workplace environment* (e.g., workstation design, noise level). The work system approach is appropriate for this research question because it does not emphasize one element of the work system, nor does it assert an explanation or predict system states. This framework serves to describe a system and its various components; therefore, it is suitable for this research question. The human and organizational factors of CIS fit into the five categories of the work system theory.

2.1.2 Research Question #2

How do human and organizational factors contribute to technical CIS vulnerabilities?

This research question explores the various pathways and mechanisms that are associated with four types of CIS vulnerabilities: design, implementation, configuration, and operational. Howard and Longstaff (1998) and Howard and Meunier (2002) developed a taxonomy of the first three CIS vulnerabilities: design, implementation, and configuration. The last vulnerability, operational, was developed by the red team members during the course of the study.

There are definitions associated with each type of CIS vulnerability. A design vulnerability is inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a technical vulnerability. Implementation vulnerabilities result from an error made in the software or hardware implementation of a satisfactory design. Configuration vulnerability results from an error in the configuration of a system, such as having system accounts with default passwords, having no access control for files, or having vulnerable services enabled.

The human and organizational factors of CIS will be described with the five work system elements of Carayon and Smith (2000) and Smith and Carayon-Sainfort (1989). These factors will be used as variables to explain the relationships among human and organizational factors and the CIS technical vulnerabilities. The Howard and Longstaff (1998) and Howard and Meunier (2002) vulnerability taxonomy serves as basis for describing various CIS vulnerabilities.

3. METHODS

3.1 Study Design

The study design consists of a qualitative-based case study of a single red team program. This study was conducted in collaboration with the red team at the IDART™ program at Sandia National Laboratories in Albuquerque, New Mexico. Sandia National Laboratories was the study site and data collection was conducted from May 9, 2005 to May 13, 2005. The research team consists of two members from the University of Wisconsin-Madison: Sara Kraemer (data collector and research study organizer) and Professor Pascale Carayon (dissertation advisor), and two members from Sandia National Laboratories: John Clem (IDART™ leader and project coordinator) and Mike Skroch (IDART™ supervisor and project support).

Fourteen semi-structured individual interviews with core red team members were conducted to explore the first research question regarding human and organizational factors associated with CIS. The interview guide for individual interviews consists of one global question, "What are the human and organizational factors associated with CIS?" and a set of probes (see Appendix A). The purpose of the interview probes is to guide the discussion when necessary and place boundaries on topics that are covered. The set of probes for this question will include each of the components of work system theory (Carayon & Smith, 2000; Smith & Carayon-Sainfort, 1989): organization, technology, task, individual, and workplace environment. The interviewer also used a "check sheet" to keep track of interviewee responses (see Appendix B). The check sheet was also based on the elements of the work system of Carayon and Smith (1989; 2000).

Two focus groups with six members each were conducted to explore the second research question, "How do human and organizational factors contribute to CIS vulnerabilities?" In each of the focus groups, red team members brainstormed various ideas on how human and organizational factors in CIS systems are related. See Appendix C for the interview guide for focus groups. Each group was tasked to link the human and organizational factors that were identified in individual interviews conducted earlier in the week to various categories of CIS vulnerabilities: design, implementation, configuration, and operational.

Three red team assessment reports were reviewed to reveal how the red team describes human and organizational factors. This information is used to aid in the description of human and organizational factors and CIS vulnerabilities, as well as how the red team characterizes various "views" of the CIS system.

3.2 Data Collection

3.2.1 Data Collection for Research Question #1

The individual interviews with core red team members were conducted in a closed, private room in an unclassified building on Kirtland Air Force Base. Twelve interviews were audio-recorded. These recordings were transcribed. Two interviews were not recorded, due to malfunctioning audio-equipment. The content of the interviews were scribed by the interviewer.

After the recordings were transcribed, and before they were analyzed, feedback was sought from each participant. The documentation of the interview was sent to each participant via email. In each email message, the participant was asked to review their interview and answer three questions (see Appendix D). The questions consisted of adding, changing, or removing any part of their interviews. The interviewees responded via email with their comments, if any.

Three red team reports were acquired from John Clem via email. Two reports were done for DARPA's Fault Tolerant Network program (Clem, Badgett, & MacAlpine, 2003; Duggan, Villamarin, Moore, & Davis, 2003). These reports were of new systems and architectures for network overlays. The third report was developed for Gas Industry Standards Board (GISB) (Duggan, 2000). The report provided an analysis of GISB's electronic delivery mechanism related standards.

3.2.2 Data Collection for Research Question #2

The focus groups with core red team members were also conducted in a closed, private room in an unclassified building on Kirtland Air Force Base. Each focus group was four hours in length. The focus groups were audio-recorded and transcribed by a transcription service. The purpose of focus groups was to flowchart how various human and organizational factors are related to one another and ultimately result in a technical CIS vulnerability. The focus group members were given a number of post-it notes in the beginning of the sessions so that they may identify and write down various human and organizational factors related to CIS vulnerabilities of design, implementation, configuration, and operational, and place them on a very large piece of hanging white paper. The focus group brainstormed the various human and organizational factors, identified their relationships, and refined the pathways in a flowchart form. In essence, each focus group constructed a "map" consisting of formalized human and organizational factors of the CIS system that are located and linked to specific types of CIS vulnerabilities.

Feedback from John Clem and David Duggan on the research summary report was reviewed and integrated into the results of the study. See Appendix E for a list of feedback questions.

3.3 Data Analysis

3.3.1 Data Analysis for Research Question #1

Data analysis for Research Question #1 consisted of a content analysis. The data analysis strategy is a combination of qualitative and quantitative content analysis. Since the first research aims to identify all the types of human and organizational factors that adversely affect CIS, the meaning of data is important. Therefore, the data coded will include segments of phrases or sentences (qualitative content analysis). The number of times participants mention each human or organizational factor or human or organizational factor that is related to a CIS, will be tracked (quantitative content analysis).

The content analysis included several phases. First, a coding structure was developed to capture the critical content of the data. Then, the coding scheme was applied to each identified comment made by the interviewees or text from red team reports. Third, the frequencies and patterns in the

results was explored and quantified. The transcribed individual interviews, with interviewee feedback comments and revisions, were analyzed by coding the content of interview themes using the qualitative software package, QSR NVivo©. QSR NVivo© does not perform the data analysis; it is simply a data organization tool for the researcher. The researcher constructs meaningful coding categories and analyzes the meaning of responses. The coding structure will consist of "nodes", which represent defined human and organizational factors associated with CIS. When coded, the node will hold references to passages of text from the interview and focus group data.

The purpose of Research Question #1 is to identify and describe the human and organizational factors that adversely affect CIS. For this reason, the coding strategy will consist of two elements: (1) comments coded will be coded once in the coding framework and (2) comments will be coded at the most specific node. Before data analysis will begin, a skeleton coding structure of human and organizational factors that are adversely related to CIS will be created. For the human and organizational factors related to CIS, the components of the skeleton coding scheme will consist of the various work system elements (Carayon & Smith, 2000; Smith & Carayon-Sainfort, 1989). Subnodes will be created to describe specific factors. The subnodes will be aggregated for each major category and the number of subnodes for each major category will be reported in results.

The human and organizational factors that adversely affect CIS will be described with narrowly bounded concepts and hence will employ a micro-level data analysis strategy. Each piece of the coding scheme will be defined before the coding process begins and each comment in the data will be coded once. New factors and themes that emerge during the analysis were added and defined to the coding scheme. The protocol for emergent themes and factors is as follows. The node structure consists of mutually exclusive categories of factors, so as the data analysis progresses, subsequent comments may make a node more specific. When this happens, the codes were removed from the higher level node to the lower level node, and all the comments are compiled at the new, more specified node. The codes moved from the higher level node to the lower level node were renamed to describe the new specificity. For example, if an interviewee made a comment about planning security implementation, a new node entitled "implementation planning" was created under the organizational element category. If the same or different interviewee made another comment about another aspect of implementation, for example, "implementation procedures", three new nodes were created. The new structure contained one higher level node, entitled "implementation" with two lower level nodes, "implementation planning" and "implementation procedures". The coding strategy involved coding a comment once, therefore, there was no need to re-examine the entire data set once a node was created, moved, or renamed. Each interview was coded in this fashion.

3.3.2 Data Analysis for Research Question #2

Data analysis for Research Question #2 also included several phases and each focus group was analyzed separately. As was done with the first research question, a coding structure was developed to capture the critical content of the focus group data. The coding structure consisted of the human and organizational factors identified by the focus group members in their flowcharts. The coding scheme was applied to each identified comment made by the

interviewees. The transcribed focus groups were also analyzed by coding the content of focus groups using the qualitative software package, QSR NVivo©. The purpose of Research Question #2 is to describe the *relationships* among variables (i.e. human and organizational factors) and outcomes (i.e. technical CIS vulnerabilities), so the coding strategy is similar to Research Question #1. The node structure yielded a set of mutually exclusive categories of factors, with comments coded once in categories. Notes by the researcher and comments made by interviewees were coded in categories to provide justification of proposed relationship.
The flowchart of human and organizational factors and CIS vulnerabilities that were produced by each of the focus groups serves as a summary description of how human and organizational factors are related to types of CIS vulnerabilities. The flowchart was scribed verbatim to electronic format, using Microsoft Visio. Then, "fragments" of the summary description were specified. The fragments consist of a chain of factors, or pathways, leading to a specific vulnerability. These pathways were grouped by vulnerability: design, implementation, configuration, and operational.

4. RESULTS

Results are summarized in two parts: Research Question #1 and Research Question #2. The first section addresses Research Question #1 and consists of five parts: (1) organizational factors; (2) technology factors; (3) task factors; (4) individual factors; and (5) environmental factors. Results for Research Question #1 consist of a data display (i.e. node structure) and a quantification of comments and number of people commenting in each category. The number of people commenting in a category is denoted with a backslash after the number of comments. For example, 9/3 comments means 9 total comments made by 3 different people.

The second section addresses Research Question #2 and is divided into two parts: the first and second focus group. Each pathway associated with a type of technical CIS vulnerability, i.e. design, implementation, configuration, and operational, were also reported via data display and short narrative.

In the reporting scheme, there are several key terms. A “node” refers to a group of comments referring to common theme (i.e. a type of work system element). A “sub-node” refers a more specific theme of the same category. A “comment” refers to an interviewee’s view of a type of work system element.

4.1 Demographic Information

Demographic information was gathered from 13 red team members in the following areas: (1) age; (2) gender; (3) years of red teaming experience; and (4) background and training. One person declined to participate in this portion of the study. In order to protect the identity of the participants, ages and years of experience in red teaming are reported in average ranges. Gender, years of experience, and backgrounds are summarized. Refer to Table 1 for a summary of demographic information on the red team participants.

Table 1. Summary of Red Team Member Demographic Data

Demographic Categories	Responses (n=13)	
Age	Average: 38 years	Range: 26 years – 51 years
Gender	12 males, 1 female	
Years of red teaming experience	Average: 7 years	Range: 2 years – 14 years
Summary of background	Electrical engineering	Nuclear weapons research
	Computer science	Engineering degree
	Business administration	Military service
	Information technology	Systems engineering
	Unix administration	Management
	Cisco Systems	Modeling and simulation
	Networking	Red team experience outside of IDART™
	Network security technologies	Network administration
	Communications systems	Product support
	JAVA development	Quality assurance engineering
	Enterprise technology	Wireless security
	Operating systems	Intrusion detection
	Systems programming	Programming
	Information security	

4.2 Human and Organizational Factors Associated with CIS

The coding process resulted in 589 total comments and 217 total sub-nodes, consisting of five separate categories: organizational factors (372 comments, 130 sub-nodes), individual factors (124 comments, 56 sub-nodes), task factors (46 comments, 13 sub-nodes), technology factors (40 comments, 16 sub-nodes), and environmental factors (7 comments, 2 sub-nodes). See Figure 1 for the frequency of comments related to human and organizational factor and CIS. See Figure 2 for a summary of nodes and comments associated with human and organizational factors.

Figure 1. Frequencies of Comments Related to Human and Organizational Factors and CIS

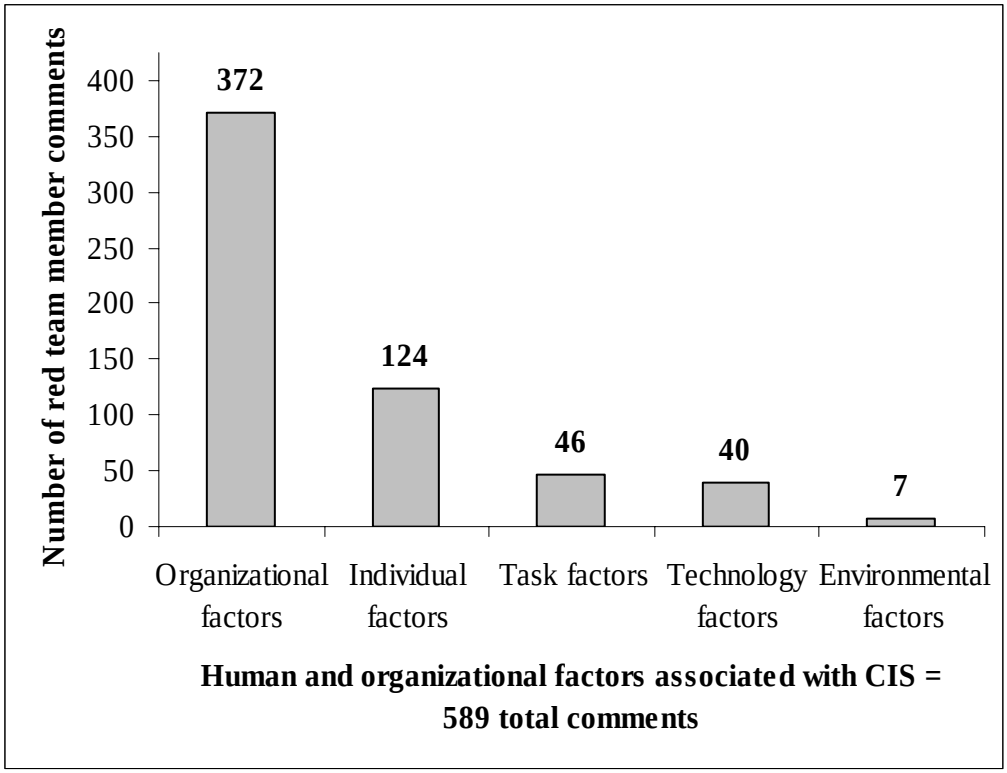
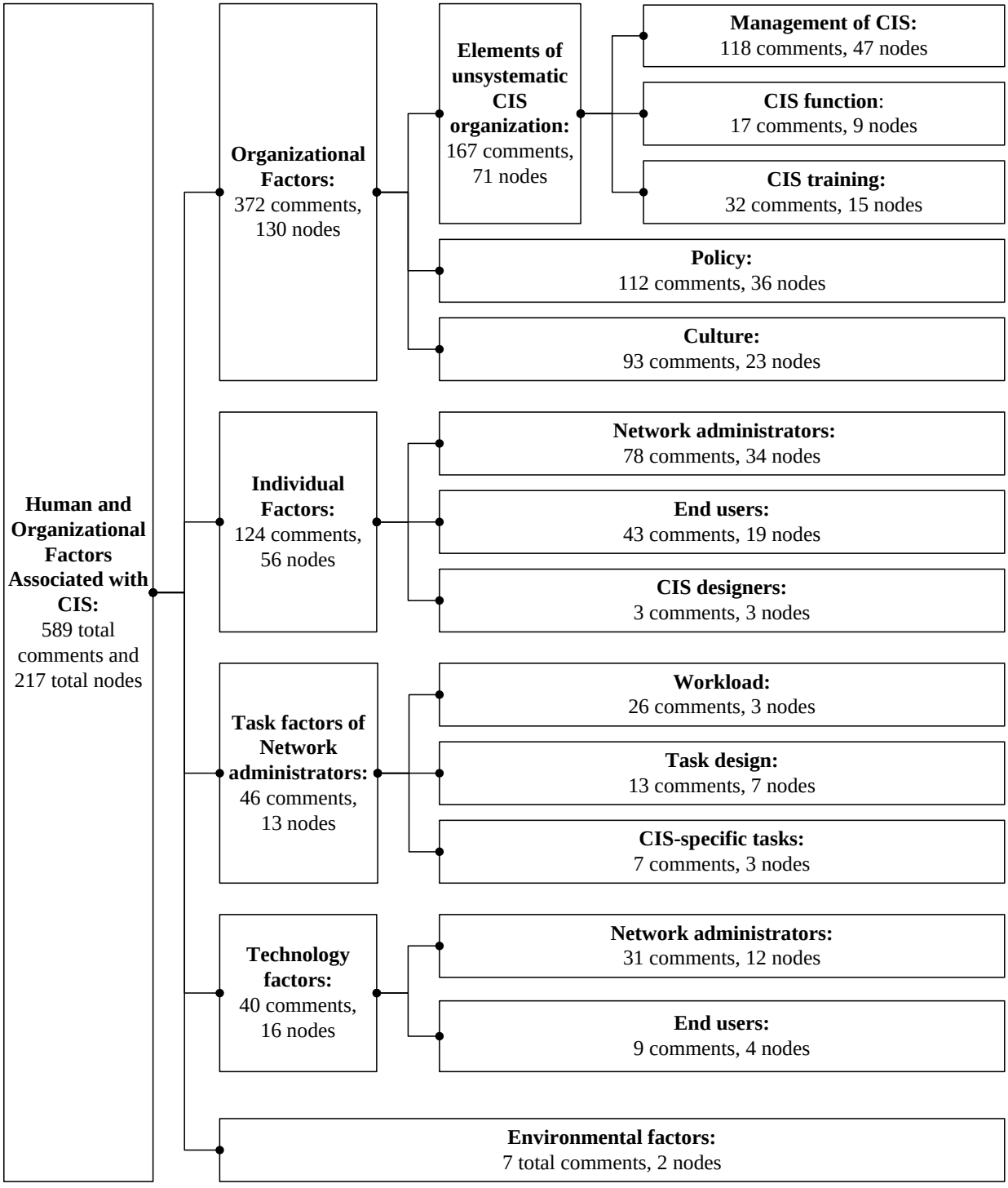


Figure 2. Summary of Comments and Nodes of Human and Organizational Factors and CIS



4.2.1 Organizational Factors Associated with CIS

The category of *organizational factors associated with CIS* (372 comments, 130 sub-nodes) is comprised of three major parts: policy (112 comments, 36 sub-nodes), culture (93 comments, 23 sub-nodes), and elements of unsystematic CIS organization (168 comments, 71 sub-nodes). For a

complete set of definitions for each node in the organizational factors category, please refer to Appendix F.

4.2.1.1 Organizational Factors of CIS: Policy

For the node of *CIS policy* (112 of 373 total comments on organizational factors), red team members commented on the following sub-nodes: policy content (48/9 comments), lack of procedures for writing policies (21/7 comments), poor guidelines or procedures (9/4 comments), and policy management (34/7 comments). See Figures 3.1 and 3.2 for summaries of comments on the *CIS policy* node.

4.2.1.1.1 Policy Content

In the *policy content* category, there were 48/9 comments and 15 sub-nodes. A large number of comments were on clarity of policy (22/9 out of 48 total comments on policy content, 8 sub-nodes). One red team member commented on *imprecise policy:*

> *"Policy is really intended to be a control on behavior in the organization…I believe that there are certain vulnerabilities related to policy. If we look at policy, for example, the way we would look at law, it is a higher level and it is language-based. Complexity becomes a factor in the policy in the degree of reliability and that the policy will have its intended effect throughout the organization. It requires interpretation so they can be misinterpreted if they're not well-written or clear."*

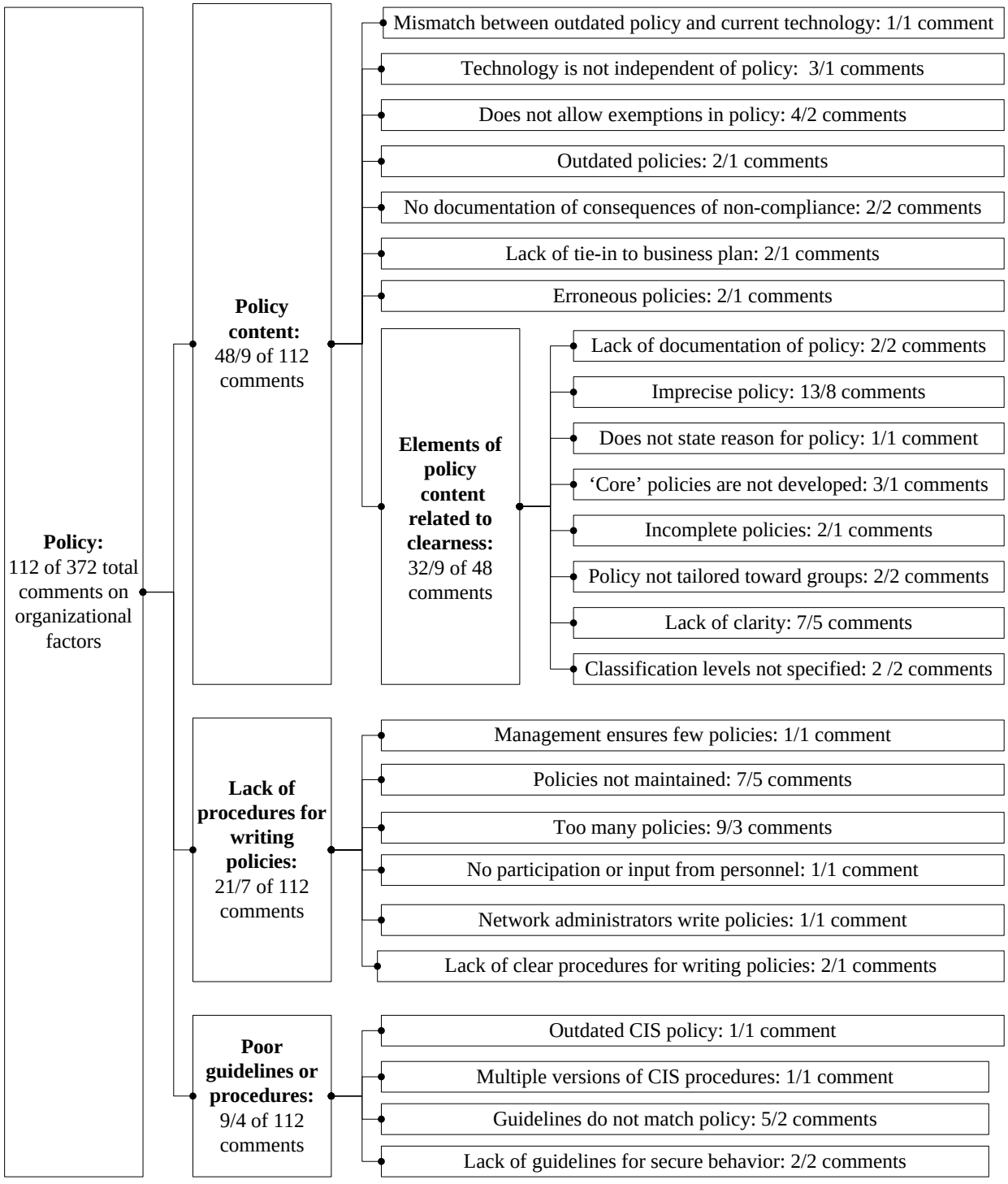
The 16 remaining comments in this category comprised 7 sub-nodes. One red team member commented on *technology is independent of policy:*

> *"Policies need to be technology independent otherwise you'll never be able to make the correct policies for the current technology. So, under policies you need to have something that changes every time you [incorporate] a technology, so you write a guideline for that technology. And when the technology goes away, you throw the guideline away. [Guidelines] have to be less rigorous but they have to show the intent of the policy. What you end up with, if you have policies that are [technology dependent], is that the newer technologies are not covered by any kind of policy. So, people do whatever they want to with them. They [use] the passwords they want, they create whatever kinds of accounts, and they hook them up to whatever networks they want."*

Another red team member commented on the sub-node *does not allow exemptions in policy*:

> *"In my ideal world… exceptions have to be made to policy. There needs to be a process of [granting them]. An exception has to be documented …. So that later, there is a [viewable] justification."*

Figure 3.1. Quantification of Comments on CIS Policy



4.2.1.1.2 Lack of Procedures for Writing Policy

In the *lack of procedures for writing policy* node, there were 21/7 comments and 6 sub-nodes. The *policies are not maintained* sub-node contained one of the largest number of comments (7/5 comments). A red team member commented on the sub-node *policies are not maintained*:

> *"They [organizations] believe that you build something and you're done… You bring in two or three people; you secure all of the machines and the network with today's technology. Then you have those two or three people go off and do something else. There's nobody to maintain it, there's no process in place to keep it going so that it updates [over] time. If you sleep for a week in this business, you're out of date."*

On another sub-node, *too many policies,* a red team member made this comment:

> *"Many organizations are overwhelmed with policies - too many for principals to understand, and too many to have any effective component of enforcement. Making a policy is often a "band-aid," which does not actually create any real security [if the policy is not followed]."*

4.2.1.1.3 Poor Guidelines or Procedures

In the *poor guidelines or procedures* node, there were 9/4 comments and 4 sub-nodes. Within this category, the sub-node *guidelines do not match policy* (5/2 comments) was the largest.

4.2.1.1.4 Inadequate Policy Management

In the *inadequate policy management node*, there were 34/7 comments and 11 sub-nodes. The largest sub-node in this category was *organization fails to enforce policy* (8/3 comments). One red team member made this remark:

> *"Exploiting and attacking computer systems and networks are made much easier by the way humans fail to enforce and adhere to the security policies that typically apply to information systems."*

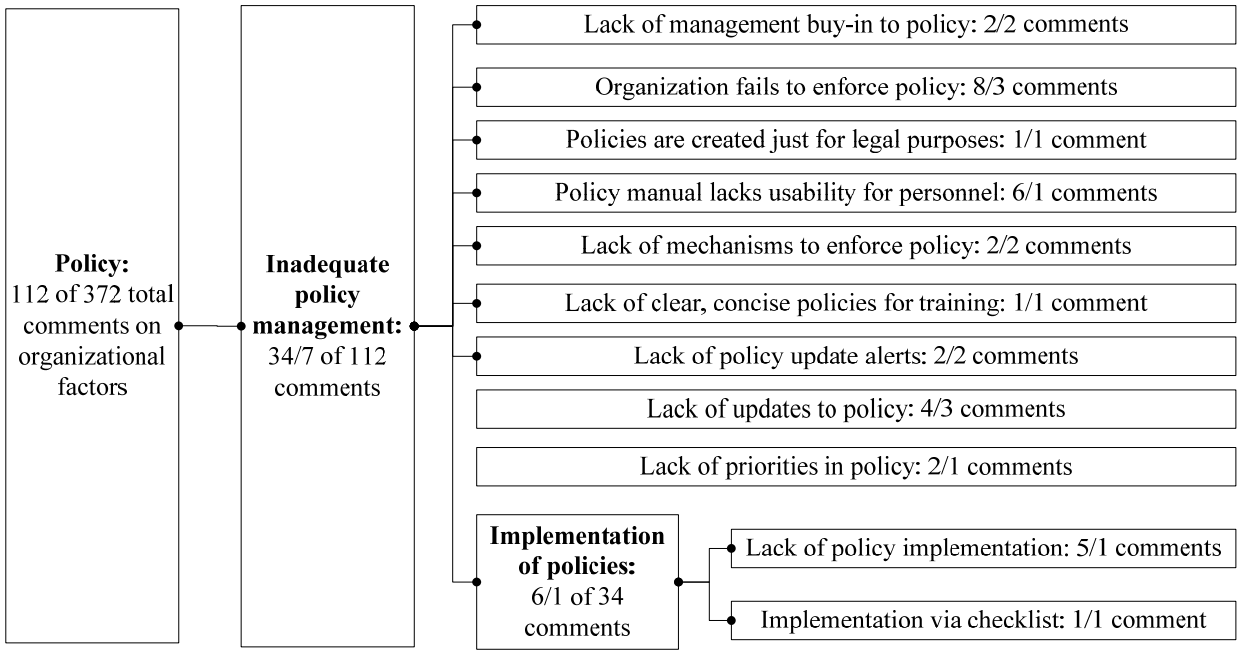
Another category was the sub-node *policy manual lacks usability for personnel* (6/1 comments). On this sub-node, a red team member said this:

> *"Different organizations that I've looked at have very thick documents… [In one case,] I couldn't even read the whole thing because it was too long."*

The same red team member added:

> *"Some of them [just] sound like jargon ... [they] just make [the policies] sound legitimate."*

Figure 3.2. Quantification of Comments on CIS Policy, Continued

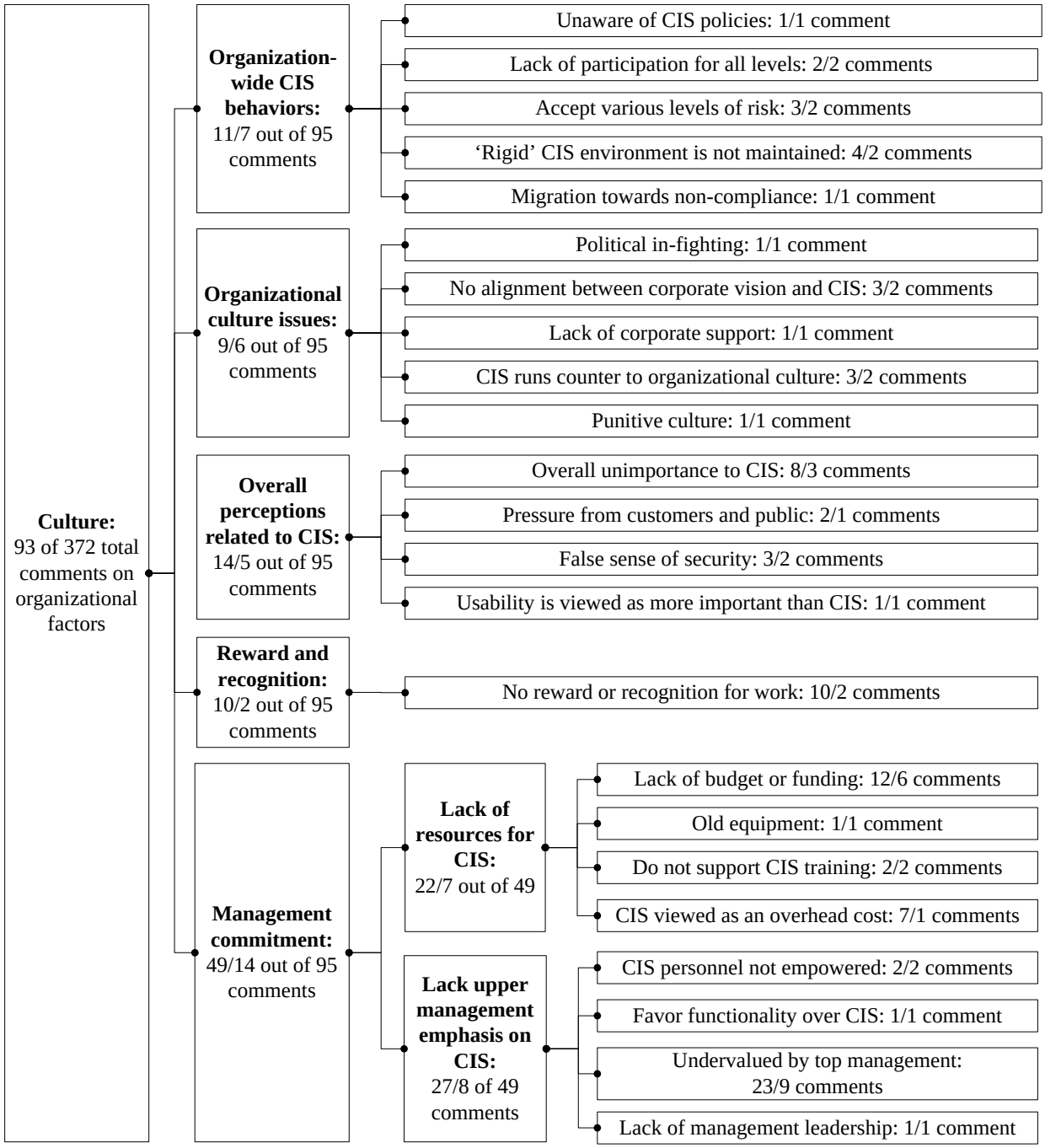


4.2.1.2 Organizational Factors of CIS: Culture

For the CIS *culture* node (93 of 373 total comments on organizational factors, 23 nodes), red team members commented on the following sub-nodes: organization-wide CIS behaviors (11/7 comments, 5 nodes), organizational culture issues (9/6 comments, 5 nodes), overall perceptions related to CIS (14/5 comments, 4 nodes), reward and recognition (10/2 comments, 1 node), and management commitment (49/14 comments, 8 nodes). The management commitment node consisted of: lack of resources for CIS (22/7 comments, 4 nodes) and lack of upper management emphasis on CIS (27/8 comments, 4 nodes). See Figure 4 for a summary of the *culture* node.

There are various dimensions used to describe organizational culture. A framework by Schein (1992) recognized the beginning levels as the “surface-level” components to culture (i.e. artifacts). As these components are recognized and understood, analysis of the deeper values and underlying assumptions to culture follow (Schien, 1984). The following data on CIS culture reflects this framework in that there are a number of sub-categories that reflect artifacts (i.e. rewards and recognition, training, management commitment) and underlying assumptions and beliefs (i.e. organization-wide CIS behaviors, organizational culture issues, overall perceptions related to CIS). These dimensions are consistent with some categories that have been developed to describe safety culture (Guldenmund, 2000) and CIS culture (Kraemer and Carayon, 2005b). The Kraemer and Carayon (2005b) study of CIS managers’ perceptions of CIS culture found the following dimensions of CIS culture: employee participation, training, issues related to hiring practices, reward system, management commitment, and communication and feedback.

Figure 4. Quantification of Comments on CIS Culture



4.2.1.2.1 Organization-Wide CIS Behaviors

In the *organization-wide CIS behaviors* node, there were 11/7 comments and 5 sub-nodes. The largest sub-node was *'rigid' CIS environment is not maintained* (4/2 comments).

4.2.1.2.2 Organizational Culture Issues

In the *organizational culture issues* node, there were 9/6 comments and 5 sub-nodes. The largest sub-nodes were*: no alignment between corporate vision and CIS* (3/2 comments) and *CIS runs counter to organizational culture* (3/2 comments).

4.2.1.2.3 Overall Perceptions Related to CIS

In the *overall perceptions related to CIS node*, there were 14/5 comments and 4 sub-nodes. The largest sub-node was *overall unimportance to CIS* (8/3 comments), on which a red team member made this comment:

> *"I think it's a commitment to support the level above and below you, and a pervasive understanding or belief that this is an issue that's important to the organization."*

Another red team member that commented on this sub-node said:

> *"It's not understanding that it's a constant cycle to [maintain] security and that cycle isn't just [one person], but it's enabled by the entire staff or the entire organization, from the CEO to the janitor."*

4.2.1.2.4 Reward and Recognition

In the *reward and recognition* node, there were 10/2 comments and a single node: *no reward or recognition for work*. One red team member made this comment:

> *"If you cause more problems by not being secure, then you're not actually doing your job …and it is because systems administrators or network administrators have been the invisible people, they have not been given any kind of kudos when nothing goes wrong. If nothing goes wrong, nobody knows they exist. They only get called when something doesn't work. And so as long as you do your job and, however you do it, in the past nobody's cared how you do it, as long as you've done it."*

4.2.1.2.5 Management Commitment

Management commitment (49/14 comments, 8 nodes) consisted of two major nodes: lack of resources for CIS (22/7 comments, 4 nodes) and lack of upper management emphasis on CIS (27/8 comments, 4 nodes). One of the larger sub-nodes in the *lack of resources for CIS* node was *CIS viewed as an overhead cost* (7/1 comments). One red team member commented on this:

> *"It's just changing the culture, changing the mentality of management and CEOs that is putting security on top of everything else, because, again, it comes out to a cost. IS groups are a high cost and they don't see a return on it. They know the work gets done and it helps them, but [they see no] real profitable return."*

The largest sub-node in the *lack of upper management emphasis on CIS* node was *CIS is undervalued by top management* (23/9 comments). One red team member commented on the sub-node of *CIS is undervalued by top management*:

> *I think one of the biggest factors…is buy-in [by top management]. If you don't get management upper level buy-in, and you don't have your CEO coming out saying security's important and this is a big deal to us, the rest of the people in the organization aren't going to care. Because if it's not important to management, [it results in a] 'why is it important to me?' type of thing."*

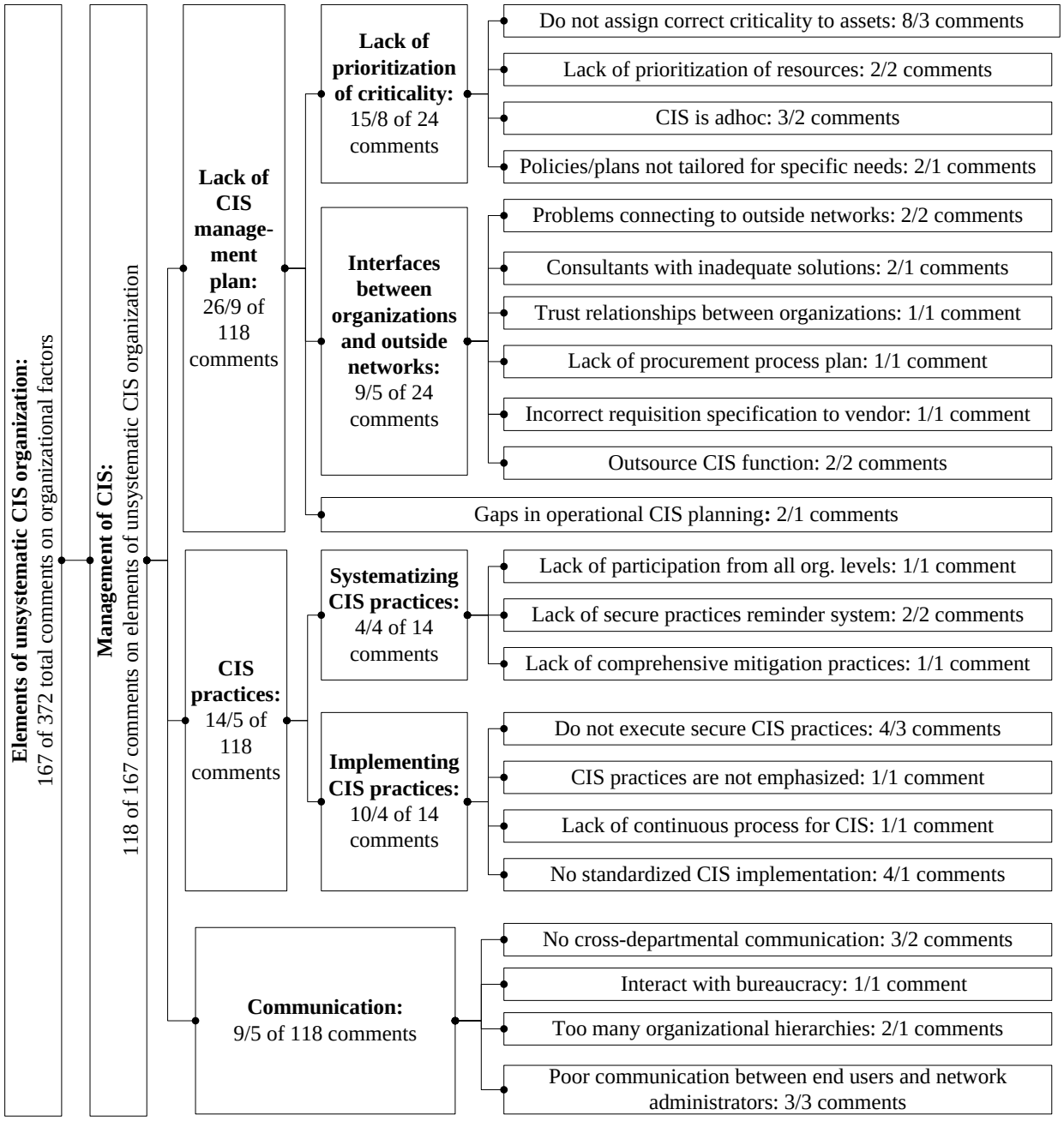
4.2.1.3 Organizational Factors of CIS: Elements of Unsystematic CIS Organization

The category of *elements of unsystematic CIS organization* (166 of 372 total comments on organizational factors, 69 nodes) was comprised of three main nodes: management of CIS (119 comments, 47 nodes), CIS function (17 comments, 9 nodes), and training (30 comments, 13 nodes).

4.2.1.3.1 Management of CIS

The *management of CIS* node (118 comments, 46 nodes) consisted of 4 sub-nodes: CIS process and performance (69/11 comments), lack of CIS management plan (26/9 comments), CIS practices (14/5 comments), and communication (9/5 comments). See Figure 5 for a summary of the quantification of comments on CIS management plan, practices, and communication.

Figure 5. Quantifications of Comments on CIS Management Plan, Practices, and Communication



Lack of CIS management: This sub-node consists of two major categories: lack of criticality prioritization (15/8 comments, 4 nodes) and interfaces between organizations and outside networks (9/5 comments, 6 nodes). Within the *lack of criticality prioritization* node, the sub-node *do not assign correct criticality to assets* (8/3 comments) is the largest. On this, one red team member said:

> *"In terms of security one thing that you see a lot of times is security at one certain level no matter what, and that's where governance and policy come in. If you secure everything at [one] level, it may be high, but it's everything at [one] level; that it shows that you really don't understand what you have and why you have it -- you're*

> *just applying a uniform level of security, and that [implies] clearly that the things that are important are easier to get to than they should be, compared to things that are not important."*

There were two sub-nodes: interfaces between organization and outside networks (9/5 comments) and gaps in operational CIS planning (2/1 comment).

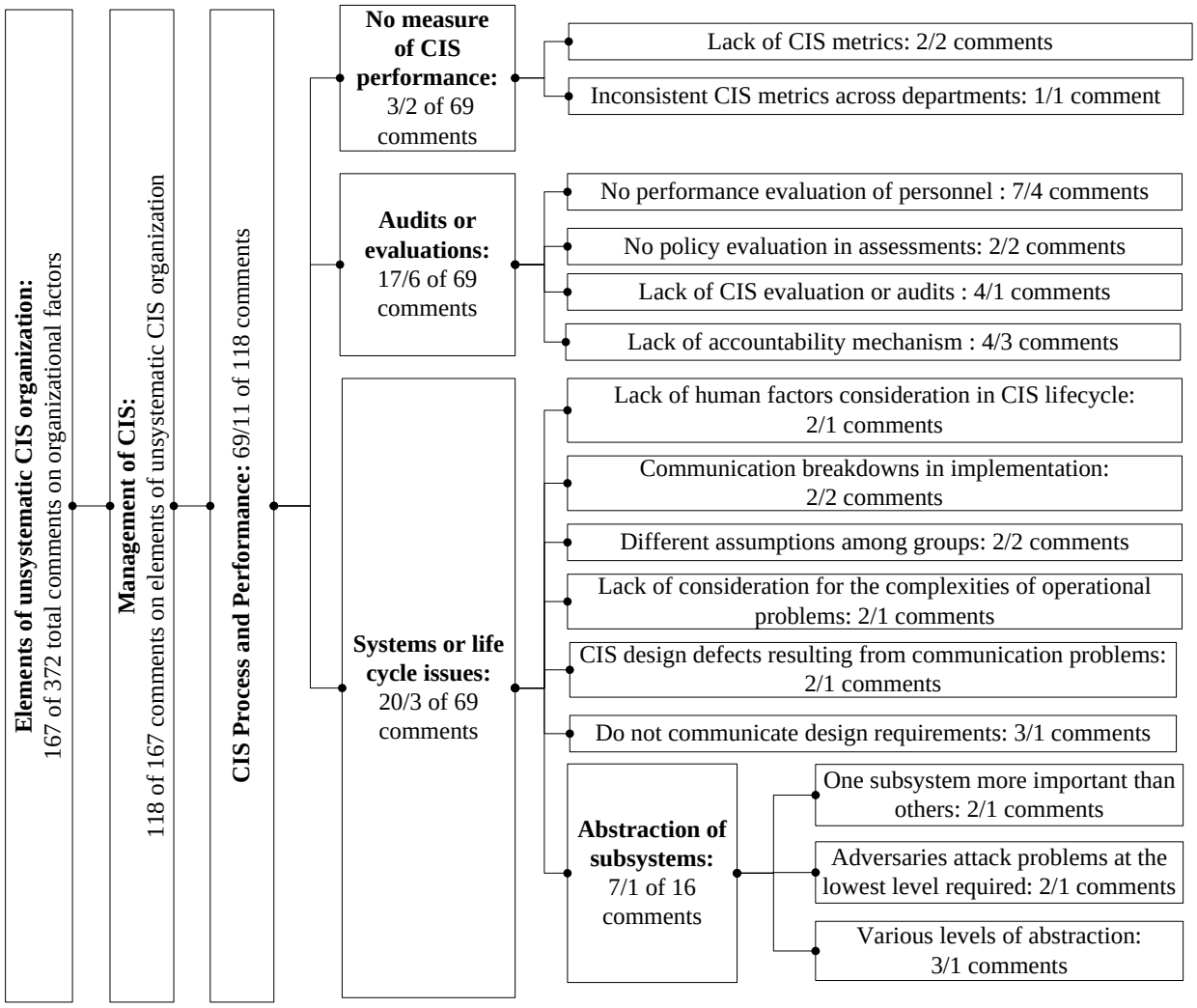
CIS practices: This node consisted of two sub-nodes: systematizing CIS practices (4/4 comments, 3 nodes) and implementing CIS practices (10/4 comments, 4 nodes).

Communication: This node consisted of 9/5 comments and 4 sub-nodes. One of these sub-nodes is *poor communication between end users and network administrators* (3/3 comments). One red team member commented:

> *"I think this type of attitude is a result of a lack of communication by both parts. If security was better at explaining the reasons for their controls, or why they are less responsive to user requests at some points in time, users would be more understanding of the situation. If the users could explain their needs better, instead of saying "because I need this," security would be more helpful and probably work with the users more."*

CIS process and performance: The *CIS process and performance* category consisted of 69/11 comments, 24 nodes, and 4 sub-nodes. The two largest nodes were: systems or life cycle issues (20/3 comments, 9 nodes) and sustainable and adaptive CIS processes (29/10 comments, 11 nodes). See Figures 6.1 and 6.2 for summaries of comments on the sub-node *CIS process and performance*.

Figure 6.1 Quantification of Comments on CIS Process and Performance



One of the sub-nodes in the *systems or life cycle issues* node (20/3 comments, 9 nodes) was *lack of consideration of the complexities for operational problems* (2/1 comments). One red team member commented:

> *"As you move further along and you start getting into operation, then it's not only the technical issues, but now you have to consider the operational issues of when do you have to lock your screen, do you need to implement a password, who's going to be locking the room to make sure that the people who are in that room are supposed to be in it. As you move up that scale, you're starting to get more and more [human] interaction and opportunity for communication breakdown."*

The *abstraction of subsystems* sub-node consisted of 7/1 comments and 3 nodes. The sub-nodes were: one subsystem more important than others (2/1 comments), adversaries attack problems at the lowest level required (2/1 comments), and various levels of abstraction (3/1 comments). On the *one subsystem considered more important than others* sub-node, one red team member commented:

> *"If you kind of think of these on a piece of paper, when any particular group gets them, they expand one of those sections and the others shrink down. Another way to look at level of abstraction that a red-teamer would go after is maybe a physical level. So, if you're thinking about policy in policy domain and you assume that it will be implemented correctly in the application, then I could attack you at the application level if your policy isn't implemented well. And if you think that your application is really well set, then I'll go through and exploit and use a back door into your operating system. And it doesn't matter what your application is doing, I'll own your system …"*

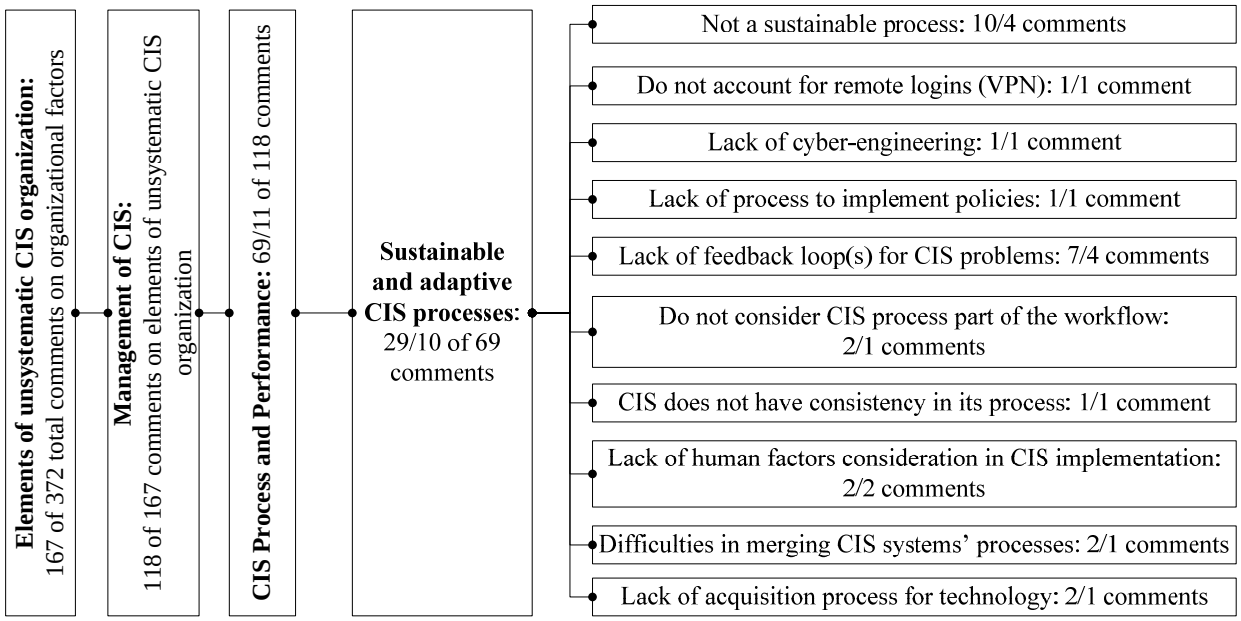
On *adversaries attack problems at the lowest level*, one red team member said:

> *"If you think you have your operating system [protected] really well, I'll go in and chip your operating system and get into your hardware and then I'll control the microprocessor that controls your operating system. But [the OS is] your level of abstraction I'll get into the microcode of the microprocessor. Even if you have a complete belief or proof that your operating instructions are [executing] correctly at a microprocessor level, I'll control your microprocessor at [still] a lower level."*

Sustainable and adaptive CIS process: This node consisted of 29/10 comments and10 sub-nodes. The largest sub-nodes were: not a sustainable process (10/4 comments) and lack of feedback loop(s) for CIS problems (7/4 comments). Refer to Figure 6.2 for a summary of comments on the sub-node of *sustainable and adaptive CIS processes*. One red team member commented on *CIS is not a sustainable process*:

> *"I think another big breakdown is making sure that computer information security is sustainable. So [security staff] may come in and make it gold-plated, make it perfect, so it's well-thought out, well-composed, but the integrity of that [process], of the information security starts to degrade over time for a number of reasons. Sustainability is a major concept in security that is overlooked. Human factors, whether organizational or operational, is a critical component to sustainability that is often overlooked even by those that understand sustainability."*

Figure 6.2. Quantification of Comments on CIS Process and Performance, Continued



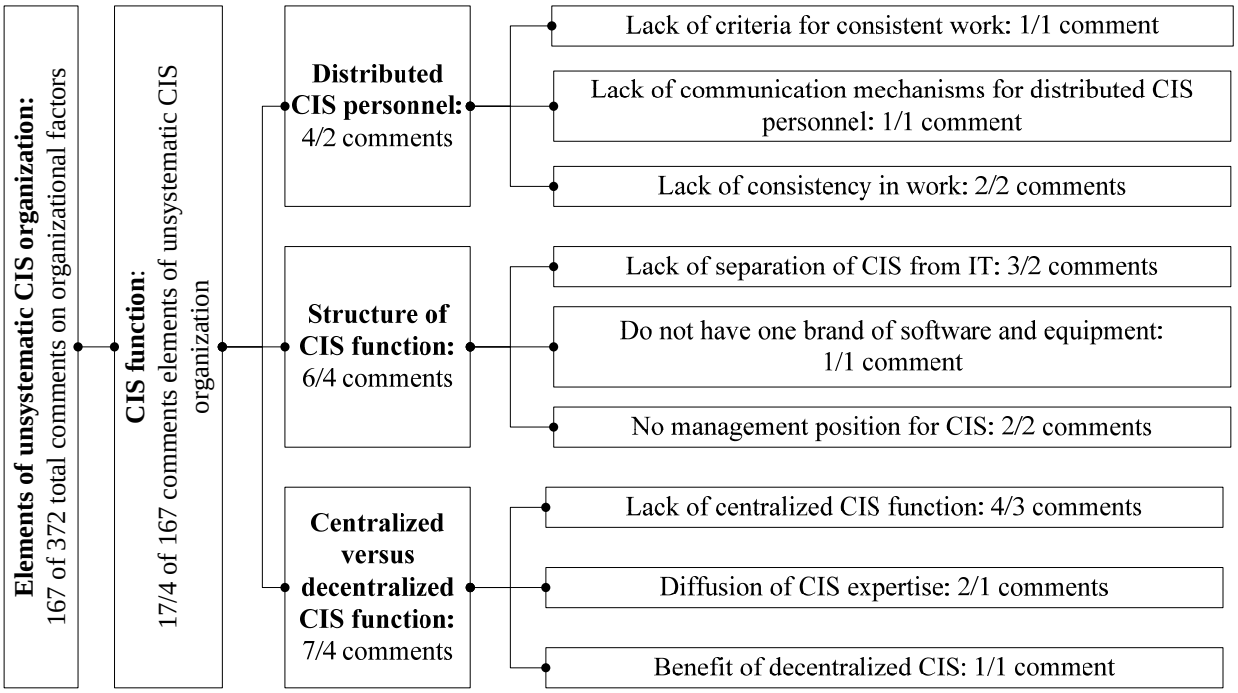
4.2.1.3.2 CIS Function

The *CIS function* node (17/4 comments and 9 nodes) consisted of 3 major sub-nodes: distributed CIS personnel, structure of CIS function, and centralized versus decentralized CIS function. Refer to Figure 7 for a summary of comments on the *CIS function* node.

A common problem is ensuring that the IT and CIS functions are separate from one another. One red team member commented on the problems associated with the *lack of separation between the CIS and IT functions*:

> *"[Many] companies make a security person do everything [administer networks]. They [end up being] one person in the same. And in practicality, it needs to be two different [classes of] people. One [class] needs to be looking and finding the problems. One [class] needs to be fixing the problems. When you have that same [class] doing both, something is going to fall through the cracks."*

Figure 7. Quantification of Comments on CIS Function



4.2.1.3.3 CIS Training

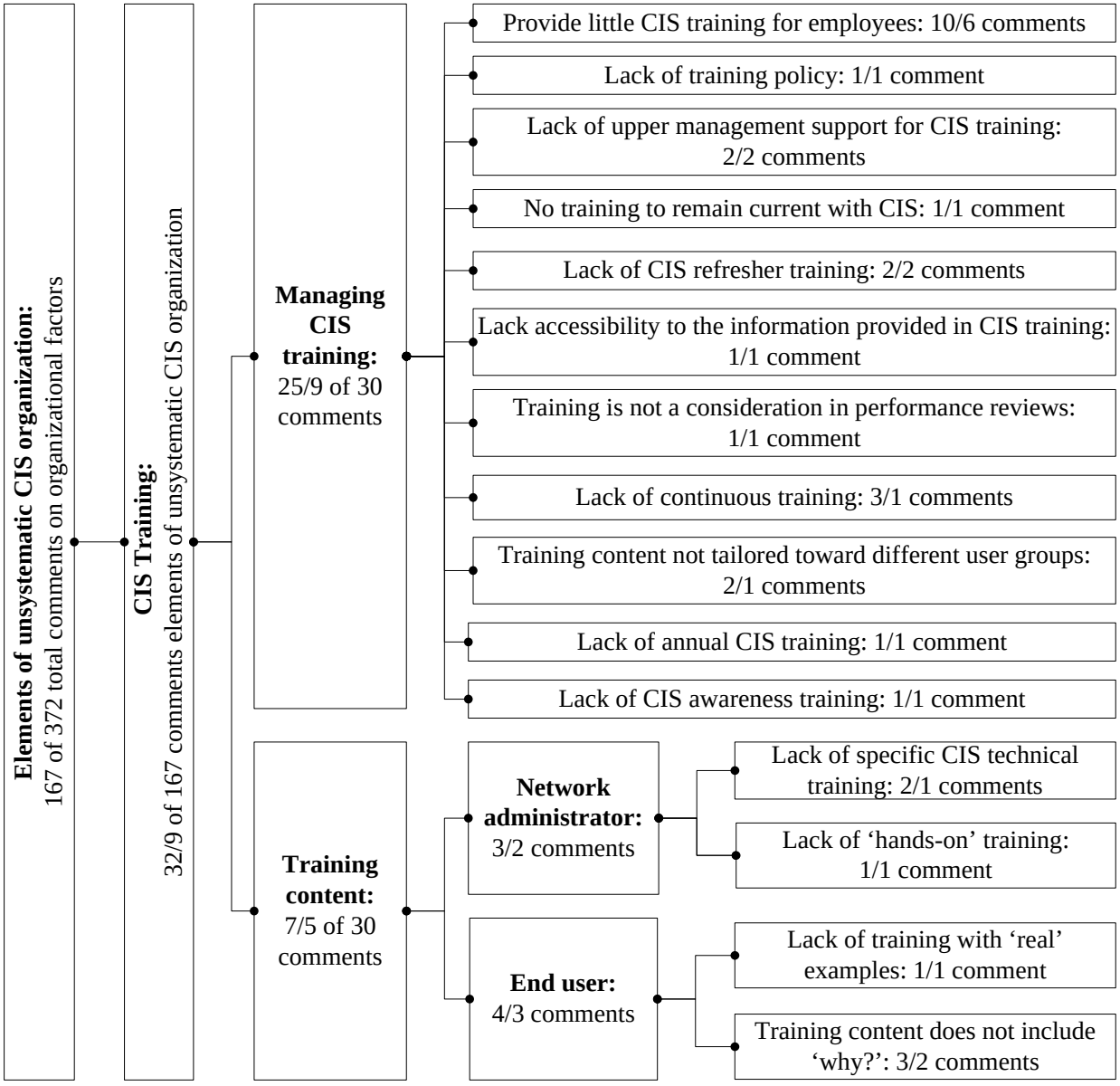
The *CIS training* category consisted of 30/9 comments and 13 sub-nodes. There were two main nodes: managing CIS training (23/9 comments, 11 nodes) and training content (7/5 comments, 4 nodes). See Figure 8 for a summary of comments on the node *CIS training*.

Provide little CIS training for employees was the largest sub-node in the *CIS training* category (10/6 comments). One red team member described *lack of CIS training for employees*:

> *"The users, CEO, all of them have to be trained. Training doesn't stay in your head for very long. [For example,] a CEO's secretary doesn't understand it [CIS] and has a weak password. You [an adversary] get on her computer because she didn't understand it [CIS], and she has the CEO's passwords. And you [an adversary] get to the CEO, and you've got their entire mailing list, customer list, and all the contact information. So, there's not really any person that you can say doesn't matter, because what you get from the lowest person on the food chain gets you up higher and higher."*

Some red team members emphasized that training content should be tailored to two groups: network administrators (3/2 comments) and end users (4/3 comments).

Figure 8. Quantification of Comments on CIS Training



4.2.2 Individual Factors Associated with CIS

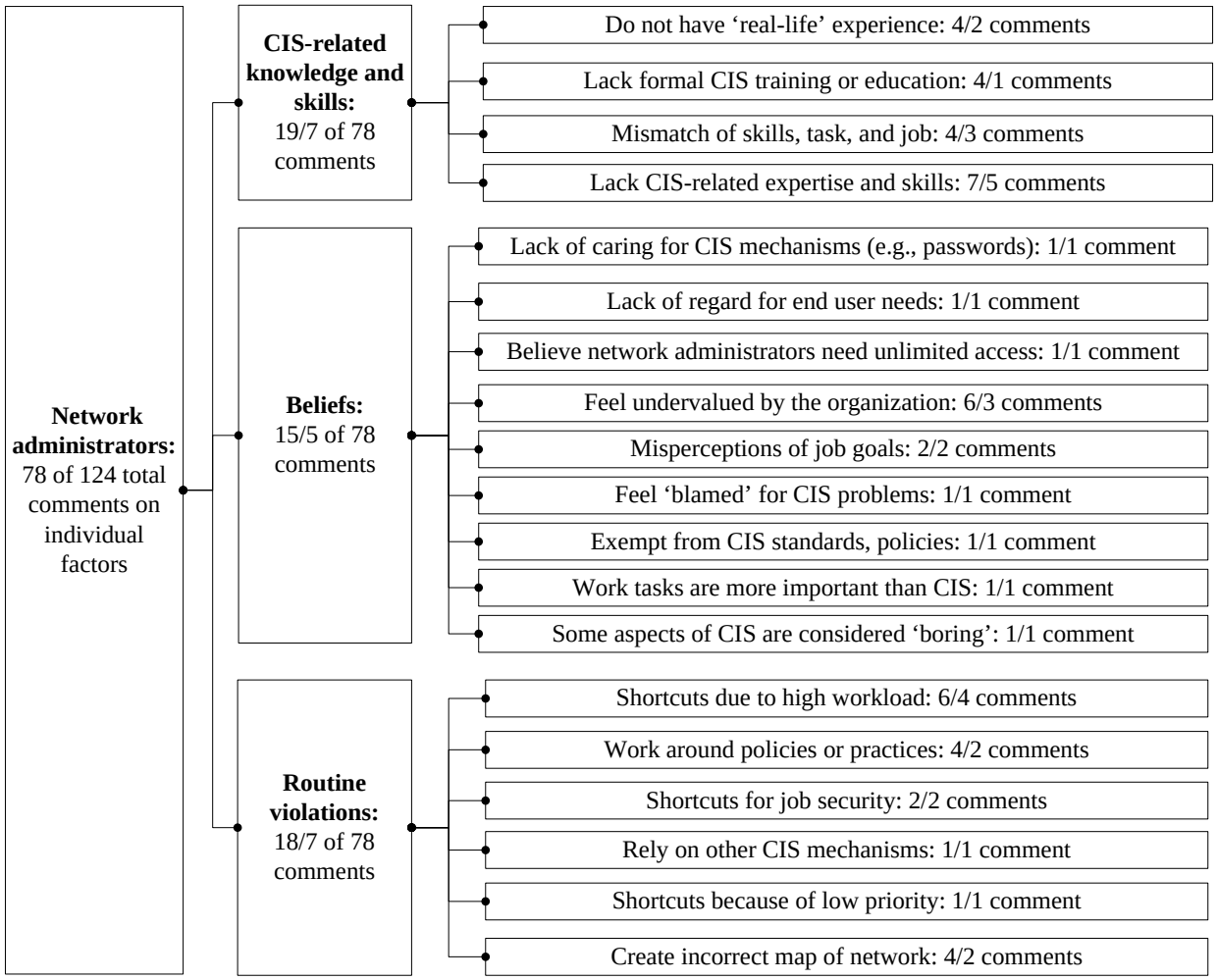
The category of *individual factors associated with CIS* (124 total comments, 56 nodes) was split into three groups: network administrators (78 comments, 34 nodes), end users (43 comments, 19 nodes), and CIS designers (2 comments, 3 nodes). Each group was reported separately. Refer to Appendix G for a complete set of definitions of sub-nodes associated with *individual factors associated with CIS*.

4.2.2.1 Network Administrators

The *network administrator* category (78 comments, 34 nodes) was comprised of seven sub-categories: CIS-related knowledge and skills (19/7comments, 4 nodes), beliefs (15/5 comments,

9 nodes), routine violations (18/7 comments, 6 nodes), lack of an adversarial mindset (16/3 comments, 8 nodes), cognitive performance (6/4 comments, 5 nodes), motivation (2/2 comments, 2 nodes), and trust (2/1 comments, 2 nodes). Refer to Figures 9.1 and 9.2 for summaries of comments on *individual factors of network administrators*.

Figure 9.1. Quantification of Comments on Individual Factors of Network Administrators



4.2.2.1.1 CIS-Related Knowledge and Skills

The *CIS-related knowledge* category consisted of 16/7 comments and 4 nodes. The largest sub-node was *lack of CIS-related expertise and skills* (7/5 comments).

4.2.2.1.2 Beliefs

The *network administrator beliefs* node consisted of 12/5 comments and 9 nodes. The largest sub-node was *feel undervalued by the organization* (6/3 comments). One red team member commented on how network administrators *feel undervalued by the organization*:

> *"If you [network administrators] cause more problems by not being secure, then you're not actually doing your job… Because systems administrators or network administrators have been the invisible people, they have not been given any kind of kudos when nothing goes wrong. If nothing goes wrong, nobody knows they exist. They only get called when*

something doesn't work. And so as long as you do your job and, however you do it, in the past nobody's cared how you do it, as long as you've done it."

In regard to network administrators' *misperceptions of job goals*, one red team member commented:

"Their [network administrators] job is to work for the company, to follow the company rules, and to maintain equipment to the best of their ability within those rules. [But] they [network administrators] [might] believe that their job is to maintain equipment and be responsive to everybody."

5.2.2.1.3 Routine Violations

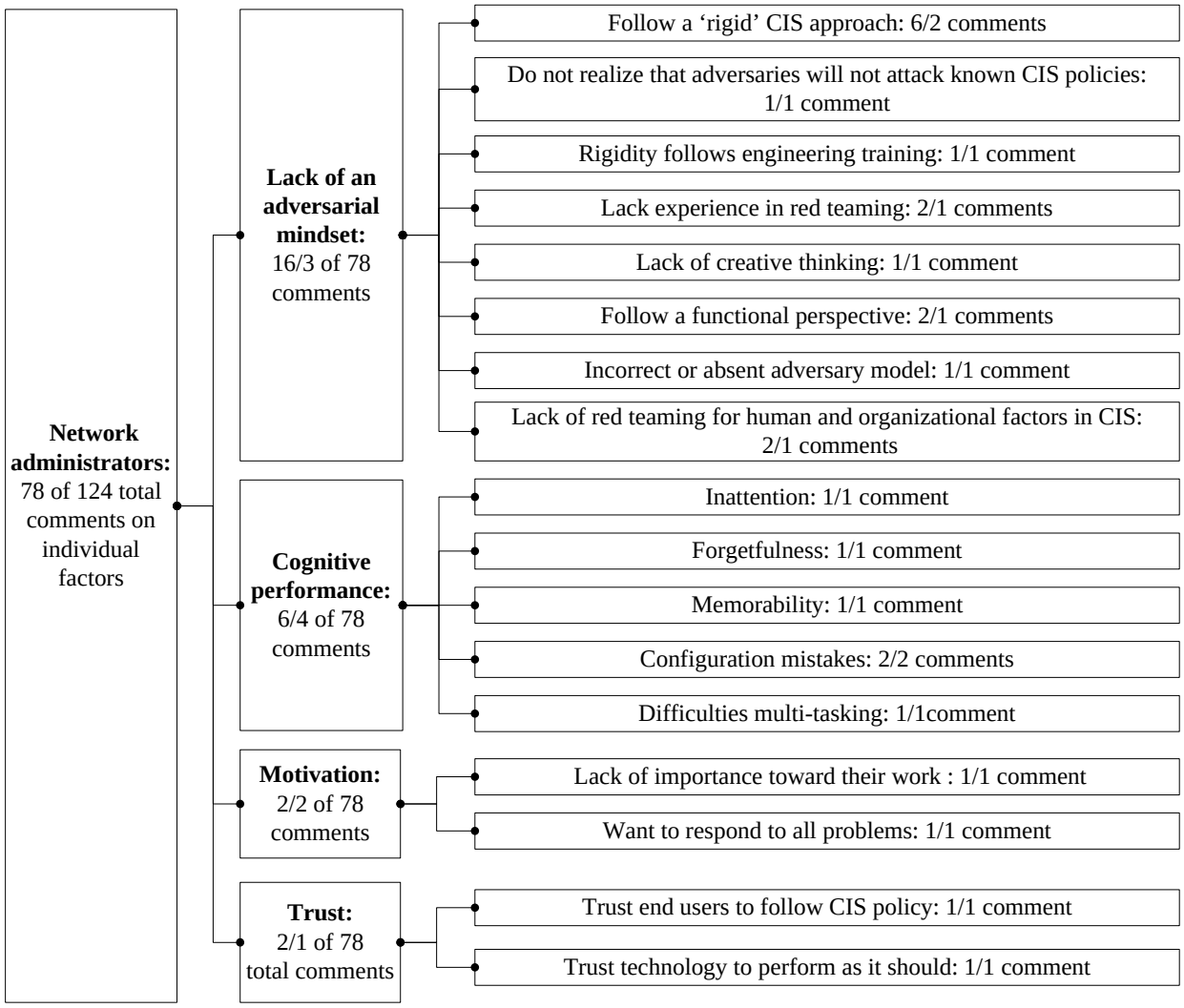
In the *network administrators' routine violations* category, there were 18/7 comments and 6 nodes. Routine violations are "corner-cutting" or short cuts, optimizing violations reflect actions unrelated to the functionality of the task (Reason, Parker, and Free, 1994) The largest *routine violations* sub-node was: *shortcuts due to high workload* (6/4 comments). One red team member elaborated on *shortcuts due to high workload*:

"Most of the time they do take shortcuts. You know, uh, if you have to take care of and manage 30 servers or 30 high level machines and network machines and your policy says you can't have the same password on each one, than that means you've got 30 different passwords."

A unique shortcut network administrators take is to *purposely create an incorrect map of the network* (4/2 comments). One red team member commented:

"If we have a general idea of what the network looks like, we can start at a piece of equipment, follow the wires and the conductivity or use our own tools to try to map out the network. And where you find discrepancies between what they thought they had and what you see they have. [During] one assessment where they gave us a map and we looked and there was not a single piece of equipment from their network that was in operation. [The network map] was 100% wrong. The things that were in place now were not following the policy. But, that's because the administrators didn't put [equipment] on the map because once it goes on the map it becomes audited and once it becomes audited, they [network administrators] have to follow policy."

Figure 9.2. Quantification of Comments on Individual Factors of Networks Administrators, Continued



4.2.2.1.4 Lack of Adversarial Mindset

The *lack of adversarial mindset* node had 16/3 comments and 8 nodes. *Network administrators' "rigid" approach to CIS* was the largest sub-node (6/2 comments). One red team member commented:

> *"They [network administrators] have a lot of work to do. So they check the list …an adversary doesn't think that way at all. In fact, the very useful thing for a red teamer is to determine the security policy, if you have one. And the other one is the 'rigidity' that the security administrators follow which then makes them very predictable which then [provides] us, the cyber warriors, a lot more places to look, or more holes to be able to break into."*

Network administrators' unique functional perspective (2/1 comments) was highlighted. A red team member commented on *network administrators' functional perspective:*

> *"I think that the biggest issues are that the people that are working on CIS don't think about the adversarial perspective when they're thinking about their security. So, they're*

> *thinking more from a functional perspective, from meeting the objectives of the operation without regard to security: what's the through-put, how responsive it is, and how reliable is it?"*

4.2.2.1.5 Cognitive Performance, Motivation, and Trust

There were three smaller sub-nodes in the *individual factors of network administrators* category: cognitive performance (6/4 comments and 5 nodes), motivation (2/2 comments and 2 nodes), and trust (2/1 comments and 2 nodes).

4.2.2.2 End Users

In *the individual factors of end users* category, there were 43 comments, 19 nodes and six main subcategories: CIS-related knowledge (7/4 comments, 2 nodes), beliefs (19/8 comments, 7 nodes), behaviors (4/2 comments, 4 nodes), trust (4/2 comments, 3 nodes), motivation (4/2 comments, 2 nodes), and cognitive performance (5/3 comments, 1 node). Refer to Figure 10 for a summary of comments on the individual factors of end users.

4.2.2.2.1 CIS-Related Knowledge

In the *CIS-related knowledge* category there were 7/4 comments and 2 nodes. *Lack of general CIS-related knowledge* was the largest sub-node is (5/4 comments).

4.2.2.2.2 Beliefs

There were 19/8 comments and 7 sub-nodes in the *end users' beliefs* node. *Do not understand "why" CIS is important* was one of the largest sub-nodes (5/1 comments). One red team remarked:

> *"…it's just a lack of knowledge. If you don't understand why you're doing something, then you don't do it correctly. So if you don't understand why passwords are important, then you tend to write [them] down because you don't understand what the password is supposed to do for you."*

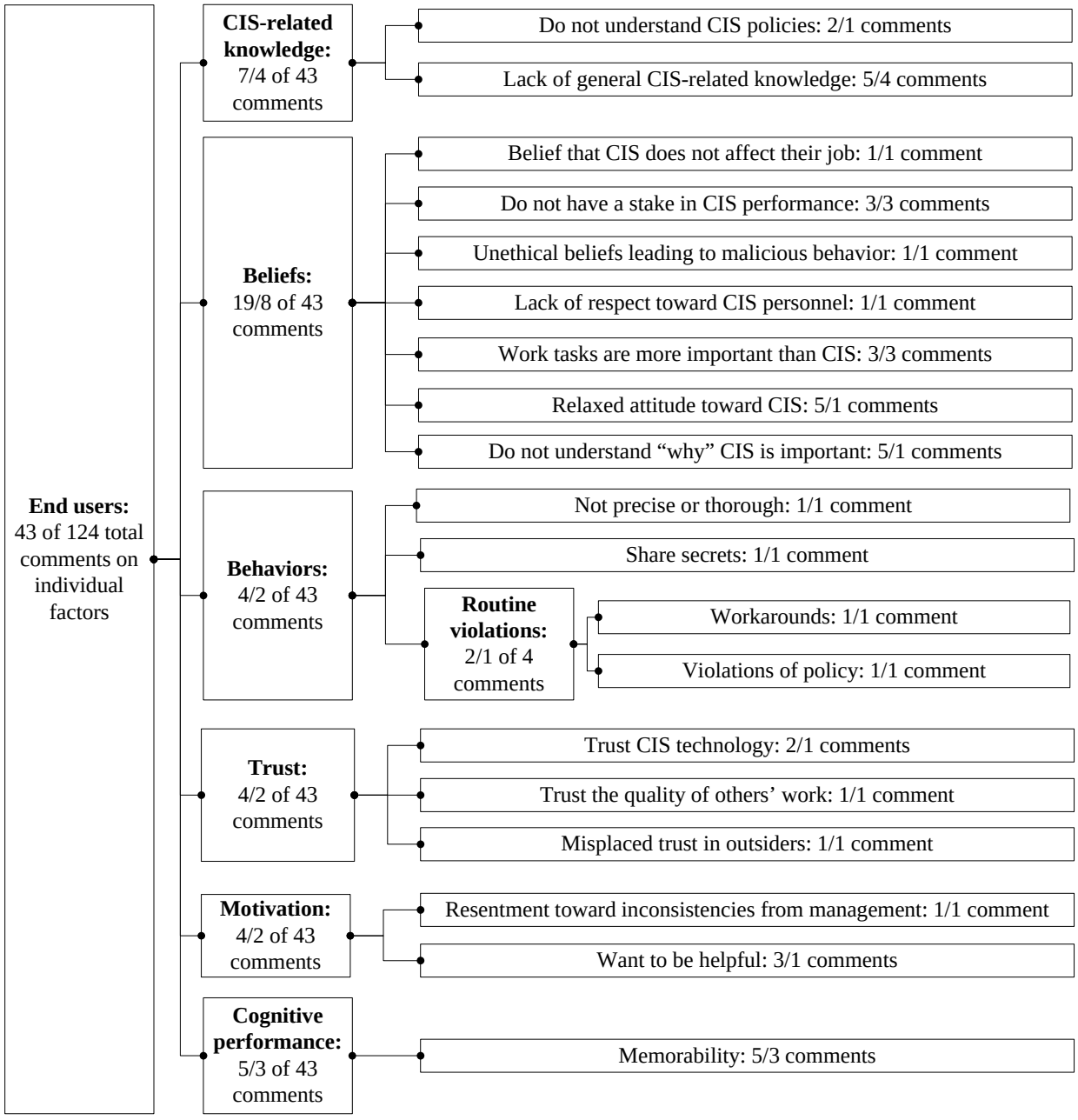
4.2.2.2.3 Behaviors, Trust, Motivation, and Cognitive Performance

There were four smaller sub-nodes in the *individual factors of end users* category: behaviors (4/2 comments and 4 sub-nodes), trust (4/2 comments and 3 sub-nodes), motivation (4/2 comments and 2 nodes), and cognitive performance (5/3 comments and 1 sub-node).

End users can be *motivated to be helpful* (3/1 comments, 1 node). One red team member expanded on how CIS is compromised when *end users are motivated by helpfulness toward others*:

> *"People want to help, and if you give them the opportunity to help without directly breaking the rules, they do everything they can to help. And I see that over and over. For example, when you call the help desk because you forgot your password, and you need it reset and you're out in the middle of nowhere, somebody's going to really want to help. And if you can just figure out a way to give them the opportunity to help you, without directly breaking the rules, they'll do it."*

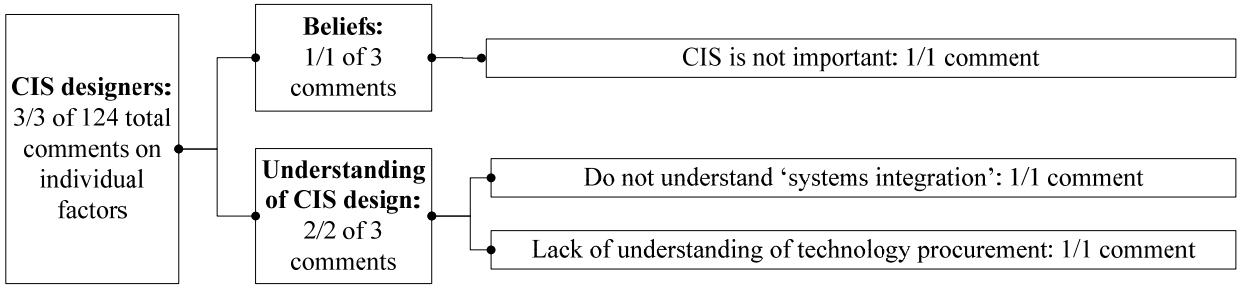
Figure 10. Quantification of Comments on Individual Factors of End Users



4.2.2.3 CIS Designers

There were 3 comments and 2 sub-nodes in the *CIS designers* category. The two sub-nodes in this category were: beliefs (1/1 comment, 1 node) and understanding of CIS design (2/2 comments, 2 nodes). Refer to Figure 11 for a summary of comments on the *individual factors of CIS designers*.

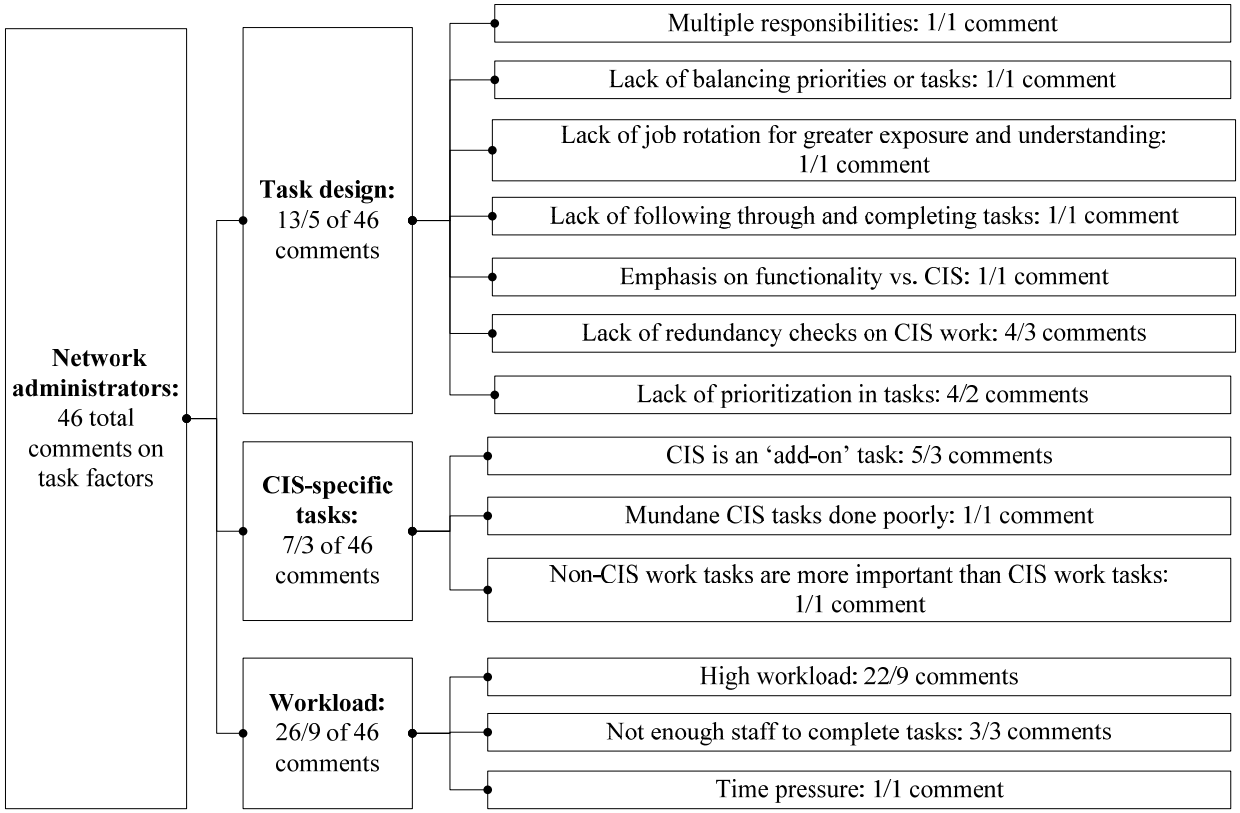
Figure 11. Quantification of Comments on Individual Factors of CIS Designers



4.2.3 Task Factors Associated with CIS

The *task factors* category was related to one group of users: network administrators. There were 46 comments and 13 sub-nodes in the *network administrator's task factors* category. The largest sub-node was workload (26/9 comments, 3 sub-nodes), followed by task design (13/5 comments, 7 sub-nodes), and CIS-specific tasks (7/3 comments, 3 sub-nodes). Refer to Figure 12 for a summary of comments related to *task factors of network administrators*. See Appendix H for definitions of task factors associated with CIS.

Figure 12. Quantification of Comments on Task Factors of Network Administrators



4.2.3.1 Task Design

The *task design* category contained 13/5 comments and 7 sub-nodes. The largest sub-nodes were: lack of redundancy checks on CIS work (4/3 comments) and lack of prioritization in tasks (4/2 comments).

4.2.3.2 CIS-Specific Tasks

The *CIS-specific tasks* category consisted of 7/3 comments and 3 sub-nodes. *CIS is an "add-on" task* was the largest sub-node (5/3 comments).

4.2.3.3 Workload

The largest sub-node in the *task factors of network administrators* category was *workload*, (26/9 comments and 3 sub-nodes). The largest sub-node was *high workload* (22/9 comments). One red team member commented:

> *"…I think people are overloaded. There's not enough time, and this is in the military and it's in the private sector. Overworked security staff leads to problems. They are often overworked because of two factors: complexity of the system with which they must address and insufficient funding."*

Another red team member expanded on [mistakes related to] *high workload*:

> *"CIS is more vulnerable because they're [network administrators] busy and [when they're over-tasked they] tend to make mistakes -- configuration mistakes primarily. Firewalls are built, but if a person [network administrator] is busy, they may not pay attention to the rules that they put in the firewall, they may just put in what they need to [make it operable]…they may not actually test it. So, there are a lot of times you can take advantage of the business and look for configuration mistakes."*

4.2.4 Technology Factors Associated with CIS

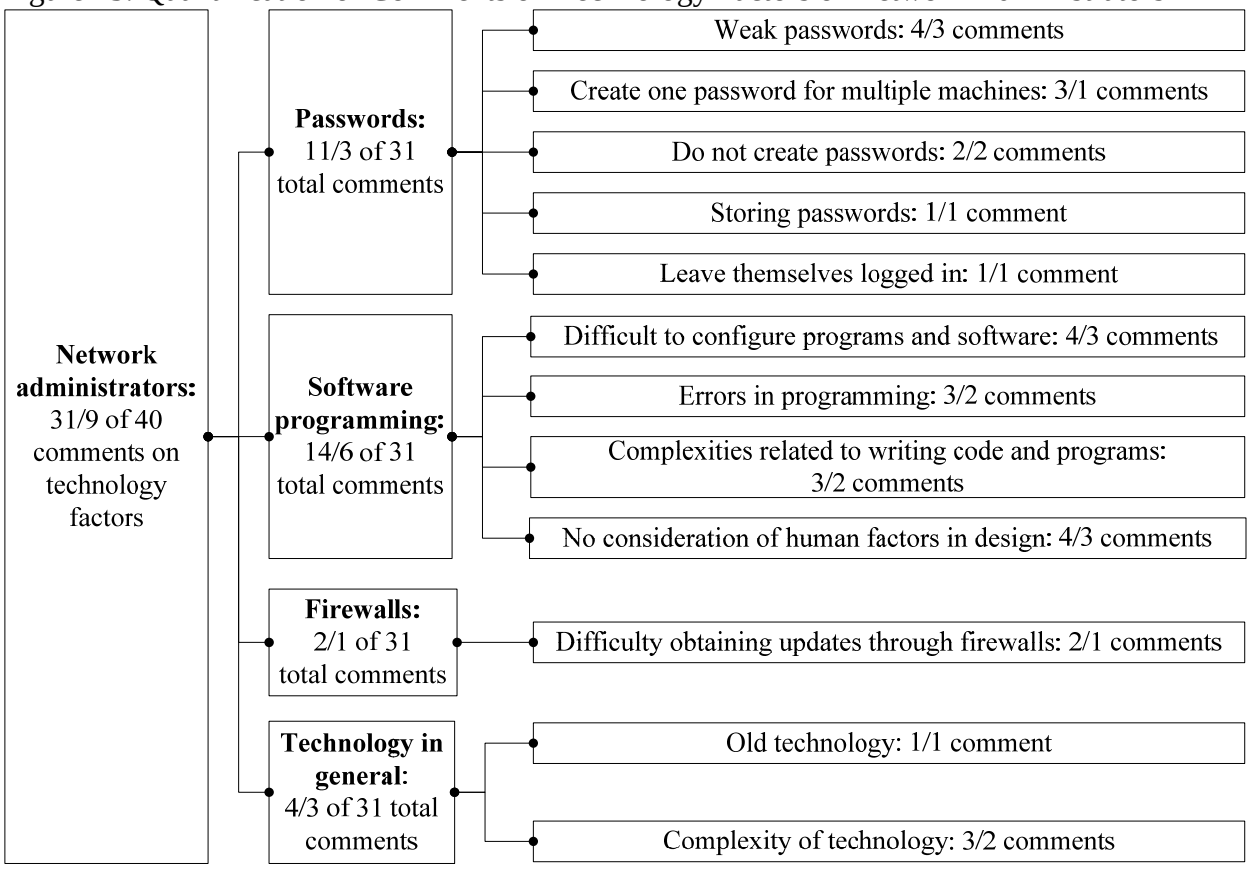
In the *technology factors associated with CIS* category (40 total comments, 16 sub-nodes), there were two groups: technology factors of network administrators (31 comments, 12 sub-nodes) and technology factors of end users (9 comments, 4 sub-nodes). Each group was reported separately. Refer to Appendix I for a set of definitions related to technology factors associated with CIS.

4.2.4.1 Network Administrators

In the *technology factors of network administrators* category (31/9 comments, 12 sub-nodes), there were four main subcategories: passwords (11/3 comments, 5 sub-nodes), software programming (14/6 comments, 4 sub-nodes), firewalls (2/1 comments, 1 sub-nodes), and

technology in general (4/3 comments, 2 sub-nodes). Refer to Figure 13 for a summary of comments on *technology factors of network administrators.*

Figure 13. Quantification of Comments on Technology Factors of Network Administrators



4.2.4.1.1 Passwords

The *passwords* category contains 11/3 comments and 5 sub-nodes. The largest sub-node was: weak passwords (4/3 comments). One red team member commented on *weak passwords*:

> *"If you remotely log in to the machine, and you type "password," they might have one that's their [network administrators] name. They [network administrators] know that is not a good password that it is not acceptable in any way shape or form, but they use it because it makes their life easier."*

4.2.4.1.2 Software Programming

There were 14/6 comments and 4 sub-nodes in the software programming node. *Difficult to configure programs and software* was the largest sub-node (4/3 comments). Removing default passwords was considered a difficulty in configuring programs and software.

4.2.4.1.3 Firewalls and Technology in General

There were two smaller sub-nodes in the *technology factors of network administrators*: firewalls (2/1 comments and 1 sub-node) and technology in general (4/3 comments and 2 sub-nodes). One

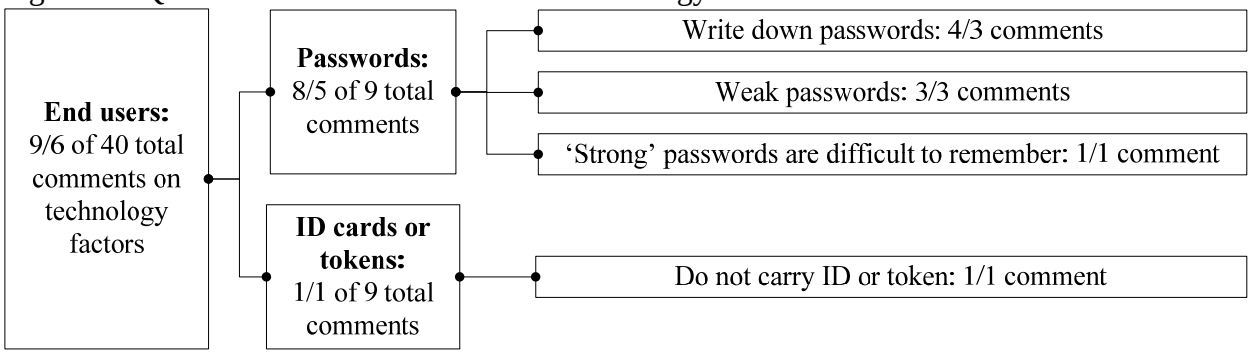
red team member commented on the common problems related to firewalls and network administrators' work:

> *"Firewalls are pretty stout. So, if I can find a way around, I will. And if I know an administrator has been having trouble getting his updates for his computer through the firewall because the proxies won't let that kind of file through, then I start looking for the backdoor network because there's going to be one. The administrator on the inside has to do something that's easy to take [advantage] of the mechanisms that are in place to get upgrades. [Also,] they have to do something that's easy for them to maintain anonymity. The only way to do that is get their own internet connection and then go out through that connection; [they] can also pick up a whole lot of other things that way too."*

4.2.4.2 End Users

There were 9/6 comments and 3 sub-nodes in the *technology factors of end users* category. The two main subcategories were: passwords (8/5 comments, 3 sub-nodes) and ID cards and tokens (1/1 comment, 1 sub-node). Refer to Figure 14 for summary of comments on *technology factors of end users*.

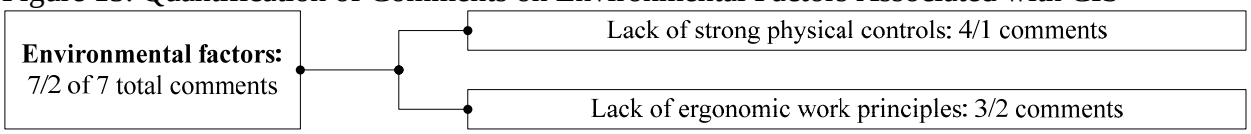
Figure 14. Quantification of Comments on Technology Factors of End Users



4.2.5 Environmental Factors Associated with CIS

The *environmental factors* category consisted of 7 comments and 2 sub-nodes. The subcategories were: lack of strong physical controls (4/1 comments) and lack of ergonomic work principles (3/2 comments). Refer to Appendix J for a complete set of definitions. Refer to Figure 15 for a summary of comments on *environmental factors associated with CIS.*

Figure 15. Quantification of Comments on Environmental Factors Associated with CIS



4.3 Human and Organizational Factors Affect on CIS Vulnerabilities

This section reports the results from two focus groups tasked with linking various human and organizational factors to specific types of CIS vulnerabilities: design, implementation, configuration, and operational. The focus groups' findings are reported separately.

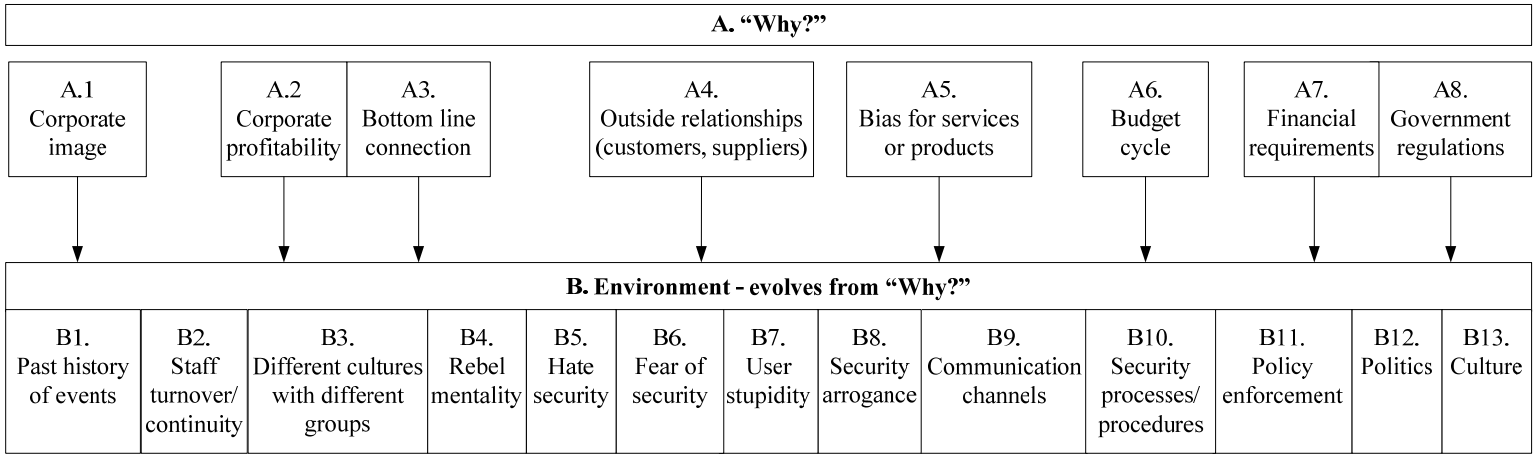
4.3.1 Focus Group #1

In focus group #1, the participants generated a flowchart linking human and organizational factors with design, implementation, configuration, and operational vulnerabilities. They also generated a number of factors that are precursors or antecedents to the development of CIS vulnerabilities. The hypothetical domain is a large, commercial organization, on the scale of a large aero-space defense contractor.

4.3.1.1 Antecedent factors

The focus group produced a set of factors that predispose the development of CIS vulnerabilities. These factors are in two groups: (1) a set of "why" factors, or factors that drive the development of the CIS environment and (2) a set of factors describing the CIS environment. Refer to Figure 16 for a summary of antecedent factors. For definitions of antecedent factors, refer to Appendix K.

Figure 16. Summary of Antecedent Factors Identified in Focus Group #1

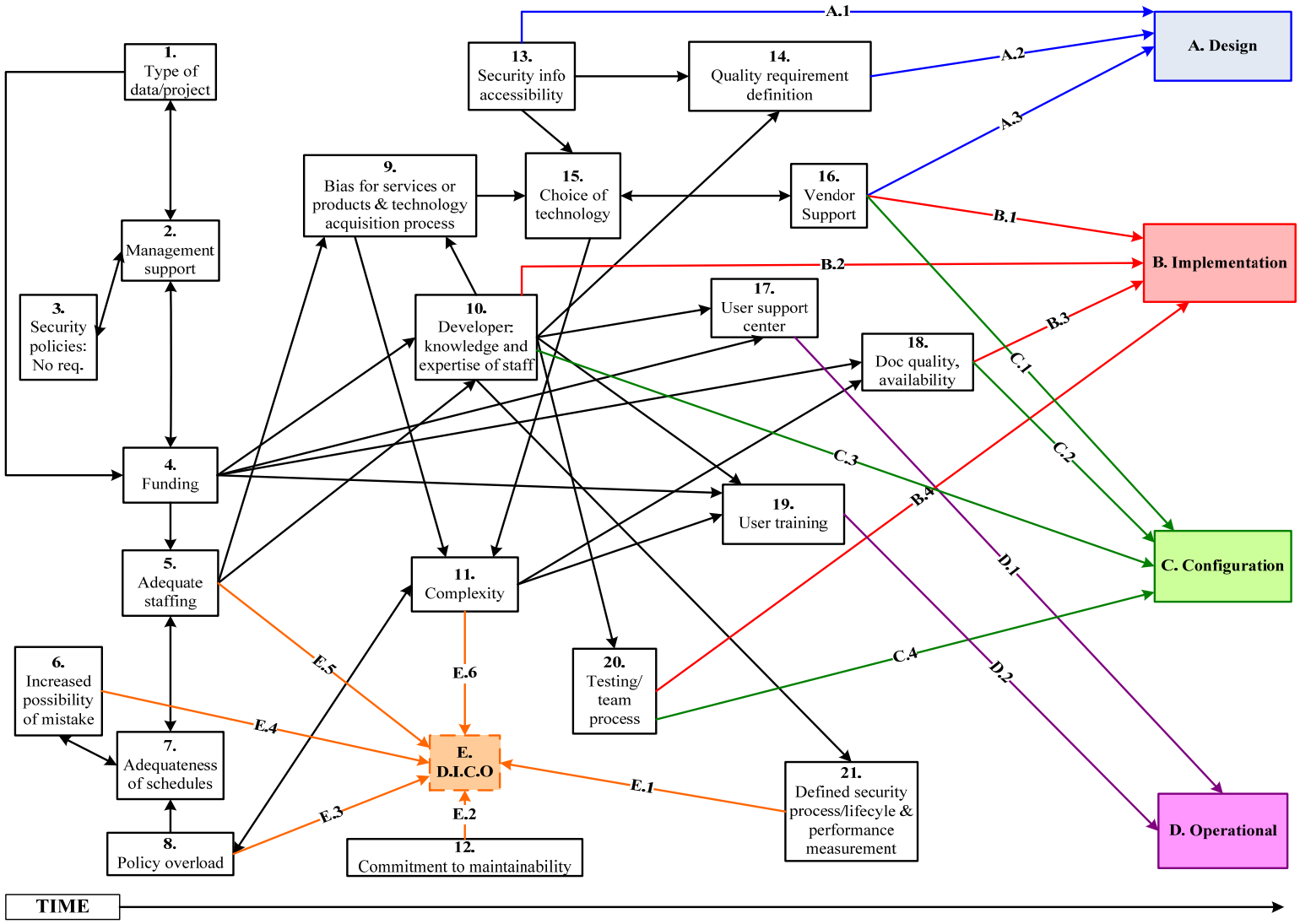


4.3.1.2 Description on Reporting Pathways

This section summarizes the pathways associated with four types of CIS vulnerabilities: design, implementation, configuration, and operational. Refer to Figure 17 for a flowchart of the various pathways associated with CIS vulnerabilities: implementation, design, and configuration (Howard and Longstaff, 1998; Howard and Meunier, 2002). A design vulnerability is inherent in the design or specification of hardware or software such that even a perfect implementation of the design would result in a technical vulnerability. Implementation vulnerabilities result from an error made in the software or hardware implementation of an otherwise satisfactory design. Configuration vulnerability results from an error in the configuration of a system, such as the use of default passwords, the lack of access control for files, or the enabling of vulnerable services. The focus group determined a fourth category of vulnerability: operational. An operational vulnerability occurs when a needed step in an operational process is undefined, missed, or performed out of order, and results in or could result in a security-related failure of the system.

The vulnerability categories are marked A-E. A *design* vulnerability is denoted by "A," an *implementation* vulnerability is "B," a *configuration* vulnerability is "C," and an *operational* vulnerability is "D." Factors leading to all four vulnerabilities, design, implementation, configuration, and operational, are marked "D.I.C.O.," and denoted by "E." For example, there are 3 pathways for the design vulnerability, which are marked A.1, A.2, and A.3. Each vulnerability category is marked in this manner. Each individual pathway is reported separately. See Appendix L for definitions of factors.

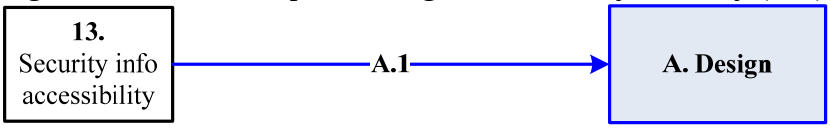
Figure 17. Focus Group #1: Flowchart of Design, Implementation, Configuration, and Operational Vulnerability Pathways



4.3.1.2.1 Vulnerability Pathways: Focus Group #1

Design vulnerability pathway A.1. Refer to Figure 18.

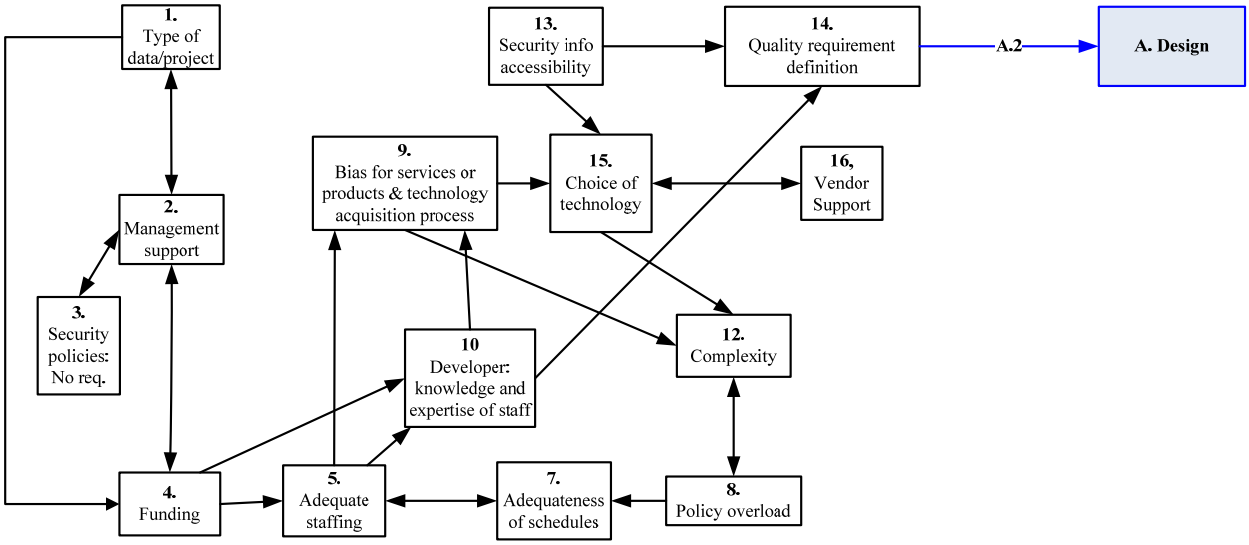
Figure 18. Focus Group #1: Design Vulnerability Pathway (A.1)



Security information accessibility (13) refers to information about the technology features that are documented and accessible from the vendor.

Design vulnerability pathway A.2. Refer to Figure 19.

Figure 19. Focus Group #1: Design Vulnerability Pathway (A.2)

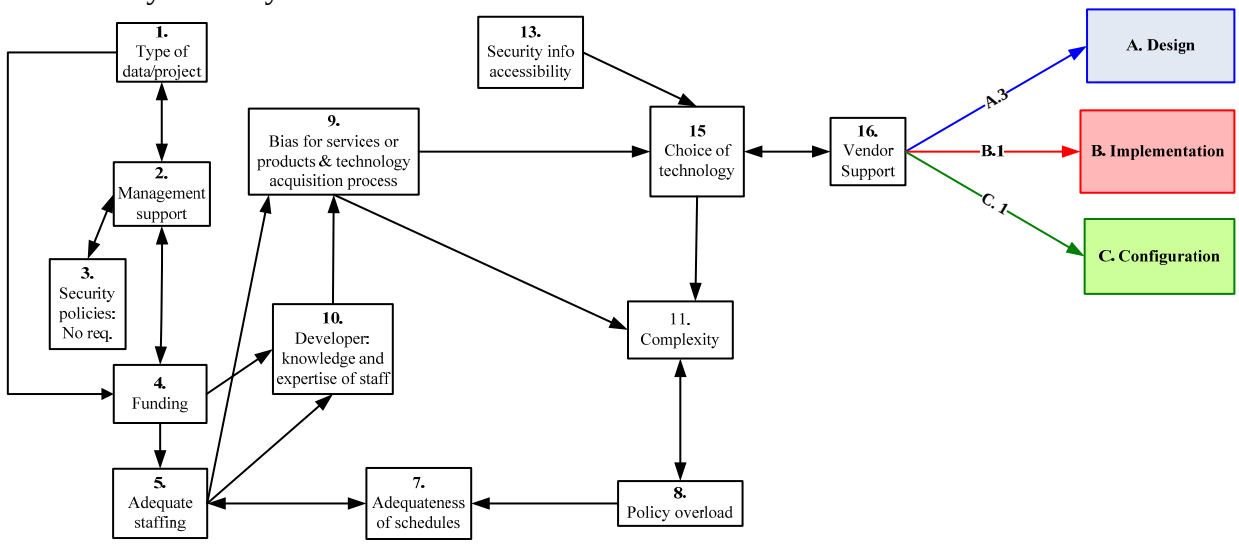


The type of data or project (1) drives the type of assets or information that is protected (e.g., high or low criticality), how much management will support CIS (2) and view the importance of the CIS protection. The type of data/project may also be related to how much funding (4) is allocated to the CIS protection of those assets. Management support is also related to how security policies are developed. For example, low management support may result in poorly specified CIS policy requirements (3). Funding (4) affects CIS staffing levels (5). The scheduling problems that emerge for CIS staff are also constrained by an overabundance of CIS policies (8), and the CIS system's interrelatedness to various CIS system complexities (12). Complexity (12) refers to interconnectedness of CIS systems with other systems or the intricacies of merging systems and is directly affected by the ease-of-use 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). Less secure products or services may not have adequate vendor support (16). An example of inadequate vendor support is not fixing bugs or not providing proper documentation for technology features (13). A lack of CIS expertise on the part of the developer and CIS staff (10)

directly affects the quality requirement definition of the system (14). Poor or incorrect quality requirement definitions may lead to design vulnerabilities (A.3).

Design vulnerability pathway A.3, Implementation vulnerability pathway B.1, and Configuration vulnerability pathway C.1. Refer to Figure 20.

Figure 20. Focus Group #1: Design (A.3), Implementation (B.1), and Configuration (C.1) Vulnerability Pathways

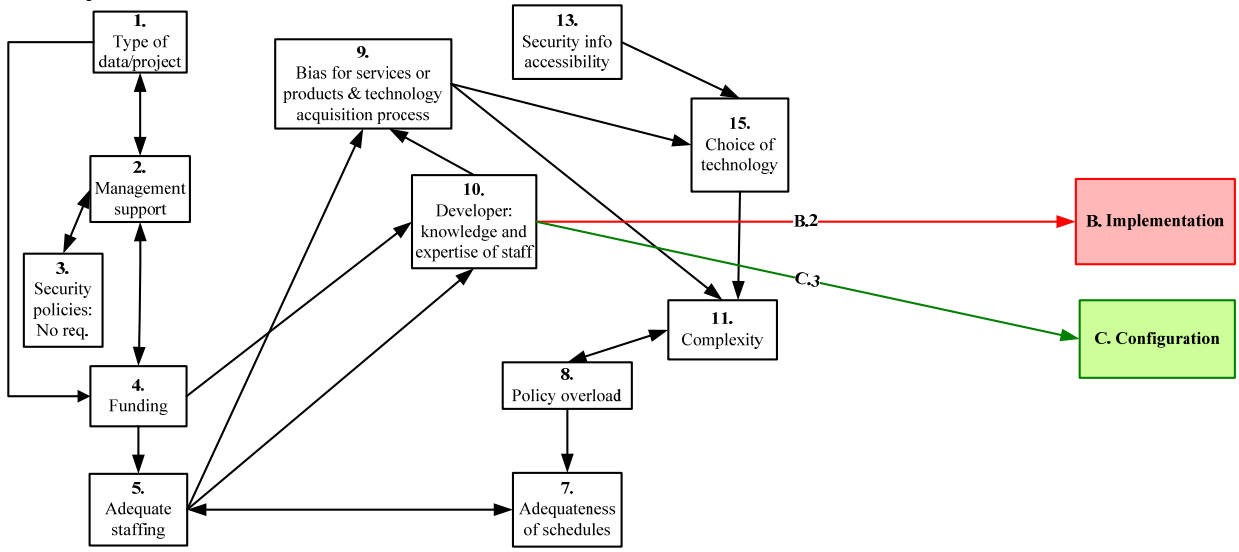


In this pathway, lack of vendor support may lead to design vulnerabilities (A.3), implementation vulnerabilities (B.1), and configuration vulnerabilities (C.1). Vendor services, products, and technologies may be less secure than other products or services (15). Examples of poor vendor support are not fixing bugs and not providing proper CIS technology documentation (13). Refer to the A.2 vulnerability pathway for a description of factors 1-5, 7-11, 13, and 15.

Design vulnerability pathway B.2 and configuration vulnerability pathway C.3. Refer to Figure 21 for a summary.

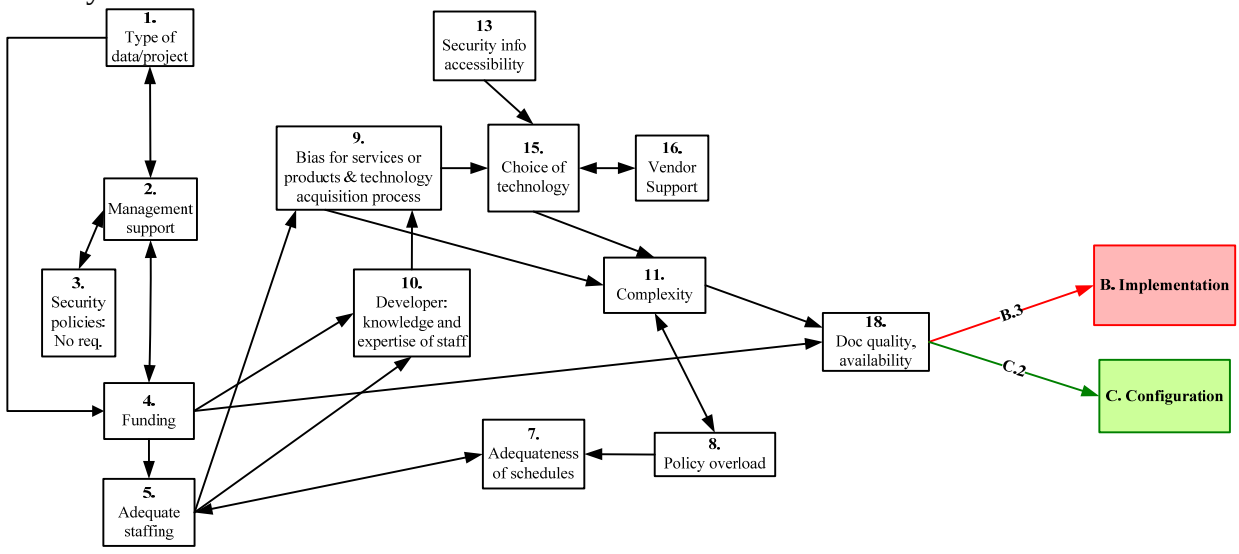
Low level of expertise by staff (10) may result in implementation (B.2) and configuration (C.3) vulnerabilities. Please refer to A.2 pathway for a description of factors 1-5, 7-11, 13, and 15.

Figure 21. Focus Group #1: Implementation (B.2) and Configuration (C.3) Vulnerability Pathways



Implementation vulnerability pathway B.3 and configuration vulnerability pathway C.2. Refer to Figure 22.

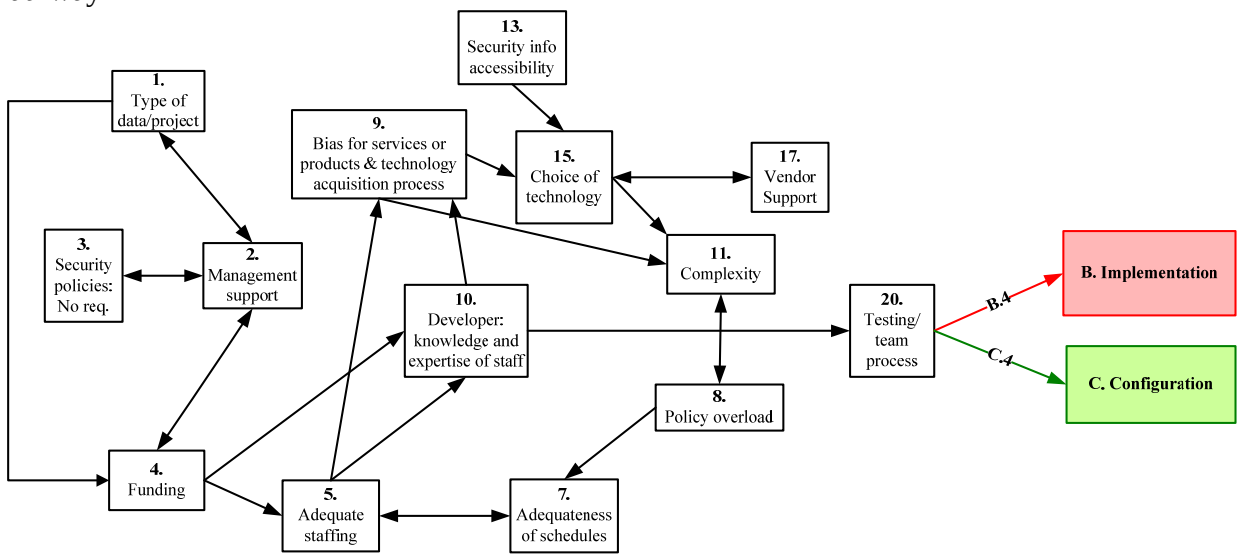
Figure 22. Focus Group #1: Implementation (B.3) and Configuration (C.2) Vulnerability Pathways



Poor CIS documentation quality and availability (18) may result in implementation vulnerabilities (B.3) and configuration vulnerabilities (C.2). Please refer to A.2 pathway for a description of factors 1-5, 7-11, 13, and 15-16.

Implementation vulnerability pathway B.4 and configuration vulnerability pathway C.4. Refer to Figure 23.

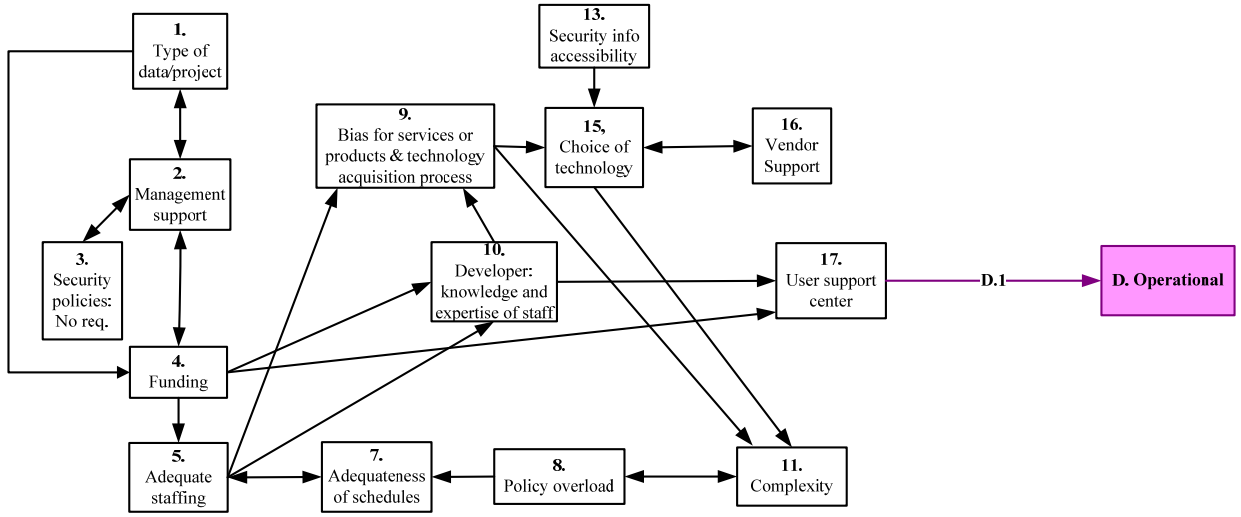
Figure 23. Focus Group #1: Implementation (B.4) and Configuration (C.4) Vulnerability Pathway



Vulnerabilities may occur when CIS systems and processes are not tested for functionality or vulnerabilities (20). If this testing is not performed correctly or not performed at all, implementation vulnerabilities (B.4) and configuration vulnerabilities (C.4) may result. Refer to A.2 pathway for a description of factors 1-5, 7-11, 13, 15, and 17.

Operational vulnerability pathway D.1. Refer to Figure 24.

Figure 24. Focus Group #1: Operational (D.1) Vulnerability Pathway

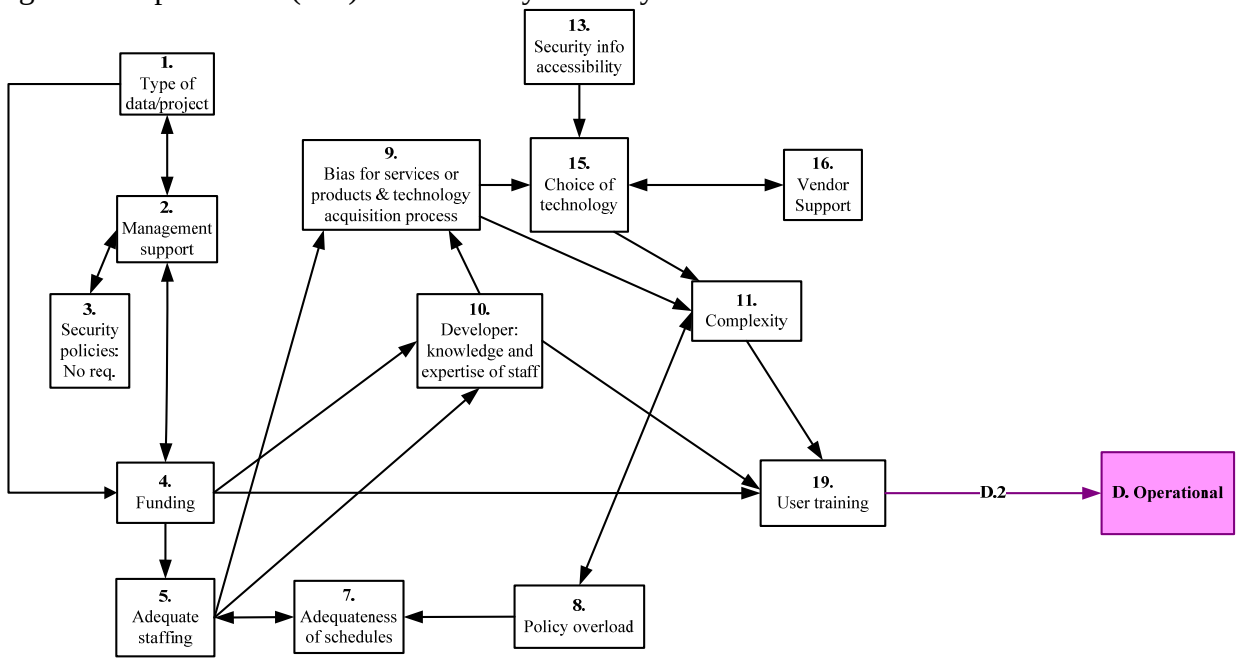


The user support center's inability to locate and remediate CIS problems may result in operational vulnerabilities (D.1). The quality of work performed by the user support center is dependent upon the staff's knowledge and expertise (10). The quality of the work performed by the user support center is also dependent upon the maturity of the center. If the user support center is mature, they may have a process for identifying and correcting CIS problems. If the

user support center is not mature, they may only correct problems identified by users. See A.2 pathway for a description of factors 1-5, 7-11, 13, and 15-16.

Operational vulnerability pathway D.2. Refer to Figure 25.

Figure 25. Operational (D.2) Vulnerability Pathway

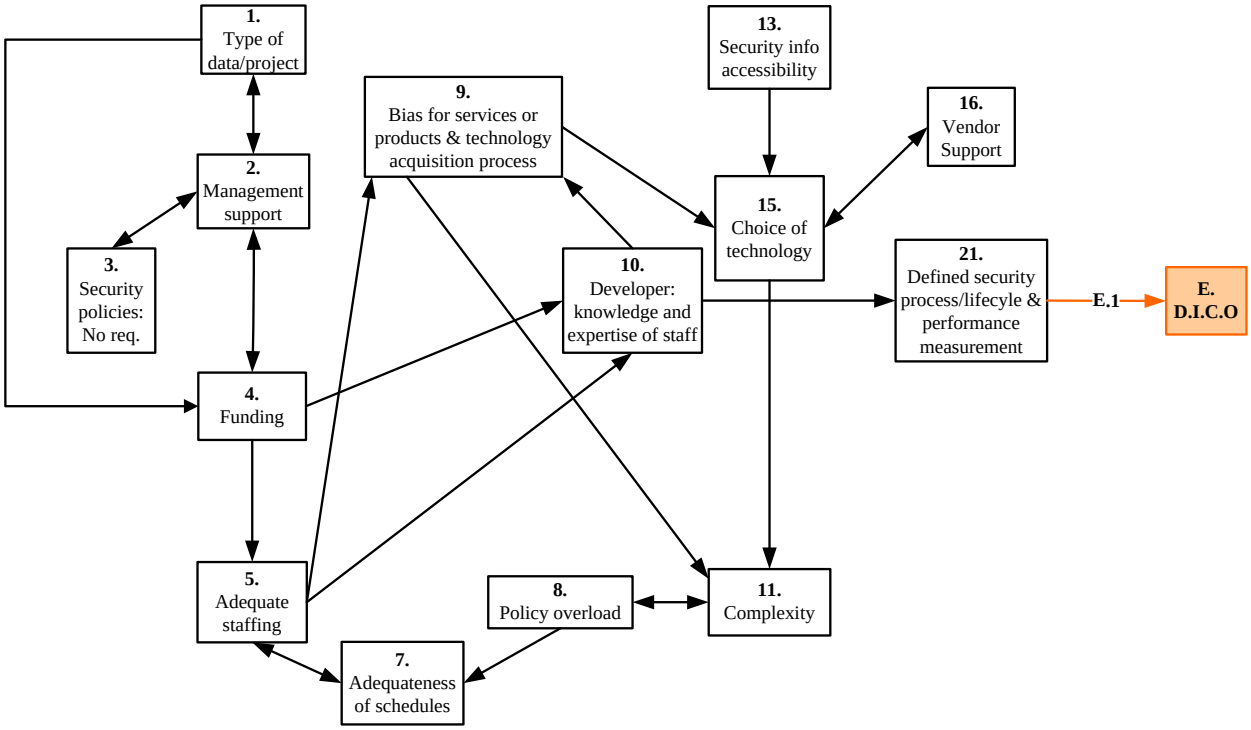


Lack of user training and time for training on CIS system complexities (11) may result in operational (D.2) vulnerabilities. Refer to A.2 pathway for a description of factors 1-5, 7-11, 13, and 15-16.

E.1- D.I.C.O. vulnerability pathways. Refer to Figure 26.

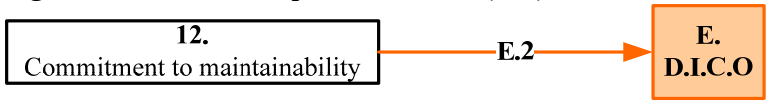
The E.1 pathway leads to all four vulnerability categories (design, implementation, configuration, and operational (D.I.C.O.). Poor quality of defined CIS processes affects the occurrence of design, implementation, configuration, and operational (E.1) vulnerabilities. Poor CIS processes include: poor maintenance of the system process, development of the system, support of the system, and the development of a defined security process for the system life cycle (21) can lead to D.I.C.O. Please refer to A.2 pathway for a description of factors 1-5, 7-11, 13, and 15-16.

Figure 26. Focus Group #1: D.I.C.O (E.1) Vulnerability Pathways



E.2 Vulnerabilities pathways D.I.C.O. Refer to Figure 27.

Figure 27. Focus Group #1: D.I.C.O. (E.2) Vulnerabilities Pathways

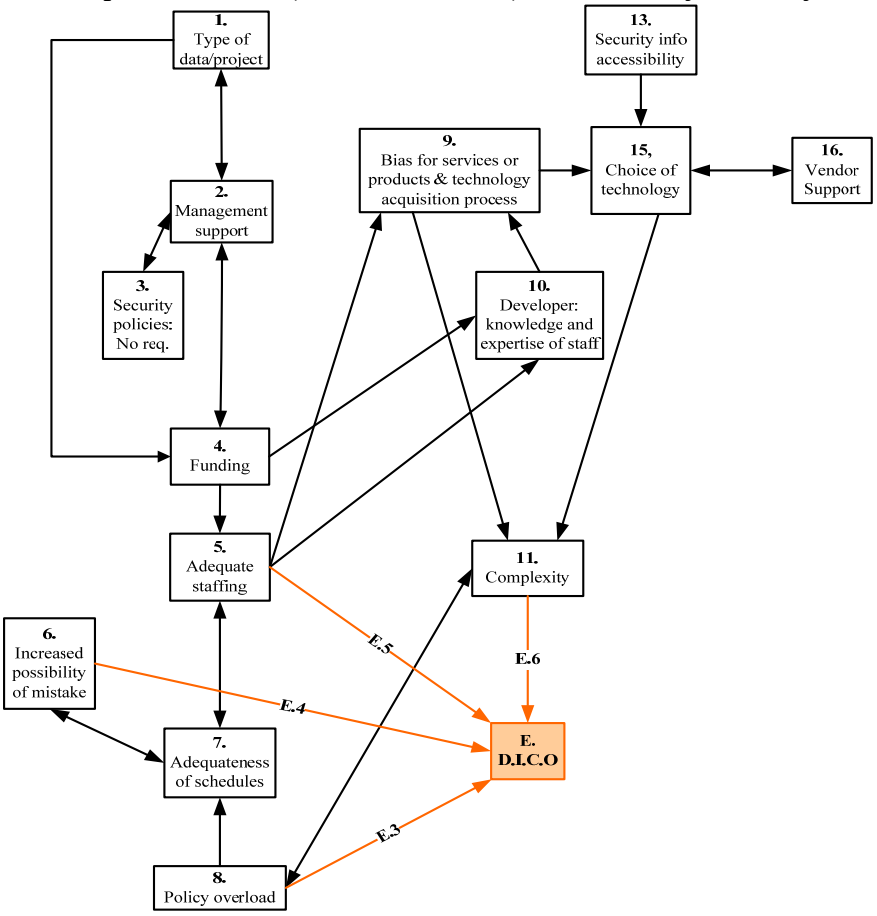


Commitment to maintainability (12) of the system is composed of many factors. The CIS staff must implement and maintain a change control process for CIS and have a maintenance process that is comprised of administration, upgrades, and failure resolution. Further, there should be a third party assessment of CIS. Lastly, a support team must be in place in order to correct CIS defects. Failure in these areas can result in D.I.C.O.

E.3, E.4, E.5, E.6 - D.I.C.O. vulnerabilities pathways are summarized in Figure 28.

This pathway leads to all four vulnerabilities (design, implementation, configuration, and operational (D.I.C.O.)). Both policy overload (E.3) and CIS complexity (E.6) can lead to CIS design, implementation, configuration, and operational vulnerabilities. Further, inadequate staffing and staff schedules (E.5) can also increase the possibilities of mistakes (6). A lack of personnel to perform the design, implementation, configuration, and operational duties can lead to vulnerabilities in those areas (E.4). CIS staff may miss important tasks or inadvertently introduce vulnerabilities into the system. Refer to A.2 pathway for a description of factors 1-5, 9-10, 13, and 15-16.

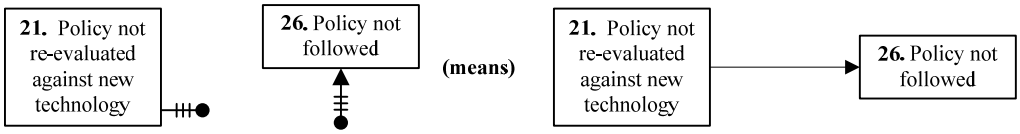
Figure 28. Focus Group #1: D.I.C.O (E.3, E.4 E.5, E.6) Vulnerability Pathways



4.3.2 Focus Group #2

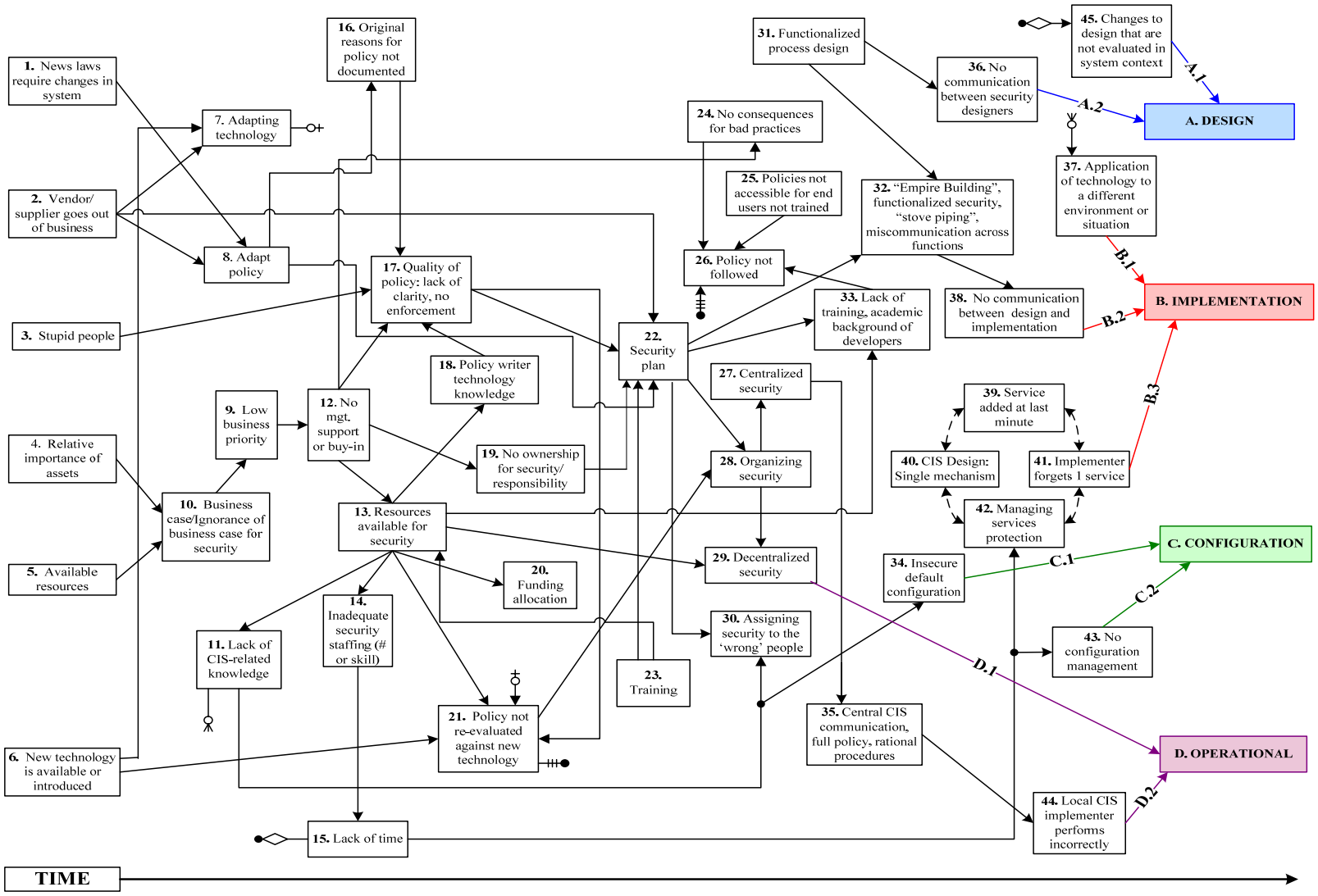
The participants in focus group #2 generated a flowchart linking human and organizational factors with design, implementation, configuration, and operational vulnerabilities. See Figure 30 for summary of focus group #2's flowchart. Special symbols in this flowchart represent a directional relationship between two factors and are not connected with a line and arrow. The purpose of these symbols is to provide a "short-hand" for denoted relationships, and limits the number of lines depicted in the flowchart. For example, see Figure 29:

Figure 29. Example of "Short-Hand" Notation for Relationships in Flowchart



Refer to Appendix M for a set of definitions of human and organizational factors identified by focus group #2.

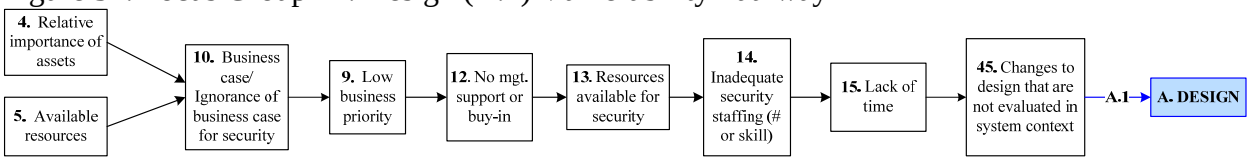
Figure 30. Focus Group #2: Flowchart of Design, Implementation, Configuration, and Operational Vulnerability Pathways



4.3.2.1 Design Vulnerability Pathways

The A.1 design vulnerability pathway is summarized in Figure 31.

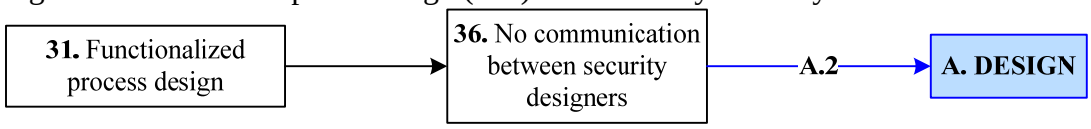
Figure 31. Focus Group #2: Design (A.1) Vulnerability Pathway



The importance of assets (4), or the assigned criticality of the protected asset, and available resources (e.g., funding, staffing) (5) contribute to creating a strong business case for CIS security (10). Without a strong business case for security, CIS becomes a low priority, relative to other aspects of the business (9) and management does not support CIS (12). The lack of buy-in and support by the management limits hiring and retaining competent and skilled CIS staff (14). The lack of appropriate staff contributes to the overall lack of time for completing CIS work (15). When changes to the CIS system occur (e.g., merging a new CIS system or performing system upgrades), it is not done in the context of the overall CIS system (45). This can result in an overall CIS system design vulnerability (A.1).

The A.2 design vulnerability pathway is summarized in Figure 32.

Figure 32. Focus Group #2: Design (A.2) Vulnerability Pathway

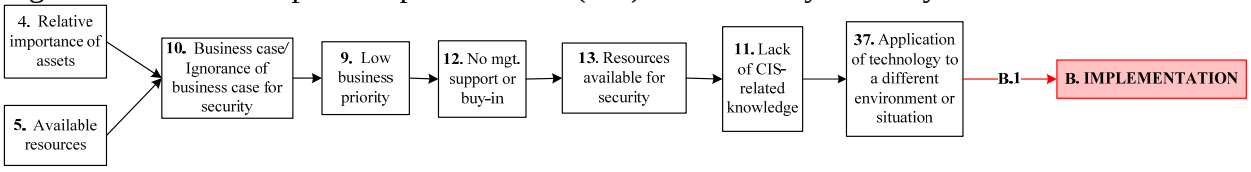


During the development of an organization's CIS process, the various aspects of the CIS process may not be harmonized to build a "system of systems." As a result, a functionalized process design (31) may develop. This occurs when one group within an organization will develop one part of the CIS design and not give or receive input on the other parts of the systems design. For example, the CIS designers of operating systems may develop their plan in isolation from the network security designers. The two groups may not communicate their design plans between each other (36), resulting in CIS design vulnerabilities (A.2).

5.3.2.2 Implementation Vulnerability Pathways

The B.1 implementation vulnerability pathway is summarized in Figure 33.

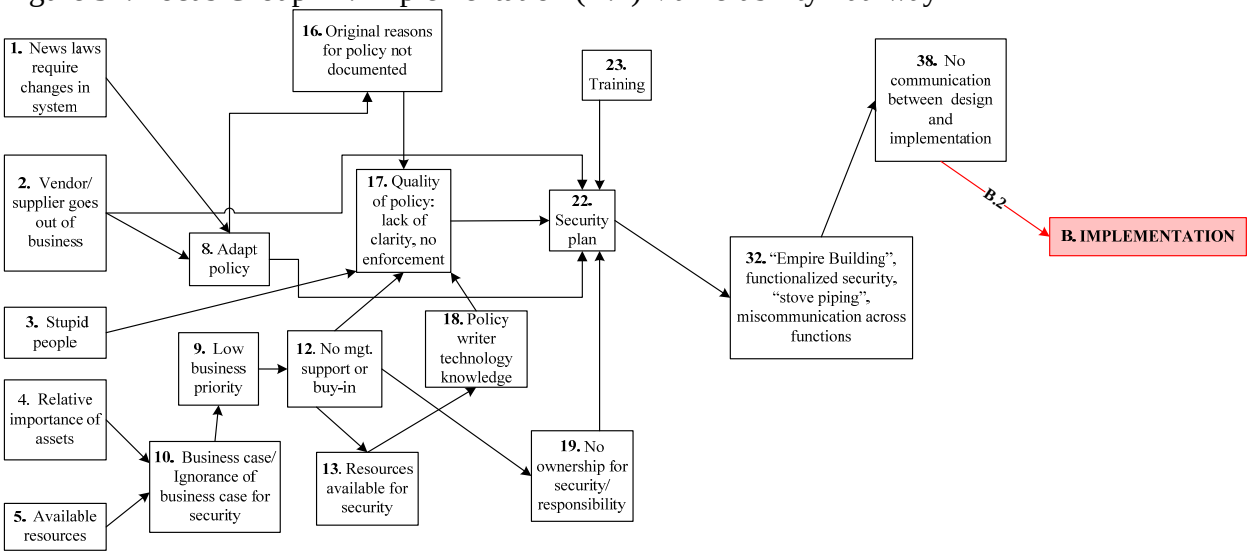
Figure 33. Focus Group #2: Implementation (B.1) Vulnerability Pathway



Implementation vulnerabilities (B.1) may occur when CIS staff lacks the experience and knowledge (11) needed to successfully implement an application in a new environment or situation (37). Refer to focus group #2's A.2 pathway for the description of factors 4, 5, 9-10, 12, 13.

The B.2 implementation vulnerability pathway is summarized in Figure 34.

Figure 34. Focus Group #2: Implementation (B.2) Vulnerability Pathway



There are two factors that contribute to the need to adapt and update CIS policy (8): new laws requiring changes in CIS system (1) and the vendor going out of business (2). Problems are introduced in the CIS policy update process when the reasons for creating the policy are not properly documented (16). This affects the overall quality of the policy (17) (e.g., lack of clarity, little enforcement) and also contributes to a weak security plan (22).

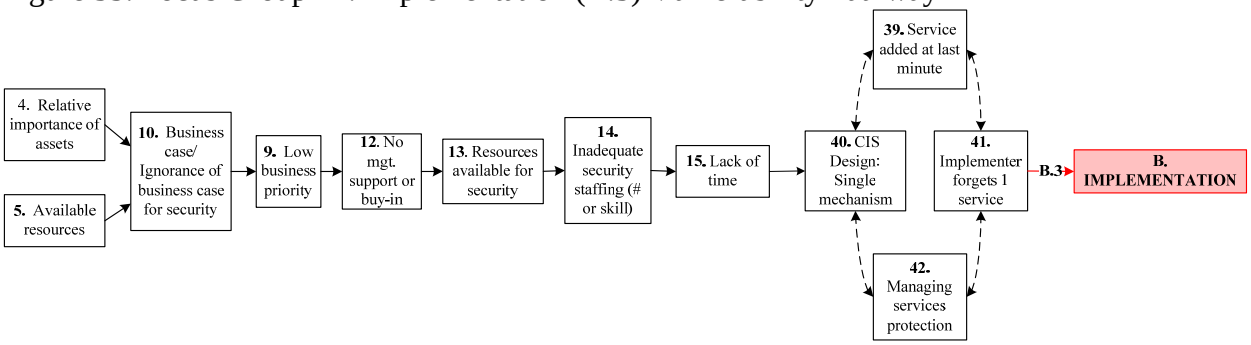
The importance of assets (4) and available resources (e.g., funding, staffing) (5) contribute to creating a strong business case for CIS security (10). A poor business case for security (10) emphasizes a low priority for CIS (11) and therefore receives little attention and resources from management (12, 13). Without financial and staff resources, it is likely that the staff creating CIS policies do not have adequate technical CIS knowledge (18). The lack of technical knowledge (18) can contribute to poor CIS policy quality (17). Further, lack of management support (12) contributes to a void for ownership or responsibility for CIS (19). Coupled with a lack of CIS training (23) these factors can contribute to poor CIS planning (22). Finally, "stupid" people (3), or CIS staff who do not have a high degree of CIS knowledge or experience, can also contribute to poor CIS policy formulation (17).

A weak security plan (22) supports "empire building" (i.e. one person or group has significantly more control than others), and functionalized security or "stove piping" (i.e. lack of integration of various components of CIS), which results in miscommunication or lack of communication across the organization (32, 38), resulting in implementation vulnerabilities (B.2). For example, improper selection of hardware based on unclear communication, incorrect sourcing of security

patches (e.g. external versus internally-supplied), and mis-ordered process steps are possible sources of implementation vulnerabilities.

The B.3 implementation vulnerability pathway is summarized in Figure 35.

Figure 35. Focus Group #2: Implementation (B.3) Vulnerability Pathway

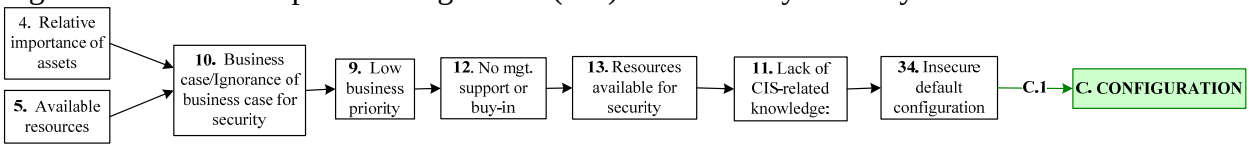


The implementer of a CIS mechanism or system may forget to implement a service (41), resulting in an implementation vulnerability (B.3). This mistake may also be related to the implementer working under time constraints (39), the service being protected by a single mechanism (40), and/or the lack of a process to manage the services protection (42). Refer to focus group #2's A.1 pathway for a description of factors 4, 5, 9, 10, and 12-15.

5.3.2.3 Configuration Vulnerability Pathways

The C.1 configuration vulnerability pathway is summarized in Figure 36.

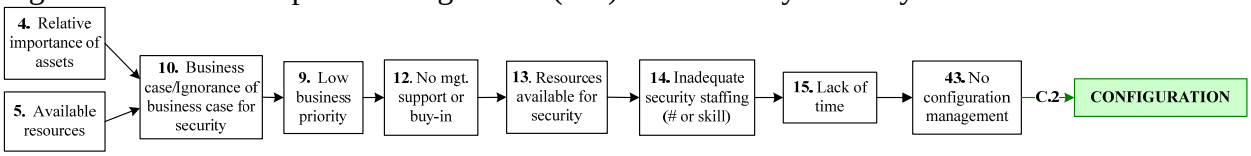
Figure 36. Focus Group #2: Configuration (C.1) Vulnerability Pathway



Faulty default configurations made by the CIS staff (34) can result in configuration vulnerabilities (C.1). Refer to focus group #2's A.1 pathway for a description of factors 4, 5, 9, 10, and 12-13.

The C.2 configuration vulnerability pathway is summarized in Figure 37.

Figure 37. Focus Group #2: Configuration (C.2) Vulnerability Pathway

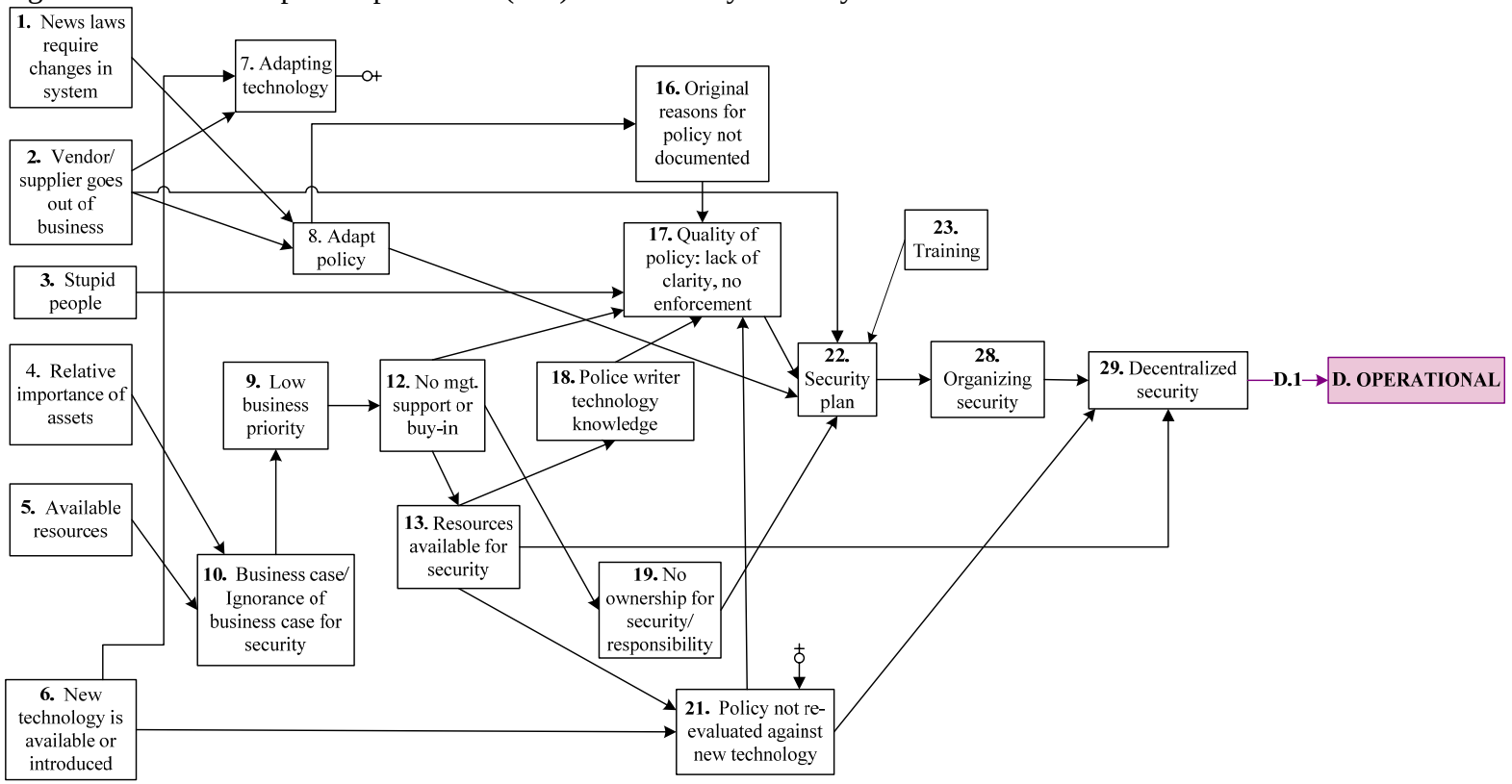


A lack of configuration management (43) can also result in configuration vulnerabilities. Refer to focus group #2's A.1 pathway for a description of factors 4, 5, 9, 10, and 12-15.

4.5.3.4 Operational Vulnerability Pathways

The D.1 operational vulnerability pathway is summarized in Figure 38.

Figure 38. Focus Group #2: Operational (D.1) Vulnerability Pathway



Operational vulnerabilities (D.1) can result from a decentralized CIS function (28, 29). Since the CIS personnel are dispersed throughout the organization, each may perform CIS duties or tasks differently. For example, a new technology should be reevaluated against the old technology's existing policy, so either can be updated or removed (7, 21). This reevaluation may or may not happen, given the distributed placement of CIS personnel. Please refer to focus group #2's B.2 pathway for descriptions of factors 1-5, 8-10, 12, 13, 16-19, 22, and 23.

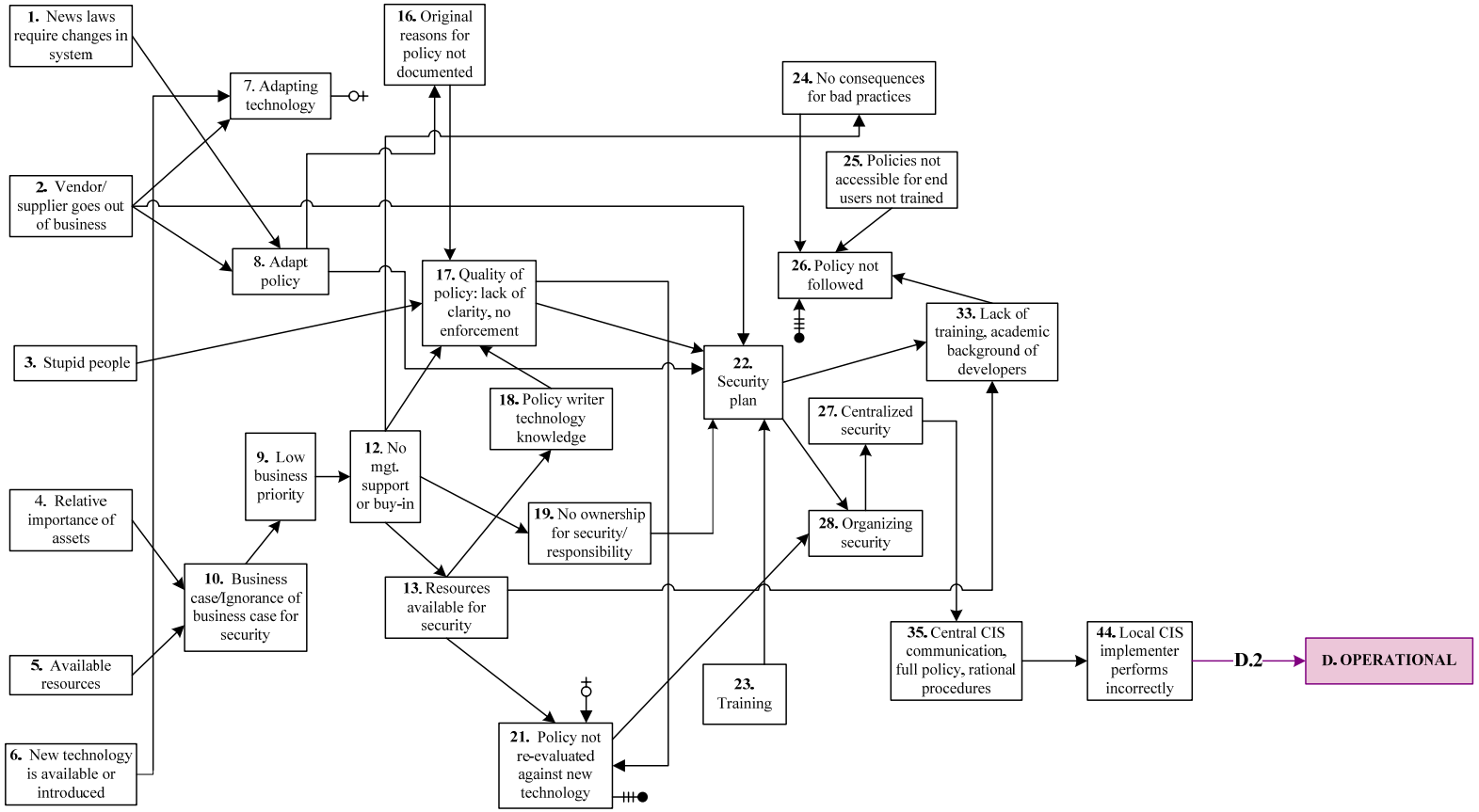
The D.2 operational vulnerability pathway is summarized in Figure 39.

There are two factors that contribute to the need to adapt and update CIS policy (8): new laws requiring changes in CIS system (1) and the vendor going out of business (2). Problems are introduced in the CIS policy update process when the reasons for creating the policy are not properly documented (16). This affects the overall quality of the CIS policy (17) (e.g. lack of clarity, little enforcement) and also contributes to a weak security plan (22). The weakened plan (22) has potential impacts on the quality of organizing security (28), for example, lack of a coherent security function (35). Without a central CIS function, communication, complete policies, and rational procedures (35), local implementers are likely to perform on-the-job errors (44) such as software configuration errors (D.2).

Information technology personnel may lack CIS-related expertise (3, 18) required to write a high-quality policy (17). In order to create a pool of CIS-related expertise and knowledge within an organization, management needs to support CIS (13), find CIS goals to be a high priority (9, 10), give CIS adequate resources (6, 13), and assign responsibility for security (19). In this case, resources and management buy-in are needed to hire and staff a team of CIS administrators and analysts, as well provide training (23) or funding for academic development (33) to them.

Problems may occur when new technology is introduced and adapted into the system (6, 7). For example, if the CIS policy is neither adapted (8) nor re-evaluated against the new technology (21), the CIS policy becomes obsolete given the new technical requirements and old operational or performance requirements (26). Further, when the policy is not adapted (8), there may not be any documentation for the consequences of bad (unsecure) practices (24). Hence, the policy is not followed. Or, the policies are not accessible for end users to train themselves or others (25).

Figure 39. Focus Group #2: Operational (D.2) Vulnerability Pathway



5. DISCUSSION

5.1 Summary of Results

This study has constructed a view of the human and organizational factors in computer and information (CIS) from an adversarial viewpoint. The "adversaries" in this study are computer analysts that simulate hackers, i.e. members of the Information Design Assurance Red Team (IDART™) program at Sandia National Laboratories. The IDART™ program conducts targeted, critical assessment of CIS systems for a diverse client base in a variety of settings.

This study has developed two areas of human and organizational factors in CIS: a taxonomy of human and organizational factors associated with CIS and a description of possible pathways leading to CIS vulnerabilities. These areas contribute to the understanding of a myriad of human and organizational factors associated with CIS while considering the entire work system in the CIS context. Previous research in CIS tends to focus solely on technical side of CIS.

A taxonomy of human and organizational factors in CIS was created in order to catalogue, specify, and define the multifarious components of CIS systems. This taxonomy also resulted in a quantification of comments made by red team members for each of the human and organizational factors of CIS taxonomy. The taxonomy is organized by the five elements of the work system model: organization, individual, technology, task, and environment (Carayon and Smith, 2000; Smith and Carayon-Sainfort, 1989).

This research study identified and characterized "pathways," or scenarios that associate various human and organizational factors with CIS technical vulnerabilities. From this effort, two "views" of human and organizational factors were created by two separate focus groups sessions. These views contain numerous pathways associated with specific types of CIS vulnerabilities (i.e. design, implementation, configuration, and operational). The scenarios also highlighted some possible temporal properties of human and organizational factors (i.e. one factor comes before the other in a sequence of events or states) as well as preliminary characterization of factors associated with specific types of CIS vulnerabilities.

5.1.1 Results Summary: Research Question #1

Interviewees provided detailed, qualitative perceptions of human and organizational factors in CIS. A quantitative assessment of comments was also performed. The coding process resulted in 592 total comments and 217 total nodes, consisting of five separate categories: organizational factors (373 comments, 130 nodes), individual factors (126 comments, 58 nodes), task factors (46 comments, 13 nodes), technology factors (40 comments, 12 nodes), and environmental factors (7 comments, 4 nodes).

There is some previous research on human and organizational factors in CIS systems (Kraemer and Carayon, 2006) using the work system model (Carayon and Smith, 2000; Smith and Carayon-Sainfort, 1989). This previous research studied perceptions of CIS managers and network administrators on human and organizational factors associated with CIS. The study of CIS managers and network administrators utilized similar questions and probes regarding human

and organizational factors associated with CIS. The coding process and data analysis of this study (identical to the process performed for Research Question #1) resulted in 236 comments in the following categories: organization (127 comments), individual (26 comments), task (47 comments), technology 22 comments), and environment (4 comments). When this current research began, there was some information on the human and organizational factors associated with CIS and it was solely from the viewpoint of CIS defenders. In this sense, the framework of human and organizational factors in CIS is now considerably expanded.

5.1.1.1 Organizational Factors Associated with CIS

The organizational factors category was the largest and most complex category of the five work system elements. The coding process for organizational factors resulted in 373 comments and 130 nodes and is comprised of three major parts: policy (112 comments, 36 nodes), culture (95 comments, 25 nodes), and elements of unsystematic CIS organization (166 comments, 69 nodes). There are possible reasons for the large set of comments in this category. The red team performs assessments that are usually at a high systems or organizational level, not at an operational or tactical level (although the red team does create systems 'views' that have operational components and they do have previous work experience in these areas).

CIS policy (112 comments) consisted of four major areas: content (48 comments), lack of procedures for writing policies (21 comments), poor guidelines or procedures (9 comments), and inadequate policy management (34) comments. In terms of policy content, imprecise policy was referred to most prolifically (13 comments) in this study, which supports earlier findings (Fullford and Doherty, 2003) in this area and indicates the need for further investigation on effective CIS policy design and implementation. The effective design and implementation of CIS policy also needs further investigation. A survey of 208 IT directors in the UK identified some of the challenges in facilitating the successful implementation of CIS policies (Fullford and Doherty, 2003). In particular, the gap between the perceived importance of each security policy success factor and the degree to which the responding organizations are successful in their adoption is disparate. However, the very low response rate (7.3%) to this survey compromises the validity of the survey results. This data suggests that organizational factors heavily influence the computer and information security of an organization. Coupled with Fullford and Doherty's (2003) analysis of organizational security policies, there are future research opportunities to investigate the contributing influences on organizational computer and information security methods, such as security policy and procedures.

The implementation, uptake, and consistent accountability for CIS policy are tied to the overall CIS culture of the organization. The red team members spoke of CIS culture (95 comments) in a variety of categories (organization-wide behaviors, 11 comments; organizational culture issues, 9 comments; overall perceptions, 14 comments; reward and recognition, 10 comments; training, 2 comments; management commitment, 49 comments). The concept of organizational culture has been applied to various functions of an organization, such as occupational safety and health (for example, Zohar, 1980).

The largest sub-node in the culture node was management commitment (49 out of 93 comments on culture). Management commitment was found to comprise two areas: (1) lack of resources for

CIS (22 comments) and lack of upper management emphasis on CIS (27 comments). Management commitment has also been found to be a key factor in safety culture studies. In Cleveland and colleagues' (1979) article on the characteristics of successful safety programs, resources allocated to safety and upper management emphasis on safety were identified as key items. This research included an evaluation and validation of results of an earlier questionnaire study, as well as expanding the knowledge of the previous findings (Cohen, Smith, and Cohen, 1975). The previous study examined 42 pairs of plants in 6 industries which were matched pairs of low and high accident rate plants to determine factors that might account for the difference in safety performance. The second study included on-site surveys of 7 pairs of the questionnaire respondents. Managers of low accident rate plants showed greater involvement in safety than those in high accident rate plants (Cleveland, Cohen, Smith, and Cohen, 1979; Smith, Cohen, Cohen, and Cleveland, 1978). Management commitment should not only be expressed through a formal policy statement, but acting as a motivator for employees by illustrating management interest is in their well-being. The previous studies on safety culture and management commitment can be extended to CIS research. Instead of mitigating safety risks and accidents, the tenets of safe organizational conditions can be applied to creating secure organizational conditions to promote lower CIS-associated risk and security breaches.

Elements of unsystematic CIS organization was the largest area in the organizational category (166 comments) and consisted of several sub-nodes: management of CIS (119 comments), CIS process (17 comments), and CIS training (30 comments). Within the management of CIS category, the red team members emphasized the lack of sustainability of CIS (30 comments). While the concept of sustainability certainly is not a new concept to the design and maintainability of CIS systems (10 comments), this data highlights the role of human factors in sustainability. For example, CIS is not considered in the design and process of workflow (2 comments), nor are there feedback mechanisms in place to remediate CIS problems (7 comments). These findings warrant further consideration investigating the role of human and organizational factors in CIS systems sustainability, as well as how work conditions and individual behaviors change over time. For example, secure behaviors could be described as migrating towards non-compliance over time. This suggests what Rasmussen (1997) describes as migration where incidents, in this case CIS vulnerabilities or breaches, are not caused by a coincidence of independent failures and human errors, but by a systematic migration of organizational behavior toward incident under the influence and pressure of various factors (i.e. economic, governmental, management). While this study did not examine human and organizational factors in terms of migration, there are implications for modeling the CIS system dynamics for improved sustainability. The concept of migrations is relevant in this discussion because it addresses the status of emergent undesirable behaviors at work (in the case where no relevant regulations have been designed, due to the absence of anticipation of such behaviors) (Polet, Vanderhaegen, Amalberti, 2003). The approach of migrations allows CIS work conditions and system performance to migrate and stabilize outside the expected secure field of use. Future work may include characterizing the features of human and organizational factors over time in the context of migrations. This would be done for the purposes of modeling the associated risks and take human and organizational factors into account in CIS design.

5.1.1.2 Individual Factors Associated with CIS

In the individual factors category (126 comments), the red team members emphasized the role of network administrators (78 comments), followed by end users (43 comments), and CIS designers (3 comments). Red team members provided numerous examples regarding the role of the network administrator in their assessments and how their work and individual traits often created opportunities to breach the CIS system. Often, network administrators are those working at an operational-level by defending the CIS system from potential attacks, which is relevant in organizations where CIS is a priority. From an adversarial perspective, organizations are vulnerable because network administrators lack the mindset of an adversary (16 comments). Often, the network administrators follow a predictable approach to administering CIS systems (6 comments), such as following a generic checklist or completing an audit of key CIS components.

The underlying beliefs of network administrators seem to evolve over time within organizations that undervalue the work of network administrators (6 comments) or do not provide any recognition of their work (10 comments, organizational factors category). Network administrators may feel "invisible" and blamed for CIS problems (1 comment); even if the problems are out of the realm of their control. Or, in conjunction with their "invisible" status, they may develop a feeling of invincibility where they are exempt from CIS standards and policies. This "cowboy" mentality may have detrimental effects on the cognitive performance and behaviors of network administrators. The lack of personal investment in their work, coupled with feelings of invisibility and invincibility, may lead to some serious compromises for CIS systems. For example, problems may arise when network administrators "cut-corners" or perform intentional routine violations (18 comments). Another example occurs when network administrators may create a single, simple password to dozens of machines, instead of maintaining individual passwords that contain alphanumeric characters and are changed frequently. Consequently, network administrators are considered "prime targets" by the red team members. One of the principles of cyber warfare is to target the entity or person in the CIS system who has the capability to provide the needed access points. Network administrators are desirable targets because they usually have the most responsibility, control, and access to technical systems of an organization.

5.1.1.3 Task Factors Associated with CIS

In the task factors category of CIS, network administrators were the only group mentioned (46 comments). Network administrators' high workload (22 comments) was the most emphasized sub-category, compared to how their tasks are designed (13 comments) or specific qualities about their tasks (7 comments), such as the tasks related to CIS that are usually an afterthought or are "add-on" (5 comments). This is consistent with the research findings of Kraemer and Carayon's (2006) study of network administrators' and CIS managers' perceptions of human and organizational factors in CIS. The findings of this study also emphasized the occurrence of high workload, especially the issue of patch management. The high number of responses in the task category may reflect network administrators' burdened work schedule. This study also highlighted numerous error examples of network administrators and how they connected to managing their CIS-related tasks (e.g., patch management, vulnerability monitoring, vulnerability testing). A lot of network vulnerabilities existed because network administrators did

not have the staff capability to fully monitor and manage every aspect of the network and its related vulnerabilities.

5.1.1.4 Technology Factors Associated with CIS

Network administrators continue to play a large role in the technology factors category (31 of 40 comments) and were emphasized over end users' technology factors (9 of 40 comments). Both groups have problems with passwords, although with varying effects on performance. For network administrators (11 comments), password management of numerous passwords (40 or more passwords by the observation of red team members) is difficult. Creating weak passwords (4 comments), a single password for multiple machines (3 comments), or lack of passwords (2 comments) were some of the more common problems. On the end user side, simple, weak passwords were an occurrence (3 comments). Or, end users may write down the password (1 comment). However, the implications are different for each group. Network administrators are the red team's "prime targets" because network administrators hold high levels of access and control and they have the ability to make the CIS system more vulnerable than end users do. Further, the vulnerabilities introduced by each of these groups are different depending on the adversary type (e.g., insider versus outsider adversary). For end users, writing down a password is a vulnerability for insider threats. Network administrators who do not use passwords or create a simple password for multiple entry points or machines are serious vulnerabilities for both insider and outsider threats (i.e. those accessing the network from remote locations). This problem is extended when network administrators weaken firewalls or create other entry points to the Internet when it is difficult to obtain updates and software through strong firewalls (2 comments).

5.1.2 Results Summary: Research Question #2

The focus groups created numerous scenarios by linking various human and organizational factors to specific types of CIS vulnerabilities: design, implementation, configuration, and operational. The two groups tended to focus their scenarios on how organizational factors affected different types of CIS vulnerabilities. One reason for this tendency may be that the vulnerability categories of design, implementation, configuration, and operational are broader category types than the more specific taxonomy of location, genesis, or time of introduction vulnerabilities as proposed by Landwehr and colleagues (1994).

Each focus group reached their goal differently. The first focus group depicted a "larger" representation of the relationships among CIS factors and vulnerabilities (i.e. more pathways, less mediating factors) while the second focus group was more specific in reaching their goal. The second focus group created a smaller number of pathways but a higher number of mediating factors than the first group.

5.1.2.1 Antecedent Factors

There are similar antecedent factors between focus groups #1 and #2. Antecedent factors are those factors that occur in the first phase in the temporal sequence of events and states leading to CIS vulnerabilities. In addition, focus group #1 summarized a host of factors that were not

included in the scenario graph (please refer to Figure 22). The consistencies between the two focus groups in antecedent factors are: government regulations and new laws, outside relationships and vendor supplier issues (such as customer perception of CIS or vendor going out of service), available resources (funding, staffing, personnel schedules), the level of criticality assigned to assets that need to be protected, "stupid" people or "user stupidity," and policy overload and enforcement.

There are some differences between focus group #1 and #2's view of antecedent factors. Overall, focus group #1 identified more antecedent factors than focus group #2. Focus group #1 identified a host of environmental and cultural factors that play a role in the performance of CIS, but are not necessarily specific factors in various scenarios of CIS vulnerabilities (refer to Figure 22). Some of these factors associated with CIS problems are: corporate image, corporate profitability, bottom line connection, bias for products and services, budget cycle, and financial requirements. The environmental or cultural factors include: the past history of events, staff turnover and continuity, different culture with different groups, a "rebel" mentality, hate of security, fear of security, security arrogance, communication channels, security processes and procedures, politics, and overall culture. For definitions of these factors, refer to Appendices K-M.

Specific combinations of antecedent factors appeared in almost every pathway identified in focus groups #1 and #2. For focus group #1, the following combination of antecedent factors appeared in every pathway: type of project or support (1), management support (2), no requirements for security policies (3), and funding (4) (refer to Figures 24-34). A dyad of antecedent factors appeared in all but one pathway (Figure 37) identified by focus group #2: relative importance of assets (4) and available resources (5) (refer to Figures 36 and 38-45).

5.1.2.2 Mediating Factors

The focus groups identified a number of mediating factors that occurred in various events or states within a CIS system. There were some similarities between the groups. These similarities occurred at the near left of each flowchart and included: complexity of CIS systems, developer knowledge and expertise, testing and team process, user training and support, and defined security process and plan.

There were more differences than similarities between the mediating factors identified by the focus groups. As a whole, focus group #1 identified less mediating factors than focus group #2, but more relationships among the factors. Conversely, focus group #2 identified more mediating factors, but fewer relationships among the factors. That is, focus group #1 created more pathways or scenarios than focus group #2. Consequently, the factors and relationship patterns tended to repeat within each vulnerability scenario in focus group #1's flowchart. Further, focus group #2's mediating factors were more specific than focus group #1. For example, focus group #2 identified a set of issues related to policy: policy evaluation, quality of policy, lack of clarity, technical skills of policy writer, policies not accessible to personnel, and policy not followed, while focus group #1 identified policy overload as a factor.

There were also differences in the types of mediating factors. As a whole, focus group #2's flowchart of human and organizational factors was more process oriented. These factors are

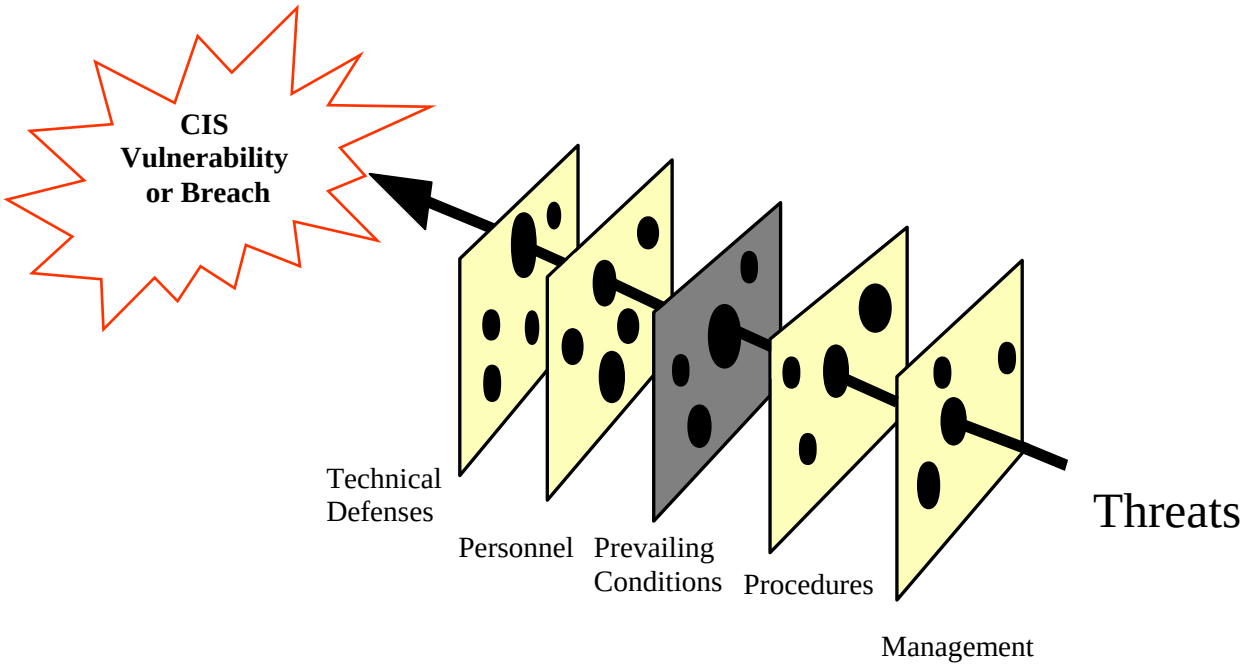
those associated with the processes related to CIS policy, the function of CIS, ownership and management of CIS, and communication. Focus group #2 also included some specific mistakes that occur, such as incorrect implementation, and insecure default configuration, and forgetting to implement a service.

The mediating factors identified by focus group #1 tended to describe larger system issues (refer to Figure 24). The large system issues were: type of technology (9, 15), the concepts of complexity (12) and maintainability (12), and lifecycle issues and performance measurement (21). Focus group #1 did identify some specific factors, such as training and team process (19, 20), vendor support (19), and security information accessibility (13).

5.1.2.3 Latent Organizational Conditions and Active Failures

The focus groups, as well as the individual interviews, revealed an emphasis on the multitude of organizational factors affecting CIS performance. Organizational factors (e.g., training, management, policy development) play a key role in a systems approach to creating the various layers of defense. On the other hand, these layers may become the conditions that set the stage for active failures resulting in CIS vulnerabilities or breaches (Brostoff and Sasse, 2001). In a perfect scenario, each defense layer would be intact. In reality, they are more like slices of Swiss cheese, having many holes. Reason (1997; 1990) described the concept of the layers of latent organizational failures as slices of Swiss cheese with holes that are continually opening, shutting, and shifting their location (see Figure 40). The presence of holes in any one “slice” does not normally line up to a bad outcome (Reason, 2000). Usually, this can only happen when the holes in many layers line up momentarily to permit a trajectory of accident (in this case, vulnerability) opportunity, bringing vulnerabilities into damaging contact with hackers.

Figure 40. The Swiss Cheese Model of Computer and Information Security (adapted from Reason, 2000)



Active failures are unsecure acts committed by people who are in direct contact with the CIS system. Active failures have a direct and usually a short-lived impact on CIS defenses. These acts can come in different forms, such as human error or intentional violations. 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 discussed below, such acts have a causal history that extends through many levels of the organization and system.

The latent organizational conditions arise from decisions made by management, designers, policy writers, and procedure creators. The latent conditions can have two kinds of an adverse affect: 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 lay dormant for a long 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 an adverse event occurs (see Operational Guidelines for Human and Organizational Factors of CIS, Section 6.2.2.1 and Appendix N).

5.2 Contributions

This research makes a number of contributions to the fields of human factors engineering and computer and information security.

5.2.1 Theoretical Contributions

5.2.1.1 Human Factors Engineering

This research proposes a framework of the human and organizational factors that are precursors to various types of CIS vulnerabilities. It initiates a first step toward modeling a CIS system by not just decomposing its work system elements, but towards developing a description of the dynamic behavior of system and its actors (i.e. end users, network administrators) by a decomposition of the behavioral flow into events, such as CIS vulnerabilities and breaches (see Section 5.1.1.1 comments on migrations).

Additionally, this work presents an integrated framework of factors and relationships, as well as a rich set of descriptions that provide context. Some research has examined human and organizational factors and CIS (Kraemer and Carayon, 2006, re-submitted), but most research focused on a specific problem or set of problems. Further, the complexities of relationships between and among human and organizational factors and its impact on CIS performance (i.e. occurrence of CIS vulnerabilities) have not been fully examined. For example, Adams and Sasse's (1999) qualitative analysis of semi-structured in-depth interviews with 30 users in two companies, highlighted several human factors and organizational issues affecting password-related behaviors, including the importance of compatibility between work practices and password procedures. For example, in one 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. This is *one* study examining a *few* relationships between human and organizational factors and CIS. In this sense, the current study has expanded the understanding of human and organizational factors in CIS. The rich set of details provided here can be used as a foundation for future research in a number of ways (see section 6.4).

While addressing CIS problems from a purely technical viewpoint yields positive impacts on CIS, this work emphasizes that a range of human and organizational factors should be considered to improve *the overall performance* of CIS. For example, to enhance and support the performance of network administrators, a multi-layered approach is needed. Not only must management deem CIS important, but it also needs to give adequate resources to the network administrator function (e.g., scheduling, staffing, and training to build expertise) as well as positive recognition and rewards for network administrators' work. In this new capacity, the limitations of the current technology should be emphasized, not the limitations of the network administrators. Problems associated with passwords were emphasized by red team members (i.e. managing long lists of hard passwords, difficulties remembering strong passwords). These limitations are not inherent to network administrator capabilities, but rather demonstrate the lack of fit between current technology and organizational and individual constraints.

The approach outlined in this study has not been applied in past research on human and organizational factors associated with CIS vulnerabilities. Rather, a piecemeal approach has been

emphasized in which one human or organizational factor is examined in relation to overall CIS (Adams, Sasse, and Lunt, 1997; 1998, Whitten and Tygar, 1998; 1999). Further, the domain of CIS vulnerabilities is large and groups of vulnerabilities may be associated with specific human and organizational factors. Past research has considered specific human or organizational factors and CIS, but this research attempts to address specific human and organizational factors associated with specific types of vulnerabilities.

Designers and administrators may be able to create more comprehensive methods and frameworks to remediate CIS vulnerabilities with this study's approach. For example, the study done by Adams and Sasse (1999) demonstrated a lack of fit between passwords and organizational factors. Individual employees had their own passwords, but the organization required employees to work in teams and share computing resources. In general, many employees may share offices, share workstations, or do not have secure access to their office or environment. The physical environment means employees will have to keep their passwords, in a secure, locked place, or will have to remember their passwords. Finally, this research addresses the interrelatedness of various human and organizational factors. For example, high workload for network administrators results from a myriad of human and organizational factors: management commitment, network administrators' perception of their value and job, and the limitations of current technology (e.g., firewalls, updates, passwords).

In sum, this research has contributed to the field of human factors engineering in the following ways: (1) demonstrated a confirmation of the presence of organizational conditions contributing to CIS vulnerabilities and breaches (e.g., Swiss cheese model of Reason, 1997; 1990); (2) provided a more systematic view of human and organizational factors in CIS than has been previously examined in CIS research by human factors engineering; and (3) made parallels between the fields of safety and accident prevention and analysis and computer and information security and vulnerability and security breach prevention.

5.2.1.2 Computer Security

The main contribution of this research to the field of computer security is that numerous non-technical factors affect the performance of CIS performance (see Section 5.1.2.3 on "latent conditions"). This work systems approach used in this study is different than current approaches for CIS problems, vulnerabilities, and breaches, which tend to focus only CIS technologies and not the CIS system as a whole. This research also presents a novel approach to assessing vulnerabilities or weaknesses in security systems, like using an adversarial (i.e. red team) analysis of human and organizational factors in CIS. This research builds from previous research examining the defenders' viewpoint of human and organizational factors in CIS (Kraemer and Carayon, 2006). In the security managers' and network administrators' perception of human and organizational factors, respondents also commented on types of errors committed by network administrators and end users (Kraemer and Carayon, 2006). Network administrators tended to view errors created by end users as more intentional than unintentional, while errors created by network administrators as more unintentional than intentional. Compared to the comments of the red team on the issue of network administrators and errors, network administrators tend to take "short-cuts" and intentionally violate protocol and procedures. Red team members also commented on end user errors, which tended to be unintentional in nature, largely due to a lack

of expertise and understanding of CIS. These discrepancies reveal some possible misperceptions within the CIS community, further emphasizing that technical controls are not sufficient protection against attackers if there is not an organizational control of those working in the CIS. For example, future research could examine the password-related behaviors and usage of network administrators (as apposed to end users) in the context of the organizational environment, highlighting the fit or misfit between password-related behaviors and the constraints in the working environment.

The study of security managers' and network administrators' perceptions of human and organizational factors also found that organizational factors, such as communication, security culture, policy, and organizational structure, were the most frequently cited factors associated with CIS (Kraemer and Carayon, 2006). This information is relevant to computer sciences because CIS design, maintenance, and development can be enhanced with a richer understanding of how humans and organizations interface with technological systems.

The members of the IDART™ program emphasized that people are the greatest weakness in the CIS system, echoing similar messages that human factors are CIS's "weakest link." However, this assertion is not given as much attention from the computer security research community, because remedies for CIS vulnerabilities and breaches tend to focus on technical mechanisms, e.g., stronger firewalls and implementation of encryption. 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. Adversaries are able to thwart technical controls by exploiting some of the human and organizational factors associated with CIS systems.

5.2.2 Practical Contributions

5.2.2.1 Operational Guidelines for Human and Organizational Factors in CIS

A similar approach was taken with CIS systems using the information obtained in this study. A set of operational guidelines was developed. This set of operational guidelines can be used as a diagnostic tool for CIS defenders (i.e. network administrators, CIS managers, top-level management) to assess the human and organizational factors in their CIS systems. The guidelines can provide a starting point to improving those factors.

The guidelines were developed using the lowest-level sub-nodes and definitions created in Research Question #1. Similar nodes were combined in order to summarize the principle of a guideline. A total of 8 categories of guidelines were developed, which resulted in 63 specific operational guidelines for human and organizational factors in CIS. See Appendix N for a complete set of specific guidelines and corresponding sub-nodes. The main categories for operational guidelines are:

1. Develop comprehensive CIS policies and a policy management plan (10 specific guidelines).
2. Cultivate and maintain a CIS culture (12 specific guidelines).
3. Create and manage systematized CIS (10 specific guidelines).

4. Create CIS sustainability with human and organizational factors (7 specific guidelines).
5. Systematically organize the CIS function within a company (9 specific guidelines).
6. Develop CIS training and a training management program (5 specific guidelines).
7. Support network administrators (6 specific guidelines).
8. Support end users (4 specific guidelines).

5.2.2.2 Human Factors and Organizational Factors "View" for Red Teaming Methodology

This concept is a novel approach for red teaming of CIS systems. Current red teaming approaches do not explicitly consider the role of human and organizational factors in CIS. The framework presented in this research can be used to develop the roles of human and organizational factors in red teaming approaches and methodologies. This information can be used to create better feedback to organizations under the assessment of the red team.

The approach used in this research can be adopted into the red team assessment methodology. During data collection and assessment, the red team can use the tree graphs as a "check-list" for assessing whether factors are present or not. In their attack-formulation stage, the methods applied in the focus group could be used to create a "human and organizational view" or attack vectors of human and organizational factors. The red team could also use a hybrid approach, integrating human and organizational factors into other system views (e.g., system, functional/logical, physical/spatial, temporal, lifecycle, and consequence-based views). For example, during assessments, the red team may characterize the system by its networks. The information provided in this study on the human and organizational factors related to network usage (e.g., monitoring firewalls, patch management, user accounts) could be linked or mapped to the technical view of networks vulnerabilities.

5.3 Limitations

There are several limitations to this study. The sample of this study is one 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.
The IDART™ program is different from other red team programs in several ways: (1) the IDART™ program can assemble multi-disciplinary teams that exist within a multi-program National Laboratory including those with a heterogeneous composition; (2) the IDART™ program has multiple approaches to red teaming, called a spectrum of assessments (Sandia National Laboratories, 2005), while other red teams tend to have a single customer, a single environment in which they red team, and a single process that they follow; (3) the IDART™ program performs assessment across the system lifecycle; (4) the IDART™ program is the most active red team working to advance the state-of-the-art and practice of red teaming, methodologies, and technique; and (5) the IDART™ program translates red teaming into assessment methods that are intended to be broadly distributed to a group of knowledgeable and trained personnel operating in their own private sector function. In sum, the red team performs assessments at a high-level (i.e. "across the system lifecycle") and therefore, this may be one of

the reasons why the IDART™ members emphasized process organizational factors over other areas.

This study contained a "traditionally" small sample size (individual interviews: n=14, focus group #1: n=5, focus group #2: n=5). It also emphasized the detail of the data over statistical or "empirical" generalizability (Trochin, 2001). Theoretical generalization is a rational for generalizing from qualitative research studies because the basis lies in logic rather than probability (Seale, 1999). This logic infers 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). The validity of the extrapolation depends not on the typicality of the case, but on the strength of the theoretical reasoning. This is how a "theoretically" diverse sampling of expertise, experience, and background of red team members is justified with what some would consider a small sample size.

There are limitations with quantifying interviewee comments. In the interview process there are possibilities that an interviewee will not mention a work system element because of an 'availability bias' (i.e. mentioning things that come to mind easily or are easily imaginable), or a 'recency bias' (i.e. remembering the most recent events). Although measures were taken to circumvent this (i.e. set of interview probes, interviewer check sheet), assessment of the quantification of interviewee comments must be interpreted with these limitations. Further, interviews were done individually, so there was little opportunity to corroborate the comments with others in the program while conducting the interview, although the results of the individual interviews were reviewed by 2 red team members. The interviewees responded with a large number of comments in the organizational element category. This emphasis fits with safety research, especially Reason's (1997, 1990) concept of latent organizational failures. In sum, the quantification of comments was provided, but this research also provided the context and content, and additional research is needed to quantify the impact of human and organizational factors on CIS performance.

Limitations with the focus group results also need to be addressed. Each focus group approached the task and goal of the session differently. Focus group #1 took a broad view of an organization's systems, citing many relationships among the human and organizational factors that they identified. Focus group #2's approach differed in that they took a more specific approach, creating relationships among factors, but identifying more factors in general. These differences need to be considered when interpreting the results of the focus group. Secondly, although the focus group process used in this study is similar to IDART ™'s brainstorm process for creating system views and attack graphs, the results should not be interpreted as conclusive. Normally, when IDART™ conducts brainstorming sessions, the red teams spend more time filtering the graphs in multiple ways and assessing the results on multiple criteria. In this sense, the results did not produce attack graphs. Rather, they composed scenarios of how vulnerabilities can be created in CIS systems. Also, the focus groups did not provide further analysis (e.g., follow-up to the brainstorming session) that they would typically apply to brainstorm results. The scenarios are the result of 2 focus group sessions that had some advanced preparation (i.e. previous individual interviews, study description and focus group guide sent via email a week before the focus group). However, when a red team typically goes into a brainstorm session, the core assessment team (i.e. project leaders) briefs the rest of the attendees on the system mission,

the red team mission, and how the system works. In each of the focus groups, this information was not created nor provided to the focus groups. This could account for some of the differences between the approaches and results of the two focus groups.

5.4 Future Research

There are many opportunities for future research in this area. The findings in both the individual interviews and focus groups could be developed further with the IDART™ program (i.e. filtering graphs, applying various metrics) or other red team programs that utilize different assessment approaches with other types of expertise. For example, the scenarios developed in future research could be subjected to a "panel of red team experts" to validate and further generalize the findings.

Future research in this area would include a taxonomy that describes work system fixes for more specified categories of security breaches, with relative weighting of each element. The information used in this study could be used to develop a quantitative tool or survey instrument to quantify risk. The checklist of human and organizational factors would be a way of measuring whether certain human and organizational factors are present in an organization. This information could then be correlated to the strength of CIS.

Organizational factors were heavily emphasized by the red team members in this study. This is not to say that there are not many more factors in the other categories of the work system. To extract the specific operational-level conditions, conducting research with end users or those who have first-hand knowledge of these problems, is warranted. This could include interviewing end users or observing their behaviors in the workplace. The purpose of this research would be to characterize the human and organizational factors at the operational or situational-level.

The results of this study were interpreted with the CIS outcomes of vulnerabilities: design, implementation, configuration, and operational. There are many different ways to characterize and interpret this and similar data. For example, research could assess the various human and organizational factors affecting different dimensions of CIS performance. For example, human and organizational factors could be associated with the CIS goals of confidentiality, integrity, and availability. Further, future research could interpret human and organizational factors in the context of various adversary models or dimensions (e.g., insider/outsider status, sophistication, level of system privileges, and motivation or goals). In particular, CIS incidents are often related to actions by 'insiders,' (i.e. network administrators and end users) (Gordon, Loeb, Lucyshyn, and Richardson, 2005), which were also emphasized by red team members in this study. Some research has begun to analyze the behavior of these groups in terms of violations and human error (Kraemer, Carayon, and Clem, 2006, Kraemer and Carayon, 2006), but much more research in identifying and characterizing the human error and latent organizational conditions could be developed for more effective risk management.

6. CONCLUSION

This study described and linked human and organizational factors and CIS vulnerabilities (i.e. design, implementation, configuration, and operational) and provided insight as to how the different types of human and organizational factors create opportunities for CIS vulnerabilities and breaches. Products of this work include: a description of work system factors associated CIS vulnerabilities and performance, scenarios depicting how human and organizational factors combine to elicit CIS vulnerabilities, both from an adversarial viewpoint. These contributions add to the understanding of the work system in which CIS systems exist, and how human and organizational factors are related to one another and contribute to CIS vulnerabilities. These findings may be used to further explore how human and organizational factors can be improved in order to enhance CIS performance.

Findings on the organizational factors in CIS in this study strongly suggest there is an opportunity to use the knowledge gained to conduct future research of CIS and to apply in the workplace. Remarks from red team members on organizational elements in CIS were mentioned most frequently warranting further investigation, possibly a taxonomy that described work system fixes for more specified categories of security breaches, with relative weighting of each element. The framework that was developed from their comments as well as the focus group pathways may also be applied in the workplace, aiding network administrators and CIS managers in building better security practices and procedures for their networks. The human and organizational factors defined and described in this research study can also be adapted by red teams as a diagnostic tool for human and organizational factors in CIS systems. This study makes novel contributions to the fields of human factors engineering, computer science, and red teaming by outlining a myriad of non-technical factors that affect CIS performance. The approach taken in this study has yet to be explored in human factors or computer science literature. Currently, human factors research in CIS focuses on single human or organizational factors or particular CIS methods (e.g., encryption techniques, passwords). Research in computer science focuses almost exclusively on technical factors that affect CIS and does not adopt a "systems" approach that considered technical *and* non-technical factors. Finally, this work contributes to the red teaming methodology by broadening the red team's approach to a work systems perspective enabling it to consider individual and organizational factors in CIS vulnerabilities.

REFERENCES

Adams, A., and Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 41-46.

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

Brostoff, S., and Sasse, M. A. (2001). Safe and sound: A safety-critical approach to security (position paper). In *Proceedings of New Security Paradigms Workshop'01*. Cloudcroft, NM.

Carayon, P., and Kraemer, S. (2002). *Macroergonomics in WWDU: What about computer and information system security?* Paper presented at the 6th International Scientific Conference on Work With Display Units - WWDU 2002 - World Wide Work, Berlin, Germany.

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

Clem, J. F., Badgett, B., and MacAlpine, T. (2003). *X-Bone: Automated system for deployment and management of network overlays*. Albuquerque, NM: Sandia National Laboratories.

Cleveland, R., Cohen, H., Smith, M. J., and Cohen, A. (1979). *Safety Program Practices in Record-Holding Plants*. Washington, D.C.: U.S. Department of Health, Education, and Welfare: NIOSH.

Cobb, C., Cobb, S., and Kaybay, M. E. (2002). Penetrating Computer Systems. In S. Bosworth and M. D. Kabay (Eds.), *Computer Security Handbook* (4th ed., pp. 8.1-8.34). New York: John Wiley and Sons.

Cohen, A., Smith, M. J., and Cohen, H. H. (1975). *Safety Program Practices in High versus Low Accidents Rate Companies - An Interim Report (Questionnaire Phase)*. Cincinnati, OH: U.S. Department of Health, Education, and Welfare, PHS, CDC, NIOSH, Division of Laboratories and Criteria Development.

Computer Science and Telecommunications Board-National Research Council. (2002). *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Washington, DC: National Academy Press.

Duggan, D. (2000). *Assessment report of the gas industry standards board (GISB) electronic delivery mechanism related standards*. Albuquerque, NM: Sandia National Laboratories.

Duggan, D., Villamarin, C. H., Moore, M. D., and Davis, T. W. (2003). *Resilient Overlay Networks (RON): Information Design Assurance Red Team Final Report*. Albuquerque, NM: Sandia National Laboratories.

Fulford, H., and Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: An exploratory investigation. *Information Management and Computer Security, 11*(3), 106-114.

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

Guldenmund, F. W. (2000). The nature of safety culture: A review of theory and research. *Safety Science, 34*, 215-257.

Howard, J. D., and Longstaff, T. A. (1998). *A Common Language for Computer Security Incidents* (No. Sandia Report: SAND98-8667): Sandia National Laboratories.

Howard, J. D., and Meunier, P. (2002). Using a "Common Language" for Computer Security Incident Information. In S. Bosworth and M. E. Kabay (Eds.), *Computer Security Handbook* (Fourth ed., pp. 3.1-3.22): John Wiley and Sons.

Kraemer, S., Carayon, C., and 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., and Carayon, P. (2005b). Computer and information security culture: Findings from two studies. In Human Factors and Ergonomics Society (Ed.), *Proceedings of the Human Factors and Ergonomics Society* (pp. 1483-1487). Orlando, Florida.

Kraemer, S., and Carayon, P. (re-submitted). Security managers' views of human and organizational factors and computer and information security. *Computers and Security*.

Kraemer, S., and Carayon, P. (2006). A human factors model of human error and violations in computer and information security. To be published in *Applied Ergonomics*.

Landwehr, C. E., Bull, A. R., McDermott, J. P., and Choi, W. S. (1994). A taxonomy of computer program security flaws. *ACM Computing Surveys, 26*(3), 211-254.

Mitchell, J. C. (1983). Case and situational analysis. *Sociological Review, 31*(2), 187-211.

Polet, P., Vanderhaegen, F., and Amalberti, R. (2003). Modelling border-line tolerated conditions of use (BTCU) and associated risks. *Safety Science, 41*, 111-136.

Rasmussen, J. (1997) Risk management in a dynamic society: A modeling problem. *Safety Science, 27*(2/3) 183-213.

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

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

Sandia National Laboratories. (2005). Sandia National Laboratories: Homeland Security. (http://www.sandia.gov/programs/homeland-security/red_teaming/redteam.html).

Sasse, M. A., Brostoff, S., and Weirich, D. (2001). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Schein, E. (1984). Coming to a new awareness of organizational culture. *Sloan Management Review, 25*(2), 3-6.

Seale, C. (1999). *The Quality of Qualitative Research*. London: Sage Publications.

Smith, M. J., Cohen, H., Cohen, A., and Cleveland, R. (1978). Characteristics of successful safety programs. *Journal of Safety Research, 10*(2), 5-15.

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

Trochim, W. M. K. (2001). *The Research Methods Knowledge Base* (2nd ed.). Cincinnati, OH: Atomic Dog Publishing.

Zohar, D. (1980). Safety climate in industrial organizations: Theoretical and applied implications. *Journal of Applied Psychology, 65*(1), 96-102.

APPENDICES

Appendix A: Study description, construct definitions, and interview guide sent to red team members.

Appendix B: “Check sheet” for individual interviews.

Appendix C: Interview guide for focus groups.

Appendix D: Email request for feedback on individual interviews.

Appendix E: Feedback and response form for study verification.

Appendix F: Definitions of organizational factors associated with CIS.

Appendix G. Definitions of individual factors associated with CIS.

Appendix H. Definitions of task factors associated with CIS.

Appendix I. Definitions of technology factors associated with CIS.

Appendix J. Definitions of environmental factors associated with CIS.

Appendix K. Definitions of antecedent factors identified in focus group #1.

Appendix L. Definitions of human and organizational factors identified in focus group #1.

Appendix M. Definitions of human and organizational factors identified in focus group #2.

Appendix N. Operational guidelines for human and organizational factors in CIS.

Appendix A. Study description, construct definitions, and interview guide sent to red team members

Study title: "An adversarial viewpoint of human and organizational factors in computer and information security"

University of Wisconsin Research Team	**Sandia Research Team**
Pascale Carayon, PhD+	John Clem
Professor of Industrial and Systems Engineering	Information Design Assurance Red Team
Director of the Center for Quality and Productivity Improvement	Sandia National Laboratories
University of Wisconsin-Madison	Mike Skroch
carayon@ie.engr.wisc.edu, 1-608-265-0503	Information Design Assurance Red Team
+610 Walnut Street 575 WARF Building Madison, WI 53711	Sandia National Laboratories
Sara Kraemer, MS+	
Graduate student of Industrial and Systems Engineering	
Research assistant of the Center for Quality and Productivity Improvement	
skraemer@cqpi.engr.wisc.edu, 1-608-263-2658	

Overview of study

The objective of this research is to examine the "non-technical" aspects (i.e. human and organizational factors) of computer and information security (CIS). The adversarial viewpoint of these factors is important and unique. Systems defenders need to take human and organizational factors into account as they plan their defenses against attacks. Their defensive strategies depend on not only understanding how to harden technical security vulnerabilities, but also how to develop a holistic system that considers how human behavior interacts with the technical CIS system. Therefore, there are two research questions being addressed in this study:

(1) What are the human and organizational factors that adversely affect CIS?

(2) How do human and organizational factors affect CIS vulnerabilities?

What are "human and organizational factors"?

Human factors, or ergonomics, is the scientific discipline concerned with the understanding of interactions among human and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human-well-being and overall system performance (International Ergonomics Association, 2000). This study will focus on both human and organizational factors associated with CIS. See Table 1 for examples of some human and organizational factors within a CIS system.

Method

This study will consist of individual interviews and two focus groups core red team members. The individual interviews and focus groups will consist of an open-ended questioning format. The individual interviews will specifically address Research Question #. The interview guides for the individual interviews will consist of two sections: (1) a global question about the human and organizational factors that contribute to CIS vulnerabilities and (2) a set of probes that details the human and organizational factors of the CIS system

The focus groups will specifically address Research Question #2. In the focus group sessions, we will build upon the discussions of the individual interviews. The focus group interview guide will consist of two sections: (1) a global question of how human and organizational factors are related to CIS vulnerabilities and (2) a set of probes to explore the nature of the relationships among factors and vulnerabilities. The use of flowcharting or drawing pictures and telling stories of examples will also be used in the focus group session.

Table 1. Human and organizational factors associated with computer and information security

Human and organizational factors	**Definitions**
Policy and standards	• Rules and regulations that are set by the organization, implemented and enforced by management. • In compliance with applicable law, industry regulations, and the decisions of enterprise leaders.
Training	• The systematic, structured development of specific skills required to perform job tasks.
Design	• The overall CIS system design. • The overall goal is to transform inputs into outputs to accomplish specified goals and objectives. • Includes the optimization of the social, technical, and environmental subsystems of the overall CIS system
Management involvement	• A participatory approach to management that includes employee involvement and fits existing working conditions.
Task/workload	• A task is an objective to be attained in fixed conditions and there are varying types of conditions: technical, organizational, social, etc… • Workload is both quantitative (i.e. there is too much to do or working under pressure to meet deadlines) and qualitative (i.e. not feeling able or capable of doing a given task or task demands are close to the upper limit of capability).
Resource allocation and process ownership	• Resource allocation refers to the management of supply or involvement that includes machines, tools, labor skills, materials, documents, and entities that must be available for work to start and be completed. • Process refers a systematic series of actions directed to the achievement of a goal; by which an organization carries out is assigned responsibilities Process ownership is the individual or group

	of individuals responsible for the carrying out the specified process.
Security culture	• A pattern of shared basic assumptions about the various facets of computer and information security. • These patterns are what the group learned as it solved its CIS problems of external adaptation, and internal integration, and considered valid. • The patterns are taught to new members as the correct way to perceive, think, and feel in relation to those CIS security problems.

Individual Interview Guide

Global Question 1:
What are the human and organizational factors that adversely affect computer and information security?

Probes:
- Do you have an **example(s)** and **stories**?
-What human and organizational factors are **missing** from this list?

1. What are the organizational factors associated with CIS?
    a. For example:
        i. Communication within the organization, security culture, security policies.
2. What are the individual factors associated with poor CIS?
    a. For example:
        i. No training in CIS, low motivation to use CIS methods.
3. What are the technological factors associated with CIS
    a. For example,
        i. Not user-friendly security methods (e.g. authentication, encryption methods), poor interface between users and CIS systems.
4. What are the tasks associated with poor CIS
    a. For example,
        i. Workload is heavy or unmanageable (e.g., overwhelmed by managing patches, updating software).
5. What are the environmental elements associated with poor CIS?
    a. For example:
        b. Noisy workplace environments.

Appendix B. “Check sheet” for individual interviews

Interviewee	
Date/Time	
Age? Male/Female?	
Email address	
Phone number	
Background	
Experience level	

Global Question 1:
What are the human and organizational factors that adversely affect computer and information security?

Probes:
- Do you have an **example(s)** and **stories**?
-What human and organizational factors are **missing** from this list?

		Themes	X	?	Comments
Organizational Factors	**Communication within the organization**	No or poor communication between users and security administration groups			
		No or poor communication among security administration			
		No or poor communication among users			
		Other			
		Other			
Organizational Factors	**Security Culture**	No or poor employee participation			
		No or poor training on CIS and various subject-specific topics, opportunities for self-initiated CIS training			

		Poor hiring practices, such as background checks, employee handbooks, attestation on CIS policy and practices			
		Poor reward system: attitude that appreciates CIS, understand the benefits of CIS, connect CIS to value in worker/user jobs.			
		Management commitment			
		Communication and feedback, corporate policy on intranet site, users commenting on CIS, and users emailing/calling CIS manager.			
Organizational factors	**Policy**	Policy does not exist			
		Enforcement of policy			
		Users not following policy			
		Attestation of policy			
		Does not address needs of users			
		Unfinished policies			

		External service providers do not meet policy			
Organizational factors	**Organizational structure**	Centralized/decentralized CIS function			
		Ownership of CIS responsibilities			
		Separating security tasks among various groups			
		Lack of security personnel			
		CIS audit is not regular, comprehensive, or does not exist			
Org. factors	**Implement ation**	No emphasis on making a new technological system secure			
		CIS is an afterthought			
Additional comments:					

Appendix C. Interview guide for focus groups

Global Question: How are these factors related to technical computer and information security vulnerabilities? Do you have **examples** or **stories**?

Probes:

1. What are the human and/or organizational factors related to:
    a. Design vulnerabilities? Do you have an example(s)?
    b. Implementation vulnerabilities? Do you have an example(s)?
    c. Configuration vulnerabilities Do you have an example(s)?
2. What is the nature of these relationships?
    a. Is there a temporal relationship (i.e. does one factor occur before another)?
    b. What kind of effect does this factor have on the vulnerability and/or intermediate factor?
    c. Can you tell a story to explain this relationship?
    d. Can you draw a picture or flowchart to explain this relationship?

Appendix D. Email request for feedback on individual interviews

September 13, 2005

Hello-

I am contacting you today because I am seeking feedback on our conversation on human and organizational factors in computer and information security. In May of this year, I conducted an interview with you to explore the following question: "What are the human and organizational factors that are associated with computer and information security?" During our hour-long conversation, I recorded your discussion and have had your interview transcribed.

Attached to this email is the interview transcript. Please read it over and respond to the following questions by September 20, 2005.

(1) Is there any topic or area that you would like to modify or expand on?
(2) Is there a topic or area that you feel should not be part of your view of human and organizational factors? If so, why?
(3) Are there topics or areas that should be included that aren't?

You may respond to these questions either in written form (email). I may also be reached at 608-263-2658 or skraemer@cqpi.engr.wisc.edu. Please let me know if there is anything I can help you with. Thanks again for your time and participation in this study.

Regards,
Sara Kraemer, MS
Center for Quality and Productivity Improvement
University of Wisconsin-Madison
610 Walnut Street 575 WARF Building
Madison, WI 53726
+608-256-2658
skraemer@cqpi.engr.wisc.edu

Appendix E. Feedback and response form for study verification

Hi,

Your response to the results in this preliminary study report will help in the validation of the study. Please provide feedback and explain where the study's explanations are partial or mistaken, and need to be revised for more accuracy.

1. Looking at the study report:
    a. What errors to you see?
    b. What differences in interpretation do you have? (feel free to insert notes or "track changes" directly on the study report itself).
2. Looking at the flowcharts (Research question #2 specifically)
    a. Generally speaking, how accurate do you consider the flowchart to be? Please say why think so.
    b. Are there any important elements missing? List them here (with numbers), and/or draw them in on the chart.
    c. Looking at the specific boxes of factors, are any of them unimportant, trivial, of little effect? Explain briefly why they are of little value, from your point of view.
    d. Looking at the arrows between boxes, do you think they are accurate? If not, please cross off the arrows or draw in new arrows. Write the numbers of the boxes involved here. Please explain your revisions briefly.
    e. Is the discussion of the vulnerabilities (i.e. outcomes) at the end of the flowchart description accurate from your point of view? What revisions would you suggest to make more accurate?
    f. If you would like to draw a revised flowchart that would show your explanations, please feel free to do.
3. Any other concluding comments or suggestions?
4. If you can think of any specific examples of vulnerabilities, please write it down.

Please let me know if I can be of any help.

Sara

Appendix F. Definitions of organizational factors associated with CIS

Policy-1			
Nodes	**Sub-nodes**		**Definitions**
Policy content	Mismatch between outdated policy and current technology		When technology is changed or updated, policies are not.
	Technology is not independent of policy		Written policy needs to reflect goal of CIS, not a specific guideline to a type of technology.
	Does not allow exemptions in policy		CIS policies do not to allow for exceptions to the CIS rule.
	Outdated policies		The content of the policy is not current with the technological changes of the CIS system.
	No documentation of consequences of non-compliance		CIS policies need to document the ramifications of violations.
	Lack of tie-in to business plan		Policy is not linked to business goals or objectives.
	Erroneous policies		Policies are written or documented incorrectly.
	Elements of policy content related to clearness	Lack of documentation of policy	No written verification of policies.
		Imprecise policy	Policy is not written in detailed specification.
		Does not state ‘why’ policy exists	Do not state the reasons behind a policy.
		Core policies are not developed	Policies need to have a foundation of principles that do not change.
		Incomplete policies	Policies that do not fully reflect actual practice, procedure, or state of the system.
		Policy is not tailored toward groups	Policy needs to address the specific need of various CIS user groups.
		Lack of clarity	Policies are not written in clear, understandable language.
		Classification levels are not specified	Policy needs to specify the exact access classification of each employee/user group.

Policy-2		
Nodes	**Sub-nodes**	**Definitions**
Lack of procedures for writing policies	Management ensures few policies	Role of management to make sure that there are a few number of policies and are effective.
	Policies are not maintained	Policies are not updated on a consistent basis.
	Too many policies	A large number of policies such that is unmanageable and difficult to use.
	No participation or input from personnel	Lack of input from key stakeholders in CIS on policy needs.
	Network administrators write policies	Instead of employing/assigning qualified personnel whose job officially includes writing CIS policies. This can be a danger because network administrators often lack the superior writing skills needed to produce coherent policies
	Lack of clear procedures for writing policies	Official guidance for writing policies does not exist.
Poor guidelines or procedures	Outdated CIS policies	Policies for secure CIS behavior are not relevant because they are out of date.
	Multiple versions of CIS procedures	More than one version of CIS procedures or guidelines exist
	Guidelines do not match policy	The written guidelines for CIS behavior and protocol are not consistent with the corresponding policy.
	Lack of guidelines for secure behavior	Lack of a set of procedures or protocol for CIS.
Inadequate Policy management	Lack of management buy-in to policy	Describes a management structure or culture that fails to place an adequate emphasis on CIS policy.
	Organization fails to enforce policy	As a whole the organization does not actively enforce the CIS rules and regulations.
	Policies created for legal purposes	Written to cover against potential legal trouble, rather than promote true CIS security.
	Policy manual lacks usability for personnel	Policy manual is created without the needs of those who use it.

Policy-3			
Nodes	**Sub-nodes**		**Definitions**
Inadequate Policy management, continued	Lack of mechanisms to enforce policy		The organization lacks the controls to make policy obligatory.
	Lack of clear, concise policies for training		No specifications for policy training.
	Lack of policy update alerts		An absence of an alert mechanism to revise policies or alert users of revised policies.
	Lack of updates to policy		No update to policy when state of system or process changes.
	Lack of priorities in policy		No set of prioritization applied to the importance of some security measures versus others.
	Implementation of policies	Lack of policy implementation	No management process to implement policies.
		Policy implementation via checklist	CIS policies are implemented by adhering to a generic list of measures or protocols.

Culture-1		
Nodes	**Sub-nodes**	**Definitions**
Organization-wide CIS behaviors	Unaware of CIS policies	An overall obliviousness to the existence or content of CIS policies.
	Lack of participation for all levels	Personnel does not have input into CIS processes or system.
	Accept various levels of risk	Tolerate different amounts of danger associated with CIS threats.
	'Rigid' CIS environment is not maintained	Describes organizations without a strict, structured CIS environment.
	Migration towards non-compliance	Describes a phenomenon that over time, secure practices and procedures degrade to behaviors that are not secure.
Organizational culture issues	Political in-fighting	CIS is compromised when personal agendas are elevated over organizational interests.
	No alignment between corporate vision and CIS	Describes a lack of connection between the overarching goals of the organization and the function and goals of CIS.
	Lack of corporate support	Lack of importance of CIS from the corporate level.
	CIS runs counter to organizational culture	Refers to the goals of CIS conflict with aspects of overall organizational culture. For example, in research-oriented organizations, the culture of information-sharing may be pervasive. This mindset may conflict with a set of CIS practices to keep information secret.
	Punitive culture	CIS-organizational culture that includes an element of "punishing" employees for mistakes or un-secure behaviors.

Culture-2			
Nodes	**Sub-nodes**		**Definitions**
Overall perceptions related to CIS	Overall unimportance to CIS		Describes an organization that, as a whole, disregards the importance of security.
	Pressure from customers and public		Refers to a lack confidence in an organization's CIS performance from outside entities (e.g., customers, public as a whole).
	False sense of security		Describes an organization that generates a perception that they are more secure than they actually are.
	Usability is viewed as more important than CIS		Refers to compromising CIS when the usability of the IT system is held in higher regard than CIS standards and performance.
Reward and recognition	Lack of reward and recognition for CIS work		Refers to a lack of acknowledgment for CIS-related efforts.
Management commitment	Lack of resources for CIS	Lack of budget or funding	No monetary resources dedicated toward CIS.
		Old equipment	Use of antiquated technology due to a lack of support from management.
		Do not support CIS training	Lack of emphasis on importance of continued CIS education.
		CIS viewed as an overhead cost	Describes management's regard that CIS is not an investment, but rather a liability.
	Lack of upper management emphasis on CIS	CIS personnel not empowered	Refers to the disenfranchisement of CIS staff.
		Favor functionality over CIS	Refers to the priority of usability of technology controls and methods, rather CIS.
		Undervalued by top management	An overall lack of consideration for CIS by top management.
		Lack of management leadership	No top management role to assume responsibility and ownership of CIS and its importance.

Elements of unsystematic CIS organization: Management-1			
Nodes	**Sub-nodes**		**Definitions**
Lack of CIS management plan	Lack of prioritization of criticality	Do not assign correct criticality to assets	Refers to problems with identifying the proper importance to the organization's assets.
		Lack of prioritization resources	Refers to lack of preference to assigning proper budget and staff to key CIS components.
		CIS is adhoc	Refers to when CIS is an afterthought to the design and management of IT systems.
		Policies and plans are not tailored to specific needs or priorities	Standard or generic policies or plans that do not address the unique characteristics of the organization or the corresponding CIS system.
	Interfaces between organizations and outside networks	Problems connecting to outside networks	Vulnerabilities that exist when organizations' networks are interconnected.
		Consultants with inadequate solutions	Describe the tendencies for external reviewers to propose solutions that are "canned", or generic, which do not cover all of the aspects of a CIS system.
		Trust relationships between organization	Vulnerabilities develop when one organization assumes that another organization with whom they connect with has and maintains a high level of CIS.
		Lack of procurement process plan	Refers to a deficient or absent acquisition plan for technology.
		Incorrect requisition specification to vendor	Refers to erroneous technology requirements to vendors.
		Outsource CIS function	Refers to sub-contracting CIS support from an outside entity.
	Gaps in operational CIS planning	Cyber vs. physical	Refers to operational planning for all security, both CIS (e.g., networks, internet access, software, hardware) and physical (e.g., locks on doors, employees wear badges).

Elements of unsystematic CIS organization: Management-2			
Nodes	**Sub-nodes**		**Definitions**
CIS practices	Systematizing CIS practices	Lack of participation from all organizational levels	Describes a lack of input or insufficient information from personnel in the organization.
		Lack of a reminder system for secure practices	Refers to no method to alert end users to practice secure CIS.
		Lack of comprehensive mitigation practices	Refers to an incomplete approach and process for investigating and resolving vulnerabilities.
	Implementing CIS practices	Do not execute secure CIS practices	Refers to personnel not following secure CIS protocol or procedures.
		CIS practices are not emphasized	Refers to a lack of importance to CIS procedures.
		Lack of continuous process for CIS	The process in which CIS practices and principles are implemented are fragmented - not an ongoing process.
		No standardized CIS implementation	Refers to a lack of regular procedures to put CIS principles into practice.
Communication	No cross-departmental communication		Refers to a lack of information exchange across organizational departments.
	Interact with bureaucracy		Refers to the difficulties implementing change to improve CIS performance when the organization is large and inefficient.
	Too many organizational hierarchies		Refers to the difficulties communicating with and implementing CIS across various organizational levels.
	Poor communication between end users and network administrators		Refers to inadequate information exchange between end users and network administrators.

Elements of unsystematic CIS organization: Management-3			
Nodes	**Sub-nodes**		**Definitions**
CIS process and performance	No measure of CIS performance	Lack of CIS metrics	Refers to a lack of benchmarks or measurements to track CIS performance.
		Inconsistent CIS metrics across department	Refers to CIS performance measures that are not the same throughout the organization.
	Audits or evaluations	No performance evaluation of personnel	Describes an organization that does not check for consistency between the written policy and personnel's' CIS-related behavior.
		No policy evaluation in assessments	Refers to a lack of policy review in critical assessments of CIS systems.
		Lack of CIS evaluation or audits	Refers to a lack of critical CIS assessment in the organization.
		Lack of accountability mechanism	Describes methods to make sure that CIS policy and procedure is followed. For example, passwords that expire and force end users to change passwords.
	Systems or life cycle issues	Lack of human factors consideration in CIS lifecycle	Refers to minimal significance of human factors in the design and overall CIS life cycle.
		Communications breakdowns in implementation	Describes inconsistencies in technology specifications across groups during the implementation phase.
		Different assumptions among groups	Among the various groups involved with the CIS system life cycle (e.g., designers, administrators, managers), there may different assumptions related to the decisions, knowledge, and state of CIS systems.
		Lack of consideration for the complexities of operations problems	Refers to no realization for the potential or real communication breakdowns in the inherent complexity of an operations environment.
		Do not communication design requirements	Refers to the 'conceptual' errors that occur at the design stage as a result of problematic communication.

Elements of unsystematic CIS organization: Management-4				
Nodes	**Sub-nodes**			**Definitions**
CIS process and performance, continued	Systems or life cycle issues, continued	Abstraction of subsystems	One subsystem more important than others	A user in the CIS system may abstract the problems in the life cycle differently. User groups may place different levels of important on various aspects of the CIS life cycle. For example, executives in a company may place higher importance on the organizational elements of CIS, while the IT personnel may place emphasis on the technological aspects of software and hardware.
			Adversaries attack problems at the lowest level required	Red team members attack at the lowest level of CIS system that is vulnerable (e.g. a design vulnerability is a high level of the CIS system, a configuration vulnerability is a low level of the CIS system).
			Various levels of abstraction	Refers to the different types of abstraction, such as physical, organizational, topical, legal, operational, technical, or policy.

Elements of unsystematic CIS organization: Management-5			
Nodes	**Sub-nodes**		**Definitions**
CIS process and performance, continued	Sustainable and adaptive CIS processes	Not a sustainable process	Describes how and why CIS system performance degrades over time or cannot keep up with the changes in technology or the environment.
		Do not account for remote logins (VPN)	Refers to an organization that does not monitor and manage those users who use their laptops to access the company's network from remote locations.
		Lack of cyber-engineering	Refers to a lack of research and development in the science and engineering of CIS.
		Lack of process to implement policies	Absence of a consistent or organized process to implement CIS policies.
		Lack of feedback loop(s) for CIS problems	Describes deficiencies in communicating various CIS-related problems to appropriate sources.
		Do not consider CIS as part of the workflow	Refers to how CIS mechanisms or methods do not necessarily fit into the work context of end users. For example, computer generated passwords that changes frequently are difficult to remember. Users may write down passwords in order to easily access their passwords.
		CIS does not have consistency in its process	Reflects on how the CIS industry does not have a systematic engineering foundation. Most organizations customize their CIS systems to their own design (or lack thereof).
		Lack of human factors consideration in CIS implementation	Refers to a need consider human (or user) performance in the implementation of CIS methods, mechanisms, and controls.
		Difficulties in merging CIS systems processes	Considers the complexities of merging architectures, taking into account differences, such as requirements, processes, and data sharing.
		Lack of management planning for CIS	Refers to a lack of organizational planning for CIS at the management level.

		Lack of acquisition process for technology	No formal process for determining the criteria for acquiring new technology.

Elements of unsystematic CIS organization: CIS function			
Nodes	**Sub-nodes**		**Definitions**
CIS function	Distributed workers	Lack of criteria for consistent work	Refers to no protocol for performing CIS-related duties. This refers to CIS personnel, such as network administrators or system analysts.
		Lack of communication mechanisms	Describes a lack of channels to share information (e.g., threats, viruses, patches) across distributed locations of CIS personnel. They may be in different departments or organizations.
		Lack of consistency in work	Refers to CIS personnel executing different CIS methodologies and metrics for performance.
	Structure of CIS function	Lack of separation CIS from IT	Refers to the need to separate the IT personnel from the CIS staff.
		One brand of software equipment used	Refers to an organization utilizing many different kinds of technology, which may lead to inconsistencies and problems.
		No management position for CIS	Refers to an absence of a leader for the CIS function.
	Centralized versus Decentralized	Lack of centralized CIS function	Refers to an absence of a unified CIS function.
		Diffusion of CIS expertise	Describes a situation where CIS expertise is distributed throughout an organization.
		Benefit of decentralized CIS	Describes aspects of decentralized CIS function that are valuable. For example, a decentralized CIS function may be more dynamic and nimble to address CIS problems in different locations.

Elements of unsystematic CIS organization: CIS Training			
Managing CIS training	Provide little CIS training for employee		Describes the organization's lack of provision of CIS education.
	Lack of training policy		Refers to no documentation of training guidelines.
	Lack of upper management support for CIS training		Describes upper management's lack of dedication to CIS training.
	No training to remain current with CIS		Refers to a lack of mechanisms to educate staff on new technology or CIS issues.
	Lack of CIS refresher training		Lack of re-training or updates for past lessons learned in CIS training.
	Lack accessibility to the information provided in CIS training		Refers to end users not being able to find the information presented or learned in a CIS training effort. This may be due to a lack of documentation or the documentation is incomplete, inaccurate, or disorganized.
	Training is not a consideration in performance reviews		Refers to a lack of emphasis on training efforts in employee's performance reviews.
	Lack of continuous training		Lack of training on an on-going basis.
	Training content not tailored toward different user groups		Describes training that does not fit the different needs of various groups (e.g., network administrators, end users).
CIS Training content	Training content for network administrators	Lack of specific CIS technical training	No training for the various aspects of CIS administration. For example, USENIX versus Windows administration.
		Lack of “hands on” training	Lack of on-the-job training for CIS administration.
	Training content for end users	Need training with “real life” examples	Lack of examples of “true” CIS problems that end users can relate to.
		Training content does note include “why?”	Training does not supply the reasoning behind CIS rules, procedures, policies, or practices.

Appendix G. Definitions of individual factors associated with CIS

Individual Factors of Network Administrators-1		
Nodes	**Sub-nodes**	**Definitions**
CIS-related knowledge and skills	Do not have “real-life” experience	Paucity in work-related practice.
	Lack formal CIS training or education	Describes scarcity in organized CIS education, as found in college coursework.
	Mismatch of skills, task, and job	Describes a misalignment among the skills or expertise of the worker versus the technical requirements of the tasks and job.
	Lack of CIS-related expertise and skills	An all-round lack of CIS skills of the pool of NAs within an organization.
Beliefs	Lack of caring for CIS mechanisms (e.g., passwords)	A lack of regard for some CIS methods.
	Lack of regard for end user needs	Describes a disparaging attitude toward end users and their work requests of network administrators.
	Believe that network administrators need unlimited access	Describes network administrator's view that they need complete, open access to the organization's networks.
	Feel undervalued by the organization	Sense of disenfranchisement resulting from the organization’s dismissal of their work.
	Misperceptions of job goals	Network administrators misunderstanding of their job's purpose.
	Feel “blamed” for CIS problems	Feel punished or responsible for CIS problems, even if the problems were not their fault.
	Exempt from CIS standards, policies	Belief that their status as network administrators does not apply to CIS protocol.
	Work tasks are more important than CIS	Describes the prioritization of completing network administrators own work, rather than adhering to CIS practices and principles.
	Some aspects of CIS are considered “boring”	Refers to network administrator's view of CIS as a mundane task (e.g. patch management).

Individual Factors of Network Administrators-2		
Nodes	**Sub-nodes**	**Definitions**
Routine violations	Shortcuts due to high workload	Intentional violations of CIS protocol or procedure in order to cope with an overwhelming workload.
	Work around policies and practices	Creating ways to bypass policies and procedures by.
	Shortcuts for job security	Cut corners to perform job better, in order to enhance job security.
	Rely on other CIS mechanisms	Instead of performing a mandated CIS task or procedure, the network administrators will rely on automated methods to perform CIS function.
	Shortcuts because of low priority	Cut corners to perform job better, in order to enhance job security.
	Purposely create incorrect map of network	Intentionally create a map of the network that is wrong or is missing component to avoid being audited.
Lack of an adversarial mindset	Follow a “rigid” CIS approach	Describes a tendency to implement CIS systems in an inflexible manner.
	Do not realize that adversaries will not attack known CIS policies	Refers to an adversary obtaining an organization's CIS policy so they avoid the CIS mechanisms, practices, or protocols outlined in it. They will attack other areas that are not covered by the policy.
	Rigidity follows engineering training	Refers to most system defenders and designers design their CIS systems based upon engineering principles, not allowing for the flexibility and adaptive approach that is required.
	Lacks experience in red teaming	Network administrator or people tasked with CIS do not have any direct experience in red teaming or adversarial modeling.
	Lack of creative thinking	Refers to network administrators not approaching CIS systems and their related problem innovatively, as red teams or adversaries do.
	Follow a functional perspective	Refers to network administrators focusing on operational issues, rather than security.
	Incorrect absent adversary model	CIS defenders do not consider the type of threat or adversary relevant to the system or assets they are protecting.
	Lack of red teaming for human and organizational factors in CIS	Refers to a lack of consideration of human and organizational factors in red team engagements.

Individual Factors of Network Administrators-3		
Nodes	**Sub-nodes**	**Definitions**
Cognitive performance	Inattention	State of distraction.
	Forgetfulness	State of absentmindedness.
	Memorability	Inabilities or poor performance related to memory.
	Configuration mistakes	Errors related to configuring software or programs. For example, leaving default passwords on in software or programs.
Motivation	Lack of importance toward their work	The level of value to the job and tasks of network administration.
	Want to respond to all problems	Describes a drive to find ways to remediate all CIS problems, even if it means introducing new vulnerabilities into the system.
Trust	Trust end users to follow CIS policy	Network administrators' confidence that end users will follow the policies and practices set forth by network administrators.
	Trust technology to perform as it should	Describes a belief that technology will execute their intended goals without fail.

Individual Factors of End Users-1			
Nodes	**Sub-Nodes**		**Definitions**
CIS-related knowledge	Do not understand CIS policies		Lack of comprehension of meaning of CIS policies.
	Lack of general CIS-related knowledge		An absence of basic CIS understanding.
Beliefs	Belief that CIS does not affect their job		Refers to ambivalence toward CIS because end users do not believe that compromising CIS will impact their job security.
	Do not have a stake in CIS performance		Describes a general lack of caring about status CIS performance.
	Unethical belief leading to malicious behavior		Refers to a belief system relating to intentionally compromising the CIS system.
	Lack of respect toward CIS personnel		End users' belief that the work of network administration is of little value. This also includes malicious behavior toward the network administrators.
	Work tasks are more important than CIS		Describes end users placing a higher priority on completing their work tasks rather than adhering to CIS practices and principles.
	Relaxed attitude toward beliefs		Refers to end users decreasing their diligence on practicing secure practices, procedures.
	Do not understand “why” CIS is important		Refers to a lack of logical reasoning for the justification of the significance of CIS.
Behaviors	Not precise or thorough		Describes a tendency for end users to not completely adhere to secure CIS practices
	Share secrets		Refers to a tendency for end users to reveal sensitive information.
	Routine Violations	Workarounds	Circumventing a CIS protocol, practice, mechanism or some other organizational or technical control in order to accomplish a work performance goal.
		Violations of policy	Shortcuts to established policy or guidelines to achieve a performance goal.

Individual Factors of End Users-2		
Nodes	**Sub-nodes**	**Definitions**
Trust	Trust CIS technology	Refers to the implicit belief that the technology will perform as expected, all of the time. For example, an end user may implicitly trust that their virus scanners will catch 100% malicious code, so they will open email attachments from sources they don't trust.
	Trust quality of others' work	Refers to a belief that others, such as network administrators, efforts are legitimate and correct.
	Misplaced trust in outsiders	Refers to a tendency to believe that everyone has benevolent intentions, and consequently, end users may engage in unsecure behaviors, such as giving out passwords.
Motivation	Resentment towards inconsistencies from management	Management may announce new or different operating procedure without any explanation or justification. Additionally, management may use an accusatory tone, creating further offense to end users.
	Want to be helpful	Reflects a motivation to help others, but can result in violating CIS practices. This behavior and motivation has benevolent intentions.
Cognitive performance	Memorability	Difficulties remembering.

Individual Factors of CIS Designers		
Nodes	**Sub-Nodes**	**Definitions**
Beliefs	CIS is not important	A sentiment that CIS is not a priority.
Understanding of CIS Design	Do not understand "systems" integration	Refers to a lack of understanding about linking various systems of technology together into a coherent, functional, and secure system.
	Lack of understanding of technology procurement	Lack of skills needed for obtaining the correct technology in the acquisition process.

Appendix H. Definitions of task factors associated with CIS

Task Factors of Network Administrators		
Nodes	**Sub-nodes**	**Definitions**
Task design	Multiple responsibilities	Network administrators have many duties that they must perform, e.g., network administration duties and CIS-related duties.
	Lack of balancing priorities or tasks	Need to balance the various priorities and duties that must be completed.
	Lack of job rotation for greater exposure and understanding	Network administrators do not rotate duties or responsibilities leading to a lack of exposure to the breadth or CIS problems.
	Lack of following through or completing tasks	Network administrators do not complete every step needed to fully finish a duty or task.
	Emphasis on functionality versus CIS	Describes placing of greater importance on the usability of technology and networks, rather than security.
	Lack of redundancy checks on CIS work	Network administrators do not double-check others' work.
	Lack of prioritization in tasks	Tendency to not emphasize some tasks that are more important than others.
CIS-specific tasks	CIS is an “add-on” task	CIS-related duties are a secondary attachment to regular IT duties.
	Mundane tasks done poorly	Some tasks, such as back-ups, are viewed as 'boring' and therefore are not given adequate effort to make secure.
	Non-CIS work tasks are more important that CIS work tasks	CIS-related duties are not given the time and attention as other IT-related duties.
Workload	High workload	An excess of duties and tasks to perform.
	Not enough staff to complete tasks	Inadequate amount of personnel (i.e. network administrators) needed to complete the work.
	Time pressure	Lack of time to complete work tasks (CIS and non-CIS related tasks).

Appendix I. Definitions of technology factors associated with CIS

Technology Factors of Network Administrators		
Nodes	**Sub-nodes**	**Definitions**
Passwords	Weak passwords	Producing and using passwords that are guessable or easily cracked.
	Create one password for multiple machines	Producing and using one password for many machines, instead of one password for one machine.
	Do not create passwords	Not creating a password for the machines they administer.
	Storing passwords	Retaining a list of passwords.
	Leave themselves logged in	Not logging out of system or machines when they are done working.
Software programming	Difficult to configure programs/software	Software design that is difficult for network administrators to configure.
	Errors in programming	Mistakes in programming or configuring software/applications.
	Complexities related to writing code and programs	Describes the problems associated with the intricacies related to writing code.
	No consideration human factors in design	Human factors or needs are not translated or considered in the design of software or programs.
Firewalls	Difficulty obtaining updated through firewalls	Problems with obtaining software and system updates through strong firewalls.
Technology in general	Old technology	Problems working with outdated equipment.
	Complexity of technology	A lack of understanding for a particular type of technology. For example, a network administrator may set up a VPN system, then not conduct any follow up to understand how it works, who will be in charge of it, how it is being used.

Technology Factors of End Users		
Nodes	**Sub-nodes**	**Definitions**
Passwords	Write down passwords	Instances when end users write down their passwords in order to remember.
	Weak passwords	End users using passwords are common words, default passwords, or using a string of characters that are not alphanumeric.
	"Strong" passwords are difficult to remember	Long, alphanumeric passwords are difficult to remember.
Secure ID cards or tokens	Do not carry ID or token	Instances when end users do not retain their tokens or ID cards. Rather, they may leave them at their workstations.

Appendix J. Definitions of environmental factors associated with CIS

Nodes	Sub-nodes	Definitions
Environmental factors	Lack of physical controls	Lack of access mechanisms to secure the physical space of the CIS system.
	Lack of ergonomic principles	Working conditions that are not tailored to support worker performance and quality of working life.

Appendix K. Definitions of antecedent factors identified by focus group #1

"Why?" Factors	
Factor	**Definition**
A.1 Corporate image	Sustaining an impression of reputability and trustworthiness.
A.2 Corporate profitability	The "bottom line" investment and return on investment for an organization as a whole.
A.3 Bottom line connection	The connection to investment. The "bottom line connection" is directly connected to "corporate profitability"
A.4 Outside relationships	Interfacing with systems (e.g. customers, suppliers) outside of the organization, and the need to be aware of those systems' CIS levels
A.5 Bias for services or products	Refers to organizations' propensity toward buying certain types of technological services or products. The quality of those products ties directly into the presence of CIS vulnerabilities.
A.6 Budget cycle	The cycle of the financial planning for the organizations' resources, specifically funding and resources for CIS.
A.7 Financial requirements	Certification of the organization's financial documentation.
A.8 Government regulations	Restrictions or mandated measures for CIS systems

Environment Factors – Evolves from "Why?"	
B.1 Past history of events	Preceding events, such as security breaches or insider threat, which has an impact on the current state of CIS.
B.2 Staff turnover, continuity	Primarily a resultant of the budget cycle and financial requirements or restrictions.
B.3 Different cultures with different groups	Cultures that exists at different levels of the organization; for example, corporate culture versus the operational and CIS culture
B.4 Rebel mentality	Security staffs' cavalier attitude toward CIS goals and performance.
B.5 Hates security	End users' view of the value of CIS.
B.6 Fear of security	End users' attitude toward adhering to CIS principles or practices.
B.7 User stupidity	Ignorance of CIS end users, from the view of those who are experts in CIS systems.
B.8 Security arrogance	An attitude that the organization's CIS systems are hardened against attacks.
B.9 Communication channels	Mechanisms that are developed to exchange CIS information.
B10. Security process and procedures	The practices and operational mechanisms that are developed to support CIS goals.
B.11 Policy enforcement	How CIS principles are mandated, and have an effect on the technology acquisition process.
B.12 Politics	Personal agendas affecting the interactions among others within the organization, as well as the performance of the organization itself.
B.13 Culture	Organizational awareness and management commitment, with respect to CIS culture, as well as other areas of culture.

Appendix L. Definitions of human and organizational factors identified in focus group #1

Factors	Definitions
1. Type of data/project	The kind of information or goals the organization is attempting to protect. Identifying the type of information is needed in order to assign an appropriate level of criticality.
2. Management support	Refers to the level of importance, involvement, and value that management assigns to CIS.
3. Security policies: No requirements	Lack of CIS specifications in CIS policy content.
4. Funding	Monetary resources allocated to CIS.
5. Adequate staffing	Personnel resources dedicated to CIS.
6. Increased possibility of mistake	Elevated chances of unintentional human error.
7. Adequateness of schedules	Ability of CIS personnel schedules to adequately cover all of CIS tasks or work.
8. Policy overload	Too many CIS policies.
9. Bias for services or products and technology acquisition process	Tendency to favor one type of vendor, service or product.
10. Developer: knowledge and expertise of staff	Level of CIS knowledge base for CIS staff.
11. Complexity	Related to the intricacies of CIS.
12. Commitment to maintainability	Level of dedication to maintaining CIS performance.
13. Security information accessibility	Availability and readiness of CIS information, data, or policies
14. Quality of requirement definition	Performance value assigned to CIS.
15. Choice of technology	The type of technology chosen. This includes software and hardware.
16. Vendor support	The type, level, and quality of customer support received by the organization.
17. User support center	The existence and quality of a end users support group, function, or resource.
18. Documentation quality, availability	The quality of documentation of CIS policy, procedure, technical information, communication.
19. User training	Existence of CIS education for end users.
20. Testing/team process	The existence and quality of testing group and process of testing for CIS system and sub-systems.
21. Defined security process/lifecycle and performance measurement	Existence and quality of the CIS cycle, process, and related metrics.

Appendix M. Definitions of human and organizational factors identified in focus group #2

Factors	Definitions
1. New laws require changes in system	Changes, such as policy updates, to new laws (e.g. HIPAA and Sarbanes-Oxley).
2. Vendor/supplier goes out of business	When a vendor is no longer available, the organization may need to update its technology and/or adapt processes.
3. Stupid people	Ignorance of CIS knowledge and expertise.
4. Relative importance of assets	Assigned criticality to assets that need protection.
5. Available resources	The pool of assets and personnel available.
6. New technology is available or introduced	Refers to instances when a new technology is implemented into an existing CIS system.
7. Adapting technology	Refers to updating old technology to fit new requirements and adapting new technology to meet current system requirements.
8. Adapt policy	Updating policy to new system changes.
9. Low business priority	From a business standpoint, CIS is a low priority.
10. Business case/Ignorance of business case for security	Low relevance or importance for creating a case for CIS.
11. Lack of CIS-related knowledge	Refers to personnel's lack of CIS-related expertise, skills.
12. No management support or buy-in	Lack of importance, value, and priority given to CIS.
13. Resources available for security	Lack of assets and personnel available for CIS
14. Inadequate security staffing (# or skill)	Low CIS staff levels and those that work have a lack of CIS expertise.
15. Lack of time	Time pressure to complete tasks.
16. Original reasons for policy not documented	Lack of recording changes to policy or CIS system.
17. Quality of policy: lack of clarity, no enforcement	Refers to the overall value or worth of the policy: usefulness, clearness.
18. Policy writer technology knowledge	The CIS-related expertise of those creating CIS policies.
19. No ownership for security/responsibility	Lack of an accountability enforcement system for CIS.
20. Funding allocation	Monetary resources given to CIS.

Factors	Definitions
21. Policy not re-evaluated against new technology	When new technology is introduced, the current CIS-related policy is not checked and/or updated to reflect the changes of the new system or technology.
22. Security plan	Refers to the overall strategy for CIS
23. Training	Education for CIS.
24. No consequences for bad practices	Lack of punishment for not following correct CIS protocol or behaviors.
25. Policies not accessible for end users not trained	The content of CIS policies are not given or reached by end users who do not receive CIS training.
26. Policies not followed	Occurrences when CIS policies are disobeyed.
27. Centralized security	The function of CIS is in one location.
28. Organizing security	Refers to the management, processes, and design of CIS work and people.
29. Decentralized security	The function of CIS is in many locations (i.e. departments or functions).
30. Assigning security to the 'wrong' people	Giving the tasks of CIS to people who are under-qualified or untrained.
31. Functionalized process design	A process design that includes only one function of the system.
32. "Empire building", functionalized security, "stove piping", miscommunication across functions	Empire building is when a person or group of people what to control many resources or systems. Functionalized security is a CIS group that does not integrate the many functions of CIS into the processes. Stove piping occurs when there is an "overload", for example, if a person decides to control and run all of the organization's servers.
33. No training, education for developers	Lack of formal education of those creating the CIS system.
34. Insecure default configuration	Default configurations that result in vulnerabilities.
35. Central CIS communication, full policy, rational procedures	Refers to presence or absence of CIS communication, CIS policies, and coherent procedures or protocols.
36. No communication between security designers	Lack of information exchanges among those designing the CIS system.
37. Application of technology to different environment or situation	CIS design changes are not evaluated against the context of the environment or circumstances.
38. No communication between design and implementation	Lack of information exchange between CIS designers and CIS implementers.
39. Service added at last minute	Usually referring to networks, placing network service as last and unplanned step.
40. CIS design: Single mechanism	Assets are protected by one mechanism, back ups and redundancies are not created.

41. Implementer forgets 1 service	The person or persons responsible for implementation forget to implement a service.
Factors	**Definitions**
42. Managing services protection	Managing those hired or "rented" by the organization to perform CIS protection services.
43. No configuration management	Lack of administration or oversight for configuration of hardware and/or software
44. Local CIS implementer performs incorrectly	The person or groups of people does not perform the implementation of technology (i.e. hardware or software) accurately.

Appendix N. Operational guidelines for human and organizational factors in CIS

Guideline 1: Develop Comprehensive CIS Policies and Policy Management Plan -1			
Nodes	**Sub-nodes**		**Specific guidelines**
Policy content	Mismatch between outdated policy and current technology		1. Develop policy content. Update policies regularly, especially when new technologies are introduced. New technologies should be evaluated again current policy. The content of policy should be linked to the goals of the organizations' business plan. 2. Create policies that are clear and concise. Policies that are vague, incomplete or unclear, do not state its purpose, are not tailored toward the specific needs of various user groups, and does not specify the access levels of user groups are potential problems. 3. Document the consequences of non-compliance to CIS policies and identify when legitimate exemptions to policy can be made.
	Technology is not independent of policy		
	Does not allow exemptions in policy		
	Outdated policies		
	No documentation of consequences of non-compliance		
	Lack of tie-in to business plan		
	Erroneous policies		
	Elements of policy content related to clearness	Lack of documentation of policy	
		Imprecise policy	
		Does not state 'why' policy exists	
		Core policies are not developed	
		Incomplete policies	
		Policy is not tailored toward groups	
		Lack of clarity	
		Classification levels are not specified	

Guideline 1: Develop Comprehensive CIS Policies and Policy Management Plan -2		
Nodes	**Sub-nodes**	**Specific guidelines**
Lack of procedures for writing policies	Management ensures few policies Policies are not maintained Too many policies No participation or input from personnel Network administrators write policies Lack of clear procedures for writing policies	4. Create procedures for writing policy. The content of policy should include the input of all levels of personnel. Those who write the policies should have the expertise to do so (i.e. avoid "handing-off" the task of writing policies to those who are unequipped). 5. Do not "add-on" to policies, update or remove irrelevant policies as they are created.
Poor guidelines or procedures	Outdated CIS policies Multiple versions of CIS procedures Guidelines do not match policy Lack of guidelines for secure behavior	6. Create guidelines that match the content and goals stated in policy 7. Guidelines should include facets of secure behavior. 8. There should be one version of CIS guidelines on secure behaviors.
Inadequate Policy management	Lack of management buy-in to policy Organization fails to enforce policy Policies created for legal purposes Policy manual lacks usability for personnel Lack of mechanisms to enforce policy Lack of clear, concise policies for training	9. Create a management process for implementation of new policies. Consider various user groups, their needs, organizational constraints, and collect feedback after the implementation occurs. Update accordingly and often.

Guideline 1: Develop Comprehensive CIS Policies and Policy Management Plan -3			
Nodes	**Sub-nodes**		**Definitions**
Inadequate Policy management, continued	Lack of policy update alerts		10. Alert users of new policy via update alerts and priorities.
	Lack of updates to policy		
	Lack of priorities in policy		
	Implementation of policies	Lack of policy implementation	
		Policy implementation via checklist	

Guideline 2: Cultivate and Maintain CIS Culture – 1		
Nodes	**Sub-nodes**	**Specific Guidelines**
Organization-wide CIS behaviors	Unaware of CIS policies	1. Promote awareness of CIS policies. 2. Maintain a "high security" environment; do not accept various levels of risk or behavior. 3. Monitor organizational behavior over time. Migration toward non-secure behaviors can happen.
	Lack of participation for all levels	
	Accept various levels of risk	
	'Rigid' CIS environment is not maintained	
	Migration towards non-compliance	
Organizational culture issues	Political in-fighting	4. Align corporate support with CIS (see management commitment).
	No alignment between corporate vision and CIS	
	Lack of corporate support	
	CIS runs counter to organizational culture	
	Punitive culture	
Overall perceptions related to CIS	Overall unimportance to CIS	5. Assess the level of importance to CIS in the organization. Is functionality more important than being security? Are there other influences that dictate how CIS is perceived?
	Pressure from customers and public	
	False sense of security	
	Usability is viewed as more important than CIS	
Reward and recognition	Lack of reward and recognition for CIS work	Create reward and recognition systems for secure behavior. Network administrators are group that should be singled out since their work typically involves CIS duties.

<table>
<tr><th colspan="4">Guideline 2: Cultivate and Maintain CIS Culture – 2</th></tr>
<tr><th>Nodes</th><th colspan="2">Sub-nodes</th><th>Specific Guidelines</th></tr>
<tr><td rowspan="8">Management commitment</td><td rowspan="4">Lack of resources for CIS</td><td>Lack of budget or funding</td><td rowspan="8">6. Top management gives resources (e.g., funding, staffing, time) to CIS.

7. Do not favor the functionality of IT systems over CIS goals.

8. Support and training for user groups: CIS managers, CIS designers, network and system administrators, end users.

9. Create opportunities for feedback of problems to management and system designers. The goal of feedback is to reduce inconsistencies in the system and process.

10. Create a “head” of CIS within its own department. The CIS function of an organization should be centralized.

11. Consider various human and organizational factors in relation to CIS systems. Resolving a CIS problem should not involve only a technical solution; it should involve and consider the users’ needs.</td></tr>
<tr><td>Old equipment</td></tr>
<tr><td>Do not support CIS training</td></tr>
<tr><td>CIS viewed as an overhead cost</td></tr>
<tr><td rowspan="4">Lack of upper management emphasis on CIS</td><td>CIS personnel not empowered</td></tr>
<tr><td>Favor functionality over CIS</td></tr>
<tr><td>Undervalued by top management</td></tr>
<tr><td>Lack of management leadership</td></tr>
</table>

Guideline 3: Create and Manage Systematized CIS - 1			
Nodes	**Sub-nodes**		**Specific guidelines**
Lack of CIS management plan	Lack of prioritization of criticality	Do not assign correct criticality to assets	1. Create a prioritized management plan for CIS. The content of a CIS management plan includes: assigning criticality levels to assets, prioritizing resources for CIS, and include CIS in the design and management of IT systems. CIS should not be an afterthought or addressed after an IT system is implemented.
		Lack of prioritization resources	
		CIS is “adhoc”	
		Policies and plans are not tailored to specific needs or priorities	
	Interfaces between organizations and outside networks	Problems connecting to outside networks	2. Manage outside relationships. Vulnerabilities can be introduced in a system when the organization interfaces with other organizational networks. Trust relationships should not be assumed. Outside networks need to be checked for proper CIS levels.
		Consultants with inadequate solutions	
		Trust relationships between organization	
		Lack of procurement process plan	
		Incorrect requisition specification to vendor	
		Outsource CIS function	

Guideline 3: Create and Manage Systematized CIS - 2			
Nodes	**Sub-nodes**		**Specific guidelines**
CIS practices	Systematizing CIS practices	Lack of participation from all organizational levels	3. Develop a participatory process for CIS practices. The participation should include those from every level of the organization. Supporting systems, such as reminder alerts for secure practices, are useful in supporting user performance. This process should be continuous and maintained over time.
		Lack of a reminder system for secure practices	
		Lack of comprehensive mitigation practices	
	Implementing CIS practices	Do not execute secure CIS practices	4. CIS practices should be developed, specified, and emphasized. The process of developing CIS process should be a continuous one and maintained over time. 5. There should be a formal method of implementing CIS practices.
		CIS practices are not emphasized	
		Lack of continuous process for CIS	
		No standardized CIS implementation	
Communication	No cross-departmental communication		6. Develop and maintain communication throughout the organization. Create cross-departmental communication and address problems from a multi-functional perspective. Rarely does a problem affect a single group.
	Interact with bureaucracy		
	Too many organizational hierarchies		
	Poor communication between end users and network administrators		

Guideline 3: Create and Manage Systematized CIS - 3			
Nodes	**Sub-nodes**		**Specific guidelines**
CIS process and performance	No measure of CIS performance	Lack of CIS metrics	7. Develop metrics for CIS performance. The metrics need to be consistent across departments of the organization. Collect input of those measurements at various points in time.
		Inconsistent CIS metrics across department	
	Audits or evaluations	No performance evaluation of personnel	8. Perform audits and evaluation of personnel, policy, and accountability mechanisms. These audits are performed in addition to technical CIS evaluations that check for technical vulnerabilities.
		No policy evaluation in assessments	
		Lack of CIS evaluation or audits	
		Lack of accountability mechanism	
	Systems or life cycle issues	Lack of human factors consideration in CIS lifecycle	9. Consider the various needs of users and human factors over the entire CIS lifecycle.
		Communications breakdowns in implementation	10. Identify communication breakdowns in the system lifecycle. Identify and communicate design requirements across the development group.
		Different assumptions among groups	
		Lack of consideration for the complexities of operations problems	
		Do not communication design requirements	

Guideline 4: Create Sustainability with Human and Organizational Factors			
Nodes	**Sub-nodes**		**Specific guidelines**
CIS process, continued	Sustainable and adaptive CIS processes	Not a sustainable process	1. Recognize that CIS performance degrades over time.
		Lack of cyber-engineering	2. Recognize that there is a lack of cyber-engineering training available.
		CIS does not have consistency in its process	
		Lack of process to implement policies	3. Create processes for implementation, feedback loops for problems, and integrating CIS into the overall workflow.
		Lack of feedback loop(s) for CIS problems	
		Do not consider CIS as part of the workflow	
		Lack of human factors consideration in CIS implementation	4. Consider human and organizational factors in the design and implementation of CIS.
		Difficulties in merging CIS systems processes	5. Consider the complexities of merging architectures, taking into account differences, such as requirements, processes, and data sharing.
		Lack of management planning for CIS	6. Create organizational planning for CIS at the management level.
		Lack of acquisition process for technology	7. Create a formal process for determining the criteria for acquiring new technology.

Guideline 5: Organize the CIS Function within an Organization			
Nodes	**Sub-nodes**		**Specific guidelines**
CIS function	Distributed workers	Lack of criteria for consistent work	1. Create protocol for performing CIS-related duties. This refers to CIS personnel, such as network administrators or system analysts.
		Lack of communication mechanisms	2. Create channels to share information (e.g., threats, viruses, patches) across distributed locations of CIS personnel. They may be in different departments or organizations.
		Lack of consistency in work	3. Create to consistent CIS methodologies and metrics for performance.
	Structure of CIS function	Lack of separation CIS from IT	4. Separate the IT personnel from the CIS staff.
		One brand of software equipment used	5. Use one kind of technology, which may lessen inconsistencies and problems.
		No management position for CIS	6. Create or name leader for the CIS function.
	Centralized versus Decentralized	Lack of centralized CIS function	7. Create a centralized CIS function
		Diffusion of CIS expertise	8. Recognize that CIS expertise may be distributed throughout an organization.
		Benefit of decentralized CIS	9. There may be situations where a decentralized CIS function is valuable. For example, a decentralized CIS function may be more dynamic and nimble to address CIS problems in different locations.

Guideline 6: Develop CIS Training			
Nodes	**Sub-nodes**		**Specific guidelines**
Managing CIS training	Provide little CIS training for employee		1. Provide CIS training that is conducted on a regular basis, mandated in CIS policy, supported by management, and evaluated in employee performance reviews. 2. The content of training should be tailored to the needs of specific user groups. 3. The content of training should be accessible to employees after the training is completed.
	Lack of training policy		
	Lack of upper management support for CIS training		
	No training to remain current with CIS		
	Lack of CIS refresher training		
	Lack accessibility to the information provided in CIS training		
	Training is not a consideration in performance reviews		
	Lack of continuous training		
	Training content not tailored toward different user groups		
CIS Training content	Training content for network administrators	Lack of specific CIS technical training	4. The training content for network administrators should include specific technical aspects of CIS. They should also receive on-the-job training.
		Lack of “hands on” training	
	Training content for end users	Need training with “real life” examples	5. The training content for end users should emphasize real examples and explain why the training content is important (i.e. convey purpose of CIS).
		Training content does note include “why?”	

Guideline 7: Support Network Administrators-1		
Nodes	**Sub-nodes**	**Specific guidelines**
CIS-related knowledge and skills	Do not have "real-life" experience	1. Hire administrators that have experience and expertise, and have been trained in CIS.
	Lack formal CIS training or education	
	Lack of CIS-related expertise and skills	
	Mismatch of skills, task, and job	2. Identify the expertise and skills required of the job. Match the skills of the pool of administrators to the duties and requirements of the job.
Beliefs	Lack of caring for CIS mechanisms (e.g., passwords)	3. Identify and implement ways to recognize and reward the work of network administrators. Network administrators may feel "invisible" to the organization, since they typically do not receive recognition until there is a problem. For example, reward network administrators for maintaining a problem-free environment. 4. Communicate the primary goals of their job in order to help them prioritize their work.
	Lack of regard for end user needs	
	Believe that network administrators need unlimited access	
	Feel undervalued by the organization	
	Misperceptions of job goals	
	Feel "blamed" for CIS problems	
	Exempt from CIS standards, policies	
	Work tasks are more important than CIS	
	Some aspects of CIS are considered "boring"	

Guideline 7: Support Network Administrators - 2		
Nodes	**Sub-nodes**	**Specific guidelines**
Lack of an adversarial mindset	Follow a "rigid" CIS approach	5. Train or provide training for network administrators to think like an adversary. This may include training in additional methodologies, such as attending a hacker's conference or adopting adversarial models.
	Do not realize that adversaries will not attack known CIS policies	
	Rigidity follows engineering training	
	Lacks experience in red teaming	
	Lack of creative thinking	
	Follow a functional perspective	
	Incorrect absent adversary model	
	Lack of red teaming for human and organizational factors in CIS	
Workload	High workload	6. Create support mechanisms to combat the high workload of network administrators. Network administrators tend to take short cuts when faced with too much work.

Guideline 8: Support End Users			
Nodes	**Sub-Nodes**		**Specific guidelines**
CIS-related knowledge	Do not understand CIS policies		1. Provide CIS training and education opportunities for end users. Training should include "real life" examples and how problems in CIS can affect their jobs and the well-being of the organization.
	Lack of general CIS-related knowledge		
Beliefs	Belief that CIS does not affect their job		
	Do not have a stake in CIS performance		
	Describes end users placing a higher priority on completing their work tasks rather than adhering to CIS practices and principles.		
	Relaxed attitude toward beliefs		
	Do not understand "why" CIS is important		
	Lack of respect toward CIS personnel		2. Create communication mechanism for end users and network administrators to communication about needs, problems.
Behaviors	Not precise or thorough		3. Evaluate and audit CIS-related performance of end users. For example, audit the password management of end users. 4. Create a reward and recognition system for secure behaviors and practices.
	Share secrets		
	Routine Violations	Workarounds	
		Violations of policy	