Human Factors in E-Security – The Business Viewpoint

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

The US Department of Defense is providing funding for this project (PI: Professor S. Robinson; Grant number: DAAD19-01-1-0502; ARO proposal number: 42347-MA-CIP).

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

November 2003

CQPI Technical Report No. 184

Workgroup Participants

Julie Esser, Product Manager, CUNA & Affiliates
Bob Ferderer - Vice President of Information Technology, CUNA Mutual
Beth Griffin - Product Manager, CUNA & Affiliates
Mike Kleckner, Information Security Specialist, American Family Insurance
Gary Laszkiewicz - Security Manager, Brady Corporation
Leslie Peckham, Information Security Specialist, American Family Insurance

Pascale Carayon, Professor of Industrial Engineering, Director of the Center for Quality and Productivity Improvement, UW-Madison
Raj Veeramani, Professor of Industrial Engineering, Director of the Consortium for Global Electronic Commerce
Sara Kraemer, Graduate Student in Industrial Engineering, UW-Madison
Sommer Alexander, Undergraduate Student in Industrial Engineering, UW-Madison

Meeting Schedule

Meeting	Date
Workgroup launch: Workgroup goal formulation.	October 18, 2002
Meeting #2: ROI on security.	November 1, 2002
Meeting #3: Vulnerabilities of value chain and associated human and organizational factors.	December 18, 2002
Meeting #4: Vulnerabilities of value chain and associated human and organizational factors.	January 7, 2003
Meeting #5: Best practices for human and organizational factors associated with the vulnerabilities on the value chain.	January, 28, 2003
Meeting #6: Best practices for human and organizational factors associated with the vulnerabilities on the value chain. Identification of the components of security culture.	February 28, 2003

Executive Summary

One of the greatest barriers to effective e-security are the human and organizational factors that contribute to and cause the technical and social vulnerabilities of an organization's computer and information system. The purpose of this workgroup was to explore the most critical human and organizational factors facing e-security, to identify methods used to characterize those factors, and to examine best practices in attempt to relieve or solve these problems.

A risk model for categorizing e-security assets in need of protection is presented. This risk model was introduced to prioritize the critical areas of an organization, in terms of needing the most protection from outside attacks. The vulnerabilities were identified in the risk analysis. Then, two taxonomies of vulnerabilities were introduced, and are discussed in detail in chapter three.

Human and organizational factors were identified with each vulnerability. The most important factors identified were: policy, training, management commitment, communication and feedback, and culture. The workgroup stratified the vulnerabilities into three groups by level of criticality. Group one includes access control, patch management, and anti-virus protection. Group two includes backups, application design, asset classification, and password management. Group three includes contingency planning, content management, data control, enterprise architecture, and transaction log analysis. Companies in the working group identified best practices for vulnerabilities of groups one and two.

Best practices are discussed in chapter five. Chapter six identifies the dimensions of security culture, such as intrinsic motivation, employee buy-in, and management commitment. Understanding the connection among vulnerabilities, human factors, and best practices that ultimately enable security culture was explored by the workgroup.

TABLE OF CONTENTS

CHAPTER 1 - HUMAN FACTORS IN E-SECURITY

1.1 What are the workgroup member's current perspectives?

Professor Carayon has brought her expertise in human factors research to the realm of computer and information security. Professor Carayon's expertise does not lie in the technical aspects of security computer and information systems. Her expertise lies within the organizational and human factors of workplace design, as applied to computer and information security. This research is conducted under the auspices of a larger research initiative funded through the Department of Defense[1]. This project began in May 2001 and will end in May 2004.

Workgroup members identified many human and organizational factors. At the onset of this workgroup, some of the most important issues and questions to carry forward included:

1. Establishing a common security language.
2. Employee acceptance of security (security culture), especially at the grassroots level.
3. Defining safe vs. unsafe employee behavior.
4. Security "mistakes" made by employees.
5. Lack of management involvement for successful institution and deployment of e-security policy.
6. What is the ROI (return on investment) on e-security? E-security ROI is difficult to formulate.
7. How do we build a successful business case for e-security for the purposes of management buy in?
8. E-security is not proactive.
9. Most of the company's management lack IT expertise, and consequently there is a relatively low e-security awareness.

1.2 Workgroup goals and scope

Given the above interest, the workgroup formulated the following goals and scope.

1. How do we conduct a risk assessment on human factors in e-security? What is the ROI (return on investment) on e-security? What are the ways to build a business case for e-security?
2. What are the general issues of human factors in e-security?
3. What are the best practices/guidelines for human factors in e-security?
4. What are the components of security culture?

Given these goals, we examined these issues in three different ways. First, we examined what were at risk, namely, the assets to be protected that may be at risk (Chapter 1). Second, we discussed the vulnerabilities associated with different assets, and the human and organizational factors involved in those vulnerabilities (Chapters 3 and 4). We, then, focused on best practices for the most critical vulnerabilities (Chapter 5). Finally, we discussed the issue of computer security culture (Chapter 6).

[1] DOD/ARO Project: Modeling and Simulation Environment for Critical Infrastructure Protection, PI: S. Robinson, Grant number: DAAD19-01-1-0502, ARO proposal number: 42347-MA-CIP

CHAPTER 2 - RETURN ON INVESTMENT FOR E-SECURITY

2.1 Introduction

The return on investment for e-security involves a five-phase approach of (1) system and inventory definition, (2) vulnerability threat assessment, (3) evaluation of controls, (4) decision, and (5) communication and monitoring (see Figure 1). This risk analysis model includes identifying and assessing both the technical and organizational components to e-security (Brooke, 2000; Center for Strategic and International Studies, 2002).

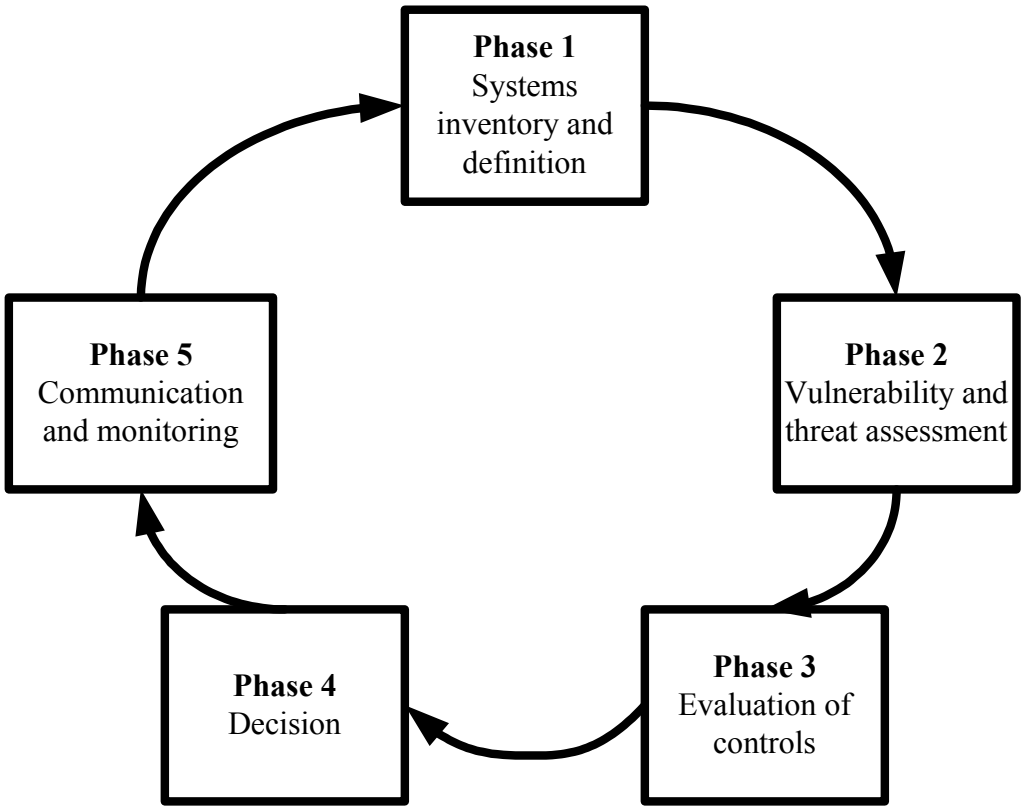

Figure 1. A Risk Model for E-Security, adapted from Brooke, 2000

2.2 Phase 1: Systems inventory and definition

This step involves the determination of **assets** (i.e. network components, servers, data, etc.) that are involved in critical business processes. After the business-related systems have been identified, their value is assigned. This step is a prioritization phase, in which the assets are given an order or importance or criticality. Some questions to guide this thinking include:

1. What is the monetary impact if critical systems are removed from service due to denial of service or failure?
2. What is the monetary impact if data integrity or confidentiality is compromised as a result of a virus or an attack?
3. What is the impact on customer loyalty and retention, brand value, and future transactions if a violation occurred?

2.3 Phase 2: Vulnerability and threat assessment

The aim of this phase is to examine the system for weaknesses that could be exploited. The prioritization done in Phase 1 guides the vulnerability assessment in Phase 2. Vulnerability assessments must be conducted against established performance standards in order to determine priorities for resources to mitigate risk. Once a list of vulnerabilities per system is compiled, each vulnerability should be classified according to the probability that it could be exploited. The human and organizational factors are also identified and assessed with the technical analysis.

Questions to answer include:

- What are the organizational issues surrounding vulnerabilities that have been identified as important threats to important business processes?
- What are the organizational components surrounding the key business processes and organize the enablers and barriers to e-security in these processes?

2.4 Phase 3: Evaluation of controls

Phases 1 and 2 provide a framework to link the measure of risk to potential business impact of a violation of that asset of area of risk. Phase 3 establishes a business case for or against the implementation of security "controls" such as firewalls, and authentication systems. Controls are aimed at reducing risk levels that are acceptable to the business. The implementation of controls is a risk/value proposition because all controls have an associated cost. Some factors of cost to consider are: acquisition, implementation, maintenance, usability, scalability, and performance. This analysis links the business cost of vulnerabilities/threats to that of the cost of implementing a control in the system. These controls include both technical e-security controls and organizational controls (e.g., training, policy development).

2.5 Phase 4: Decision

This phase is a formal method for implementing and documenting the decision process and provides an opportunity for buy-in from business management. During this phase one is evaluating the cost of a set of controls versus the value of the processes, systems, and information that are protected. Further, determinations of the effectiveness of both the technical and organizational controls are assessed, and a decision to address those issues is made accordingly.

2.6 Phase 5: Communication and monitoring

This phase includes creating user awareness and management buy-in at the implementation stage. At this stage, a sound strategy and effective deployment of the new control in the system is developed.

2.7 Categories of assets/elements that need protection

The types of asset categories may be different in different organizations, especially when identifying the type of data stored and processed. Therefore, the prioritization (in terms of needing protection) of those categories may be different for organizations.

Six categories of assets or elements can be identified:

1. An assessment of the internal network should include an analysis of both the *application servers* and *network services*.
2. The web servers need analysis of the *business processes* they support as well as the *operations* in which these processes function.
3. The company data in need of protection should be assessed and prioritized. Some examples of the types of data that need protection include: non-public personal customer information, health information, customer lists (either person or company, or both), corporate proprietary knowledge, technical system/network information, and employee data. Again, the criticality of these categories of data is dependent upon the type of organization and strategic goals of the organization.
4. Employees need protection. The issues surrounding employee protection include *uninvited contacts* and *productivity* issues.
5. Corporate resources are also elements that need attention and protection. The human capital components to this area include *disgruntled employees* and *corporate culture.*
6. Business-specific intellectual capital includes strategic planning, new product development, business relationships, design patents and company policies, procedures and the implementation of those policies and procedures.

2.7.1 Potential impact if assets are not protected

The criticality of assessing the assets is culminated in identifying the potential impact if assets are not protected. The priority of these potential impacts is largely dependent upon the strategic intent and planning of the organization. Some of the areas that may be affected, not in order of importance, include:

1. Productivity: the business and corporate operations, information, and data corruption.
2. Corporate image: business inaccessibility for customer, supplier, and employee, marketplace image, and competition resulting in business loss.
3. Legal involvement: including privacy exposure, lawsuits, fines, and extortion.
4. Regulation: including privacy/HIPA exposure.
5. Outside attack: including hackers who both sabotage and steal corporate knowledge, assets, etc…
6. Customers: compromised identity and confidentiality.

2.8 Value chain for information assets

The working group developed the concept a value chain for information assets (see Figure 2). This concept was created in order to (1) show the links of behavior and the different types of behavior, (2) organize the discussion on vulnerabilities, and (3) differentiate the elements among business assets. The value chain provided a framework for the components of e-security that could cause the most severe problems for an organization. The workgroup concluded that data is one of the most important parts to consider. Recognizing the ever-changing nature of the technical and organizational components, the analysis done in conjunction with a "Value Chain for Information Assets" was created to clarify the discussion of vulnerabilities. Vulnerabilities were identified for each element of the value chain.

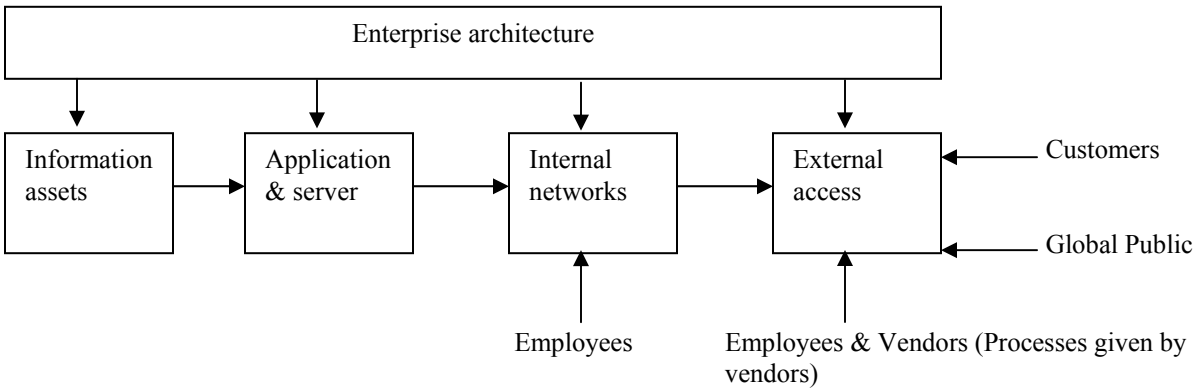

Figure 2. Value Chain of Information Assets

2.8.1 Information assets

Information assets were determined by the workgroup as strategically important. As mentioned above, this includes:

- Non-public personal customer information
- Health information
- Customer lists (either person or company, or both)
- Corporate proprietary knowledge
- Technical system/network information
- Employee data
- Intellectual capital such as strategic planning information, new product development, business relationships, design patents, company policies, and procedures which also include the implementation of those policies and procedures.

2.8.2 Application and server

Application and server include the types of applications used in conjunction with the information assets, as well as the type, structure, and configuration of the server, as it relates to information assets.

2.8.3 Internal networks

The internal networks include the technical aspects of the configuration of the network, inside of the organization. *Employees* have been identified as those who have both a direct and indirect link to this aspect of the value chain.

2.8.4 Enterprise architecture

The full design, or enterprise architecture, is the overarching system design.

2.8.5 External access

External access refers to the accessibility of the organization's technical infrastructure. This includes assessing who has access to the internal infrastructure and how access to this infrastructure is possible. *Employees*, *vendors, customers,* and *the global public* were identified as having external access to the organization's internal infrastructure, and therefore should be considered when assessing the human and organizational factors associated with technical vulnerabilities in e-security.

2.9 Conclusion

Once the value chain and the interactions were identified, we addressed the following questions. First, what are the different vulnerabilities associated with information assets? After the vulnerabilities have been identified, they need to be mapped to the impact on business if those assets are compromised. Second, once the vulnerabilities are identified, what organizational issues should be addressed? One need is to identify the organizational "controls" in place, or absent, to further address what issues are at the forefront of improving the organizational components to e-security. Two questions to consider at this point are: Is there a framework for operation? and Are there methods to evaluate? One way to stratify and categorize vulnerabilities is with the use of taxonomies of vulnerabilities.

CHAPTER 3 - TAXONOMIES OF VULNERABILITIES

3.1 Introduction

We explored the published literature for taxonomies of vulnerabilities. A taxonomy was presented to distinguish how similar or dissimilar vulnerabilities are to one another. Using the Value Chain of Information Assets, we addressed the vulnerabilities associated with each component of the Value Chain. We addressed the following questions:

1. What are the different vulnerabilities associated with the different assets of the value chain, and what are their impact?
2. Once the vulnerabilities are identified, what are the human factors and organizational issues related to the vulnerabilities?

The taxonomies presented to the workgroup members do not reflect their current technical approach. Therefore, these taxonomies were not used to categorize vulnerabilities. We included the two taxonomy models for future thinking and use by workgroup members and other interested parties.

In order to organize our meeting activities, we have mapped workgroup findings to the ROI security model. In each chapter, the highlighted box will identify where workgroup activities fall on the ROI security model (see Figure 3). In this chapter, the proposed vulnerability taxonomies comprise Phase 2 of the ROI model. Assessing vulnerabilities, as well putting them into meaningful categories, may be a part of evaluating the current status of security, specifically vulnerabilities. Since the workgroup did not draw any conclusive considerations regarding taxonomies of vulnerabilities, the dashed line indicates an indirect relationship.

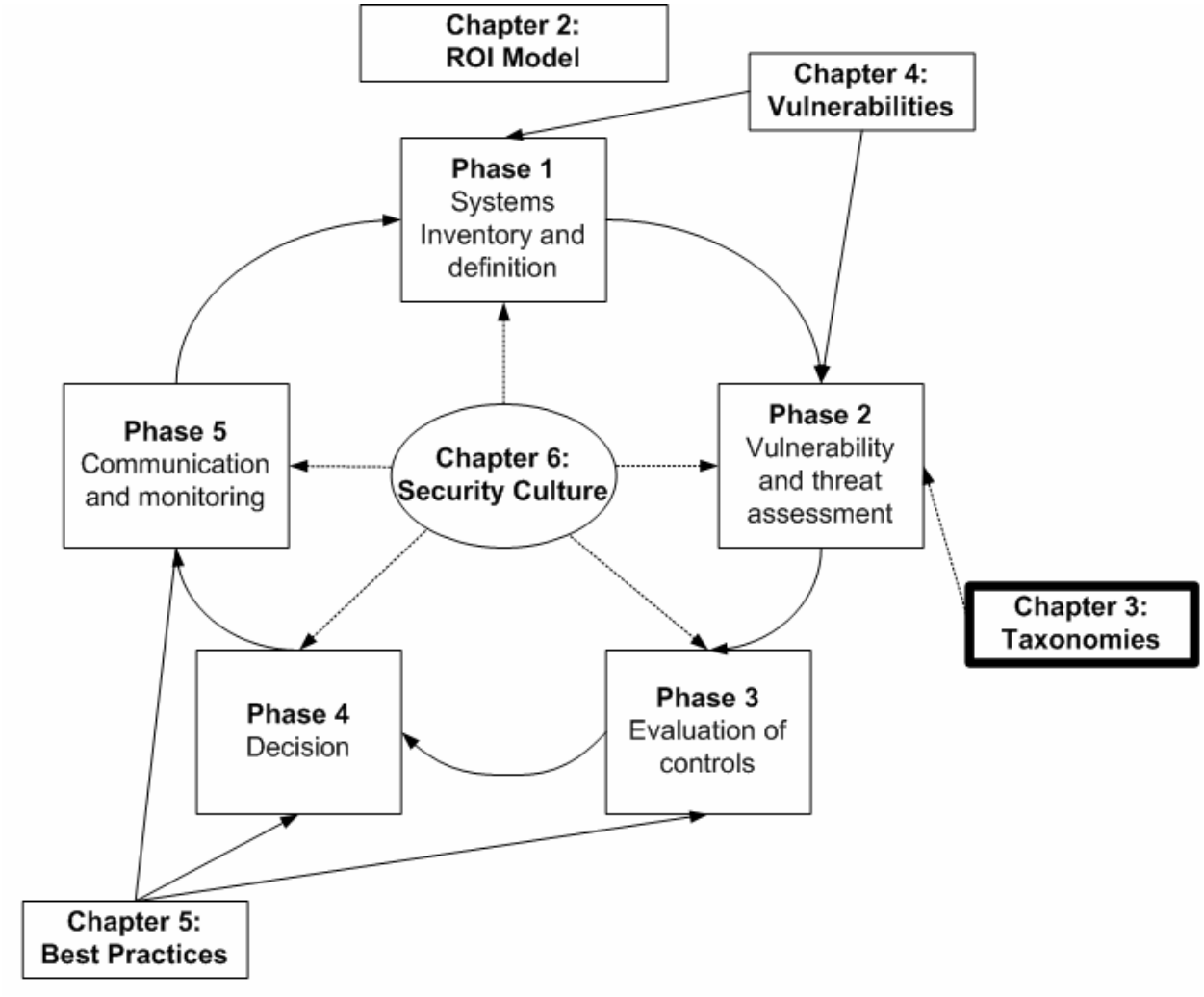

Figure 3. ROI on E-Security, Highlighting Taxonomies

3.2 Two taxonomies of computer and information security vulnerabilities

We looked at published literature for taxonomies of vulnerabilities to help us distinguish how similar or dissimilar the vulnerabilities are to each other (Landwehr, Bull, & McDermott, 1994). Taxonomies of characteristics of computer vulnerabilities provide a systematic organization for security vulnerabilities. The vulnerabilities are identified by the how, when, where questions associated with security vulnerabilities. Landwehr et al. (1994) developed three taxonomies for vulnerabilities to answer three basic questions about each observed vulnerability, or flaw:

1. How did it enter the system (genesis)?
2. When did it enter the system (when)?
3. Where in the system is it manifest (location)?

The taxonomy by Landwher et al. (1994) was chosen because it includes elements that are consistent with human error categorization.

The second taxonomy by Howard & Longstaff (1988) addresses the linkage of actions or outcomes to security vulnerabilities. This taxonomy was useful to describe the consequences of attackers' actions.

3.3 A taxonomy of computer program security flaws

3.3.1 Security vulnerabilities by genesis

<table>
<tr><td rowspan="8">Genesis</td><td rowspan="6">Intentional</td><td rowspan="4">Malicious</td><td rowspan="2">Trojan Horse</td><td>Non-replicating</td></tr>
<tr><td>Replicating (virus)</td></tr>
<tr><td colspan="2">Trapdoor</td></tr>
<tr><td colspan="2">Logic/time bomb</td></tr>
<tr><td rowspan="3">Non-malicious</td><td rowspan="2">Covert Channel</td><td>Storage</td></tr>
<tr><td>Timing</td></tr>
<tr><td colspan="2">Other</td></tr>
<tr><td rowspan="5">Inadvertent</td><td colspan="3">Validation error (incomplete or inconsistent)</td></tr>
<tr><td colspan="3">Domain error (including object re-use, residuals, and exposed representation errors)</td></tr>
<tr><td colspan="3">Serialization/aliasing</td></tr>
<tr><td colspan="3">Identification/authentication inadequate</td></tr>
<tr><td colspan="3">Boundary condition violation (including resource exhaustion and violable constraint errors)</td></tr>
<tr><td colspan="3">Other exploitable logic error</td></tr>
</table>

Figure 4. Security Flaw Taxonomy: Flaws by Genesis (Landwehr et al., 1994)

The above Genesis Taxonomy represents how a security flaw or vulnerability finds its way into a system (see Figure 4). It may be introduced *intentionally* or *inadvertently.* Different strategies may be used to avoid, detect, or compensate for accidental flaws as opposed to those inserted intentionally. *Malicious* flaws are those *intentionally* introduced into the system for the purposes of destruction or damage. Examples of this type of flaw are *Trojan horse, trap-door, time-bomb,* and *logic-bomb*. *Non-malicious* flaws are those *intentionally* introduced into the system by *covert channels.* Covert channel is a path to transfer information in a way that was not intended by the system's designers. They are categorized as intentional, but non-malicious, because they frequently arise in resource-sharing services that are intentionally part of the system. Unlike their creation, their exploitation is likely to be malicious. Covert channels are frequently classified as either *storage* or *timing* channels.

Inadvertent flaws are those that occur in requirements, as well as specification and coding. *Validation errors* occur when the program fails to check that the parameters supplied or returned to it conform to its assumptions about them, or when these checks are misplaced, so they are ineffectual. *Domain flaws*, which correspond to "holes in the fences", occur when the intended boundaries between protection environments are porous. A *serialization flaw* permits the asynchronous behavior of different system components to be exploited to cause a security

violation. An *identification/authentication flaw* is one that permits a protected operation to be invoked without sufficiently checking the identity and authority of the invoking agent. *Boundary condition flaws* reflect omission of checks to assure that constraints are not exceeded, typically leading to crashes. *Other exploitable logic errors* is a catchall category that includes bugs that can be invoked by users to cause system crashes, but do not involve boundary conditions (this would be an example placed in this category).

3.3.2 Security vulnerabilities by time of introduction

<table>
<tr><td rowspan="4">Time of introduction</td><td rowspan="3">During development</td><td>Requirement/specification/design</td></tr>
<tr><td>Source code</td></tr>
<tr><td>Object code</td></tr>
<tr><td colspan="2">During maintenance</td></tr>
<tr><td colspan="2">During operation</td></tr>
</table>

Figure 5. Security Vulnerability by Time of Introduction (Landwehr et al., 1994)

This taxonomy explains how vulnerabilities can be introduced in three different phases: the *development* phase, which covers activities leading to changes in the software, the *maintenance* phase, which covers activities leading to changes in the software performed under configuration control after the initial release, and the *operational* phase, which covers activities to patch software while it is in operation, including unauthorized modifications (e.g., by a virus) (see Figure 5). During development, *requirements errors* occur when there is an error in describing *what* a particular program or system of programs must do. *Specification errors* are *how* the program or system is organized to meet those requirements (i.e. the software design) is typically recorded in a variety of documents. *Source code* implements the design of the software system given by the specifications. Inadvertent flaws in source codes are frequently a by-product of inadequately defined module or process interfaces. *Object code* errors are primarily a concern of malicious error, since most compilers and assemblers are subjected to extensive testing and

validation procedures before release. During *maintenance,* inadvertent flaws that are introduced are often attributed to the programmer's failure to understand the system as a whole. During *operation,* the need for the security analyst to consider the possibilities for unauthorized modification of operational software during its operational use. Viruses are not the only means by which modifications can occur: depending on the controls in place in a system, ordinary users may be able to modify the system software or install replacements.

The value of this taxonomy is investigating the general question of how and when vulnerabilities are introduced into the software. The categorization provides focus to where efforts should be placed to improve the processes, as well as the organizational and human factors that contribute to each group of vulnerabilities. Similar vulnerabilities have similar causes, and narrowing the type of vulnerability also narrows the types of improvements to be made.

3.3.3 Security vulnerabilities introduced by location

<table>
<tr><td rowspan="10">Location</td><td rowspan="9">Software</td><td rowspan="6">Operating system</td><td>System initialization</td></tr>
<tr><td>Memory management</td></tr>
<tr><td>Process management/scheduling</td></tr>
<tr><td>Device management (including I/O, networking)</td></tr>
<tr><td>File management</td></tr>
<tr><td>Identification/authentication</td></tr>
<tr><td>Other/unknown</td></tr>
<tr><td rowspan="2">Support</td><td>Privileged utilities</td></tr>
<tr><td>Unprivileged utilities</td></tr>
<tr><td colspan="2">Application</td></tr>
<tr><td colspan="3">Hardware</td></tr>
</table>

Figure 6. Security Vulnerability by Location (Landwehr et al., 1994)

Software flaws can occur in operating systems, support software, or application (user) software (see Figure 6). *Operating system* normally includes memory and processor allocation, process management, device handling, file management, and accounting, although there is no standard definition. The operating system security flaws are stratified in the following ways. *System initialization* flaws occur either because the operating system fails to establish the initial

protection domains as specified or because the system administrator has not specified a secure initial configuration for the system. *Memory management* and *process management* errors permit one process to gain access to another improperly or deny service to others. *Device management* errors occur when the I/O routines fail to respect the parameters provided to them or when they validate parameters provided in storage locations that can be altered, directly or indirectly, by user programs after checks are made. *File system* errors are errors in the controls that permit users to share and protect their files, or errors in the management of underlying files. *Identification/authentication* errors occur in the maintenance of special files for user IDs and passwords and providing functions to check and update those files as appropriate.

The *support software* comprises compilers, editors, debuggers, subroutine or macro libraries, database management systems, and any other programs not properly within the operating system boundary. *Privileged utilities* are often complex and sometimes provide functions that were not anticipated when the operating system was built. *Unprivileged utilities* can represent a significant vulnerability because these programs are widely shared, and users tend to rely on them implicitly. The damage inflicted by flawed, unprivileged support software (e.g., by an embedded Trojan horse) is normally limited to the user that invoked the software. *Application software* errors cause damage by inadvertent software flaws at the application level usually restricted to the executing process, since most operating systems can prevent one process from damaging another. *Hardware errors* include the design and implementation of processor hardware, microprograms, and supporting chips, and any other hardware or firmware functions used to realize the machine's instruction set architecture.

3.4 A common language for computer security incidents

A taxonomy developed by Howard and Longstaff (1998) builds upon the above taxonomy to identify and provide a linkage between actions and outcomes of incidents and attacks (see Figure 7).

Some working definitions to the model:
A. Incident: A group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing.
B. Attack: A series of steps taken by an attacker to achieve an unauthorized result.
C. Event: a discrete change of state or status of a system or device. In computer and information security, an event is a change in state resulting from *actions* that are directed against specific *targets.*

D. Attacker: An individual who attempts one or more attacks in order to achieve an objective.
E. Tool: A means of exploiting a computer or network vulnerability.
F. Vulnerability: A weakness in a system allowing unauthorized action.

- **a. Design vulnerability:** a vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability.
- **b. Implementation vulnerability:** A vulnerability resulting from an error made in the software or hardware implementation of a satisfactory design.

c. Configuration vulnerability: A vulnerability resulting from an error in the configuration of a system, such as having system accounts with default passwords, having "world write" permission for new files, or having vulnerable services enabled.

G. Action: A step taken by a user or process in order to achieve a result, such as to probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify, or delete.

H. Target: A computer or network logical entity (account, process, or data) or physical entity (component, computer, network or Internet work).

I. Unauthorized result: An unauthorized (not approved by the owner or administrator) consequence of an event.

This incident taxonomy demonstrates the relationship of events to attacks and to incidents, and suggests that preventing attackers from achieving objectives could be accomplished by ensuring that attackers cannot make any complete connections through the steps depicted.

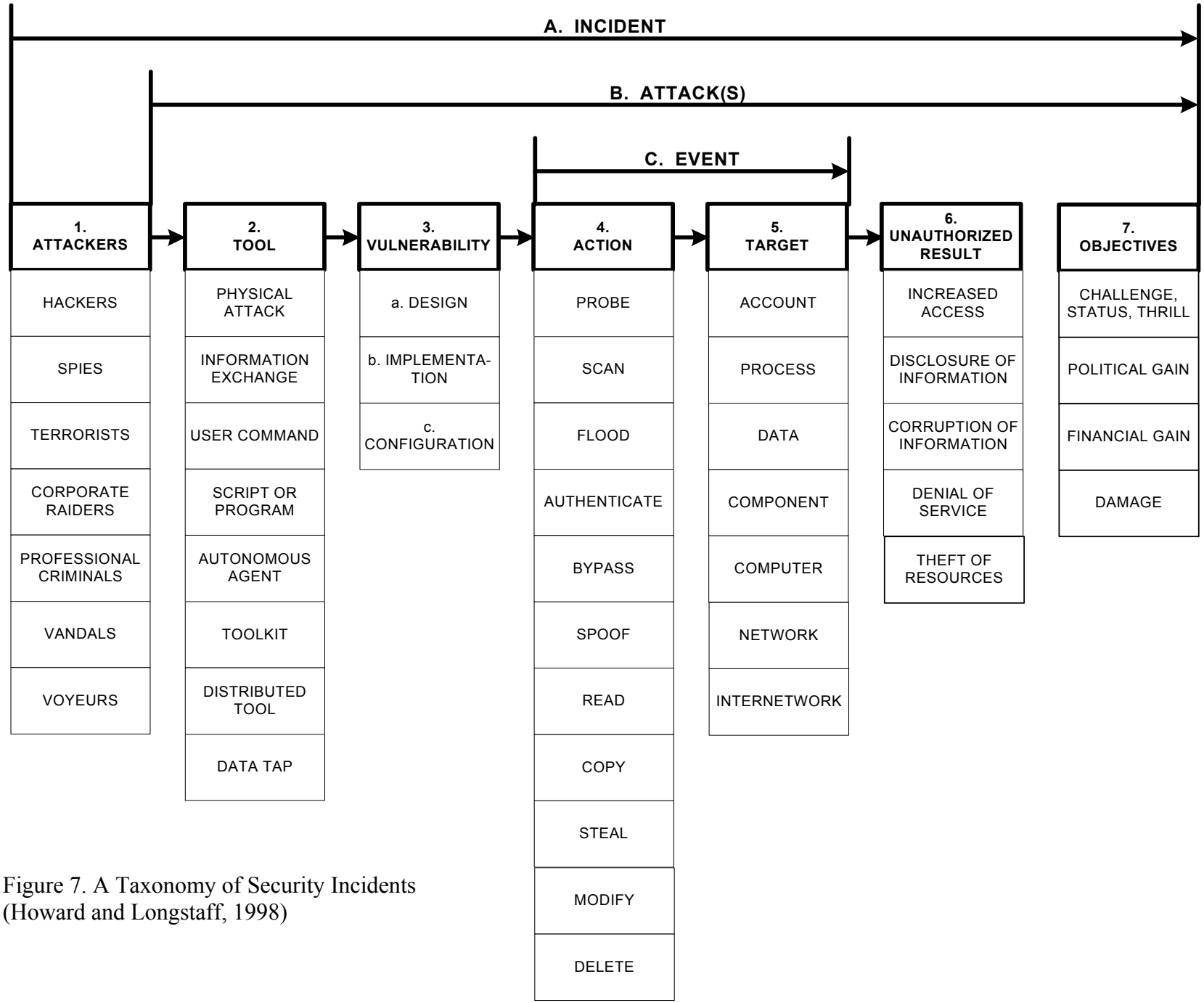

Figure 7. A Taxonomy of Security Incidents (Howard and Longstaff, 1998)

3.5 Conclusion

These two examples of taxonomies provide stratification of types of vulnerabilities and clarify the types of errors associated with them. From a human and organizational standpoint, we may use these classifications to group the human factors issues contributing to the errors that predicate the security vulnerabilities, thus creating groupings of organizational issues. In this manner, we may now be able to combine and compare these factors, and consequently, make adjustments and improvements in the organization accordingly.

CHAPTER 4 - VULNERABILITIES ON THE VALUE CHAIN

4.1 Introduction

The workgroup classified the vulnerabilities associated with each piece of the value chain elements and identified the human and organizational factors associated with those vulnerabilities (see Figure 9). All this information was inserted into a table that could be used to combine and compare the factors to one another, and across categories of factors (see Table 1). Best practices to deal with the issues identified in the human and organizational factors analysis are discussed in the following chapter.

In relation to the ROI model, identification of vulnerabilities on the value chain is part of Phase 1: Systems and inventory definition and Phase 2: Vulnerability and threat assessment (see Figure 8). Identification of vulnerabilities on the value chain is related to Phase 1 because the value chain identifies the security system and defines what is important to the information assets. Identification of vulnerabilities on the value chain is related to Phase 2 because vulnerability identification is one of the two major components to Phase 2.

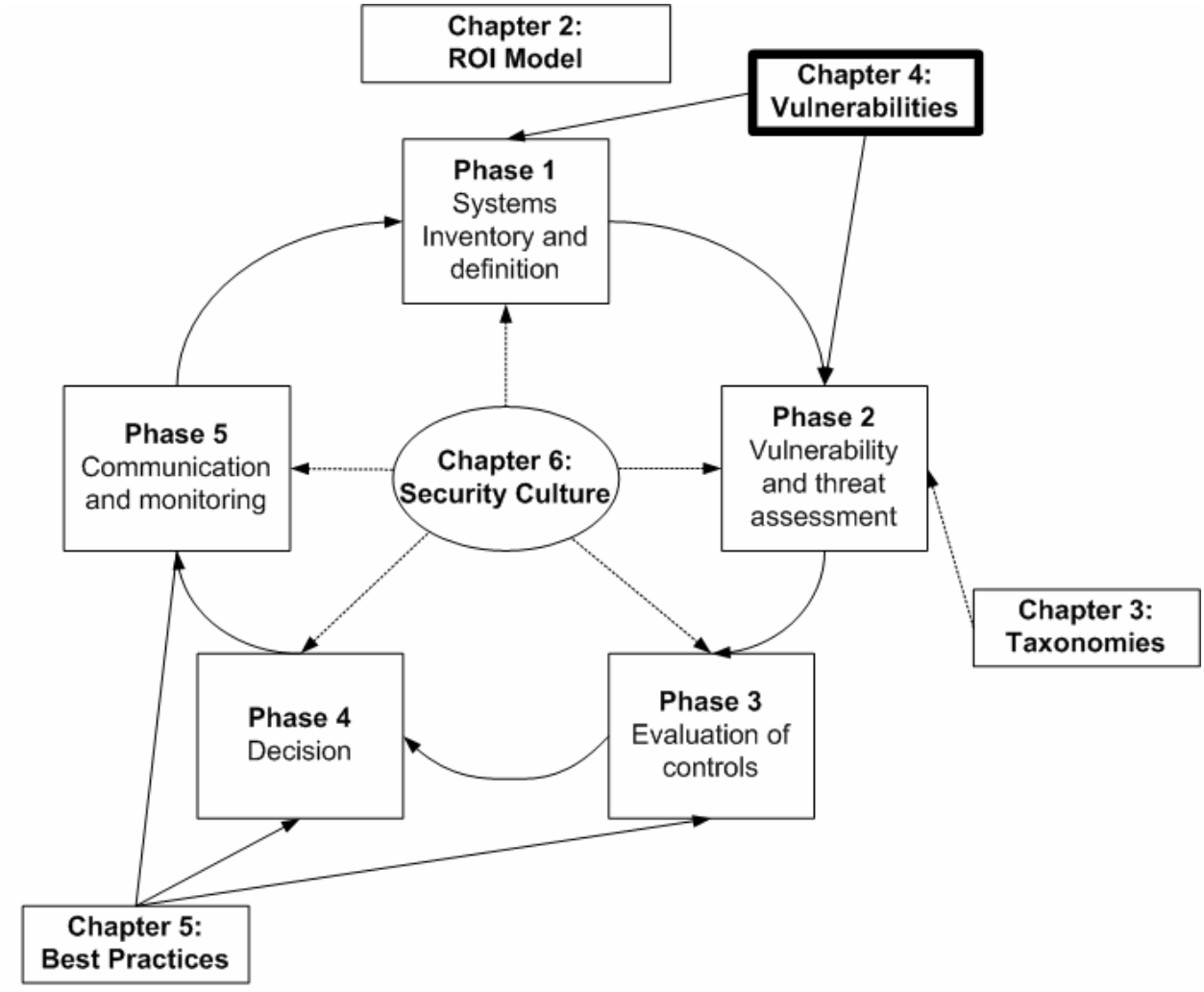

Figure 8. ROI in E-Security Model, Highlighting Vulnerabilities

4.2 Vulnerabilities on the value chain

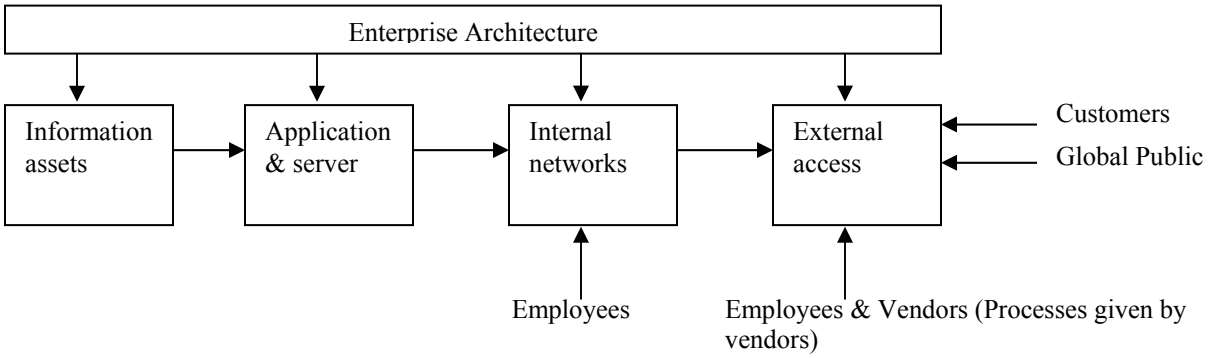

Figure 9. Value Chain of Information Assets

4.2.1 Information assets

Vulnerabilities associated with information assets include:

1. *Content management*. What is present, what is secure, such as credit card numbers-these may be called "customer vulnerabilities".
2. *Poor access control*. This addresses application: Who has access to information? Do the appropriate people have access to the information? There are different levels of information that must be recognized and attended to.
3. *Inadequate asset classification.*

Policy formulation and development was identified as a major human/organizational factor related to information asset vulnerabilities. Some of these issues include:

1. Is the organization policy orientated? If yes, how are the policies communicated? How do we test that employees know the policies?
2. There needs to be training and continuous training for policy. This includes reminders, posters, newsletters, etc… Users need to understand the risks associated with performing job tasks with information technology.
3. Attestation is the employee's responsibility. There may be documents for the employees to sign to corroborate their knowledge of security policy.
4. Policy cuts across the organization. Content may differ in some ways for end users versus IT professionals.
5. Policies, for the most part, address internal networks (such as passwords). They do not usually address applications and servers.
6. Policies will address both the technical assets (network configurations, passwords) and business information (customer data) in the same way, but the impact will be different. Therefore, the training for the policies and methods will be different. The training will address the different impact the technical support employees and the business end users have on the technical assets.

4.2.2 Application and server

Vulnerabilities associated with application and server include:

1. Poor/missing configuration plan.
2. Physical control/security.
3. Inadequate data control.

4. Poor application design.
5. Insufficient/lack of security audit.
6. Default software.
7. Installing operating systems (OS) without removing default software settings.
8. Patches need to be applied appropriately and in a timely way.
9. Backups not performed and recovery not tested.
10. Lack of anti-virus protection.
11. Password management: Passwords may not be changed and/or passwords may be weak.
12. Intrusion detection on host.
13. Transaction log analysis: This includes both the server and application.

Human and organizational factors associated with *access control* include:

1. *Training:* the education on responsibilities and the importance of employee responsibilities.
2. *Design* is the degree of difficulty to control the system (i.e. high complexity-not "people orientated" to simple-no control).
3. *Pressure* includes time pressure from management, assumed "laziness" of employees regarding their passwords, and conflict between system repair/management and usability. An example of usability is that most systems are shipped to consumers with different password mechanisms and managing and attempting to simplify and integrate the password system is completely dependent upon system requirements.
4. *Missing contingency planning* (disaster recovery plan) was an identified weakness. An example of a missing contingency plan is when a lot of servers go down, and there is no recovery plan. This poses the question: Why do organizations not have a contingency plan? In smaller organizations, there is too much to do. As the company grows, this becomes more relevant. There is a need for management support to develop contingency plans. The key human and organizational issues are workload, time, and money. Management needs to prioritize and link workload, time, and money together to achieve a successful contingency plan.

Human factors issues with inadequate *data control* include:

1. Weak *sign-in control*.
2. *Safety culture*: Good physical control of the organization is good for information control. Good physical control sets the standard for behaviors and actions, and sets an example for information control.
3. *Employee awareness and attitude*: Creating culture to foster awareness and positive attitude toward security.
4. *Passwords*: This includes internal change of the password within the company, as well as the policy, procedure, verification, process, and installation of "good passwords".
5. *Poor application design:* Internal organization application design versus vendor application design (purchasing applications) may be designed poorly or may not designed to work functionally together. When purchasing applications from a vendor, it would be advantageous to have a checklist of requirements.
6. *Patch management* issues include workload. For example, one company has employees that alert the security professionals to vulnerabilities, and this process is overwhelming. Management often underestimates the speed of technology improvements and the amount

of effort required to maintain secure systems. Three questions that need to be answered are:

- Who is in charge of this, who owns this process?
- Who is notified of patches/vulnerabilities?
- How do you test the patch? As volume of tasks related to patch management increases, the complexity of administering all of the tasks also increases. Further, there are difficulties in both *implementation* and *design* of the patches. The security professionals need to know what is installed on the machine and who has access to information on machine. The task of tracking patches may be outsourced. There are also email lists such as CERT®, Microsoft Security Bulletin, and TruSecure, which provide specific information and risk levels. Red teams are also used for external assessment. Red teams require very high levels of trust by the organization.

7. *Backup vulnerability* includes performing backups on systems. Often, these backups are not performed frequently enough, and end users are those who are primarily the ones who should be performing the back up. This is mainly due to high workload, a perceived low risk, a lack of caring since it is not their data, and a difficult process that is not user-friendly. Issues surrounding this process are:
   - How much information do you keep, and still remain effective?
   - Communication to functions of the organization regarding the backup tasks: is it effective, not effective?
   - How do you know when the backup is completed?
   - What is the verification that it has been backed up?
8. *Anti-virus protection*. The workgroup agreed that there is no reason for not having anti-virus protection. If it were not for lockdown, an employee (end user) might turn off the anti-virus protection. One company uses Symantec™ and can scan all PCs and laptops for anti-virus. Snort™ is one useful tool in dealing with viruses.
9. The *intrusion detection* vulnerability has several factors, such as organization, process, and pattern recognition. Some questions to consider here are:
   - How is intrusion detection organized?
   - What is the process to follow?
   - How do we follow up with intrusion detection?
   - How do we recognize the difficult patterns, since there is too much information?
   - In this area, staffing is an important issue because employees need expertise and experience to go through the system to realize improvement in security.
10. *Transaction log analysis* issues involve managing the volume in the number of logs, monitoring the integrity of data and the access of people who could manipulate the data, deciding what information to keep (which depends on the criticality of the machine-with the exception of highly-critical machines, there is a need to keep a minimum of logs and copies), protecting of logs because they are valuable forensic information, having people specifically assigned to this task, and having a policy articulating the requirements of how long a log should be kept. Transaction log analysis does not include analysis of application logs. The person who administers the source logs usually performs the task of application log analysis. These last two points address a design issue; there should be appropriate space to store the logs. Further, these logs may be highly sensitive, which is determined by the business requirements (sensitivity and criticality).

Password management is a large issue. Password policy needs to ensure the protection of assets from the individual so that it cannot be easily guessed or spoofed (faked). All access needs to come in uniquely, under an ID and password for every activity that occurs. There needs to be a policy on the frequency of changing passwords. The training and awareness of the importance of passwords needs to be articulated. This is very important because the individual using the password chooses it. Therefore, there should be regular training for new and current employees on how to pick "good" passwords and how frequently to change passwords. The design of password systems has several human and organizational components to it:

- A system may not allow simple passwords.
- The system requires the use of passwords.
- The system may not require the employee to check the strength of password.
- Multiple passwords are difficult for employee to remember. Employees sometimes write them down on slips of paper. A cultural issue is that no one likes passwords: they are viewed as a nuisance.

4.2.3 Internal and external networks

The workgroup identified that vulnerabilities in the application and server category are the same as internal and external networks on the value chain. Internal and external networks differ by company. There is a spectrum of open/closed networks (i.e. relationships with vendors, clients, end users). Some organizations may have internal networks where only employees have access, while others may have internal networks where outside vendors have access. The *amount* of vulnerabilities introduced is dependent upon this spectrum. On the whole, organizations are becoming increasingly public. Therefore, access controls must be dissolved when vendor relationships end. Although the relationships to internal networks may differ for employees versus vendors, we do not need different systems, processes, and procedures for these groups. There may, however, need to be a different degree or level of security for different groups of users.

4.2.4 Enterprise architecture

The full design, or enterprise architecture, is an overarching design where vulnerabilities may occur. It includes the full range of vulnerabilities, but it is the relationships among the different elements that we are concerned with. Human and organizational factors regarding enterprise architecture include:

- Lack of coordination in identifying processes and procedures.
- Need to identify a person or team to define and identify the architecture, maybe even a migration plan.
- Need to do this constantly as it is an iterative process.
- Need upper management support and buy in.
- Need resources from all levels of the organization, especially IS. Without this, it is not a fully integrated design.
- Workload: This would be one more task to do, on top of an already full workload. This is why upper management support is critical.
- Resource allocation: Need the most talented employees for architectural design.
- Policy that addresses all new and integrated applications. When constructing architecture, the design must be mandated throughout the organization.

When integrating architecture and security, it is likely that the technical system architects create (but do not build) the systems, and then the security personnel will evaluate those systems. Design is derived from functionality, which greatly narrows the universe of possibilities. However, identifying the quality components of security and building the system from those factors may improve the security of the system.

4.3 Human and organizational factors across the value chain

There are human and organizational issues that cut across all vulnerabilities on the value chain. First, in the area of "*Culture*", a strong security mindset is important across the security value chain elements. Information Technology has more recently become an easy, effective and preferred means of attack. Second, management underestimates the speed of technology improvements and the amount of effort required to maintain secure systems, therefore creating and maintaining inappropriate amounts of *workload*. With *process ownership*, each business process requires an owner and IT processes are not the exception. Process owners need metrics to evaluate the process effectiveness and to identify weaknesses. Management support is a given for any project success. For *policy and standards*, each element of the value chain requires a management-approved policy. Policies must be enforced to be effective. The policies can be reviewed with employees each year, thus providing an element of training. With *training*, it is often difficult for management to see the effects of training on the bottom line, thus training budgets are often cut. When the training cuts pertain to security-related processes, the company increases the level of risk.

Value Chain Element	Vulnerability	Policy & Standards	Training	Design	Management Supervisory Support	Workload	Resource Allocation & Process Ownership	Culture
Information assets	Content management	1. Policy-orientated organization. 2. Training for policy. 3. Attestation for policy. 4. Policy must address different employee group needs. 5. Policy addresses internal networks, usually not application and servers. 6. Needs to change control policy. 7. Need enforcement of access control policy.	1. Training for policy, including reminders, and continuous training. 2. Procedural training on how to apply policies to individual jobs. 3. For CIA, need to convey proper data handling techniques and require backups.					1. Must promote adhering to policies and procedures.
	Poor access control							
	Inadequate asset classification			1. Integrity: require data signing for certain types of data 2. Availability: may need total data redundancy.	1. Classify data. 2. Enforce data handling policies.			
Application and server	Access control	1. Access is to be provided only when there is a business need, and ideally for only the amount of time required to accomplish the job. 2. Create policies based on "Access provided on a need to know basis." 3. Management or system owner approval before access is provided.	1. Education on responsibility and importance. 2. Do not underestimate training for administrators. 3. Educate admin on access technology (not simply commands to change ID). 4. Background checks on administrators. 5. Provide social engineering training.	1. Level of difficulty to control system. 2. Conflict: system repair/mgt. and usability. 3. Allocate appropriate time to classify data.	1. Time pressure from mgt. (This factor is true for every activity and element in this column). 2. Educate management, "Importance of admin role." 3. Importance of segregation of duties, fraud.	1. People are largest security vulnerability. 2. Do not overburden administrators 3. Create access control SLAs that provide sufficient time for verification during peak workloads.	1. Audit access control process regularly. 2. Audit user access rights regularly.	1. Establish a security-minded culture. 2. Management must demonstrate security, lead by example. 3. Management cannot be given special security privileges.

Value Chain Element	Vulnerability	Policy & Standards	Training	Design	Management Supervisory Support	Task/ Workload	Resource Allocation & Process Ownership	Culture
Application and server	Missing contingency plan	1. Policy must mandate business continuity planning and drills.	1. How to act in the event of an incident – and practice the procedures.	1. Design in redundancy if criticality requires it.	1. Require all areas to have a backup plan 2. Support testing, drills.	High workloads do not allow for planning or testing the plan.	Lack of time and money to create contingency plans.	1. Nurture a mindset of "what could go wrong", and plan for contingencies.
	Inadequate data control	1. Have a policy (and enforce it) regarding access control, data handling, "C-I-A" elements.	1. Train on mandated data handling procedures and techniques.	1. Physical control of organization sets precedence for information control (i.e. security mindset). 2. Design of processes and procedures.				Cultivate awareness and attitude.
	Poor application design (vendors-purchasing applications)	1. Any external service providers must meet the organization's security policy, and perhaps its security standards as well.	1. Nurture a 'security mindset' to be alert to vulnerability factors, insecure practices, "Top 20 vulnerability" issues.	1. There should be a checklist to evaluate the design of the application.	1. Look for security assessment of vendor(s) product or service. 2. Review of code by security staff person.	1. Application design must address or include security elements – make it not an option.		1. Address application evaluation. 2. Culture must sustain a level of awareness.

Value Chain Element	Vulnerability	Policy & Standards	Training	Design	Management Supervisory Support	Task/ Workload	Resource Allocation & Process Ownership	Culture
Application and server	Patch management	1. Management supported policy for patch management.		1. Need to know machine installation. 2. Need to know who has information access. 3. Integrate patch management into new processes. 4. Include in system maintenance costs. 5. Patch only systems requiring the patch.	1. Management must require that security patches be evaluated and installed, and staff for this activity. 2. Educate management on importance of patch management. 3. Demonstrate cost effectiveness when compared to potential system downtime and recovery costs.	1. Large number of patches. 2. Patch notification, verification, and testing. 3. As patch volume increases, complexity of task and workload increases. 4. Tracking patches. 5. Maintain accurate database of operating systems, applications, patch levels. 6. Setup test environment.	1. Identify patch process owner, associate metrics to performance review. 2. Register with sites for email notification of new patches.	
Application and server	Backup vulnerability	1. Policy must mandate backups; require offsite storage; require periodic testing of the backups.		1. Design backups into the work processes.	1. Management must support testing the backups and the restoration plan.	1. Too busy to backup files.	1. Process not user-friendly.	1. Perception of low risk. 2. Lack of caring. 3. Ineffective communication.

Value Chain Element	Vulnerability	Policy & Standards	Training	Design	Management Supervisory Support	Task/ Workload	Resource Allocation & Process Ownership	Culture
Application and server	Anti-virus protection	1. Need a policy that requires anti-virus. 2. Employees must understand the corporate anti-virus policy and the consequences of not complying with corporate policy. 3. Company must enforce policy.	1. Teach users the signs of a virus, what to do, how to scan for viruses. 2. New hire and annual employee training. In person or online training followed by policy sign-off.	1. Check for viruses at all "gateways" and at workstations. 2. Do not rely on employees to upgrade anti-virus signature files and anti-virus software upgrades.	1. Security should be approached like insurance, must have to run the business.	1. SNORT, outsourced tools. 2. Employees are not allowed to circumvent. anti-virus measures to improve the performance of computing equipment.	1. Identify Anti-virus Protection owner, desktop, mail and servers. 2. Setup metrics based on infections due to policy violations.	1. "Practice Safe Computing".
Application and server	Intrusion detection		1. Expertise and experience needed for effectiveness. 2. Train people to become a 'human firewall' to detect, report incidents.	1. Consider both host-based and network-based IDS (intrusion detection systems).	1. Management must be sold on the benefits of an IDS (e.g., ID insider activity) as it protects (not generates) revenue.	1. Difficult to recognize patterns. 2. Organization of tasks. 3. Staffing levels.		

Value Chain Element	Vulnerability	Policy & Standards	Training	Design	Management Supervisory Support	Task/ Workload	Resource Allocation & Process Ownership	Culture
Application and server	Transaction log analysis	1. Must have policy as to how long you keep the logs. 2. Should define how log files are to be protected.		1. Access level-identify who can manipulate the data. 2. Important to have log device turned on. 3. The longer you keep logs, the more information you have. 4. The appropriate space to store logs-must acknowledge the sensitivity.	1. Allow time, or budget for resources, for log review.	1. Large volume in the number of logs. 2. Large volume of info within the logs. 3. Must monitor closely to sustain the integrity of logs.	1. Need to have people assigned to this task. 2. May out-source this task (TruSecure).	1. Should be made aware that logs are kept – can help influence behaviors.
Application and server	Password management	1. Need to have a policy on the strength of passwords. 2. All access needs a login and password. 3. Need policy on the frequency of change for passwords. 4. Policy must prohibit password sharing.	1. Training is critical because the individual chooses the password. 2. Need training on how to create a "good" password. 3. Need to train on how frequently to change passwords.	1. No weak passwords. 2. Require passwords. 3. Check the strength of passwords. 4. Check the frequency of changing passwords. 5. Create a design that employees do not have a large number of passwords.	1. Support and enforce the password policy at all times.	1. If the system does not automatically check password strength and how frequently passwords are changed, a group or individual must be assigned that task.		1. Nobody likes passwords. 2. Must link password to personal interests – "protecting your password protects YOU".

Value Chain Element	Vulnerability	Policy & Standards	Training	Design	Management Supervisory Support	Task/ Workload	Resource Allocation & Process Ownership	Culture
Enterprise architecture	Enterprise architecture Integration complexity leads to greater security complexity. Lack of standards introduces technology threats and gaps.	1. Need all new and integrated applications, when constructing architecture, mandated. 2. Mandate architectural compliance – at least a study, and sign-offs on deviations. 3. Business must also be governed by IT standards for product procurement.	1. Standards awareness.	1. Need to do this constantly, an iterative process. 2. Need both business and IT support of the architecture.	1. Need upper-mgt support and buy-in.	1. There is a lack of coordination in processes and procedures. 2. Need to have this element as a structured task to employee workload-difficult because workloads are already heavy.	1. Identify a person or team to define and identify the architecture, maybe even a migration plan. 2. Support from every area of IS and organization function. 3. Need most talented employees.	1. Need to set vision and culture to follow a standards-based approach, even if it means sacrificing technical benefits for the greater good.

CHAPTER 5 – BEST PRACTICES

5.1 Introduction

The discussion of best practices for dealing with human and organizational factors associated with vulnerabilities on the value chain focused on three groups of vulnerabilities (see Figure 10). These groups were created to represent different levels of criticality. However, it is important to recognize that criticality is highly dependent upon the type of organization, such as manufacturing-organizations as opposed to information-based organizations. Therefore, the grouping of vulnerabilities presented in Figure 10 represents the consensus of the companies participating in the working group. For each vulnerability in Groups 1 and 2, strategies and processes to deal with the human and organizational factors were identified.

Group 1: Highest criticality	Group 2: Medium criticality	Group 3: Lowest criticality
Access control Patch management Anti-virus protection	Back up Application design Asset classification Password management	IDS Contingency planning Content management Data control Enterprise architecture Transaction log analysis

Figure 10. Groups of Vulnerabilities with Varying Levels of Criticality

The identification of best practices for human organizational issues in e-security overlays Phase 3: Evaluation of controls, Phase 4: Decision, and Phase 5: Communication and monitoring of the ROI on e-security model (see Figure 11). Best practices for human and organizational issues in e-security covers Phase 3 because evaluating the controls systems for security, such as access control and data control, are relevant issues identified by the working group. Best practices for how deciding how to implement and document e-security practices (Phase 4) as well as communicating those practices (Phase 5), such as policy, training, and management, were identified by the working group.

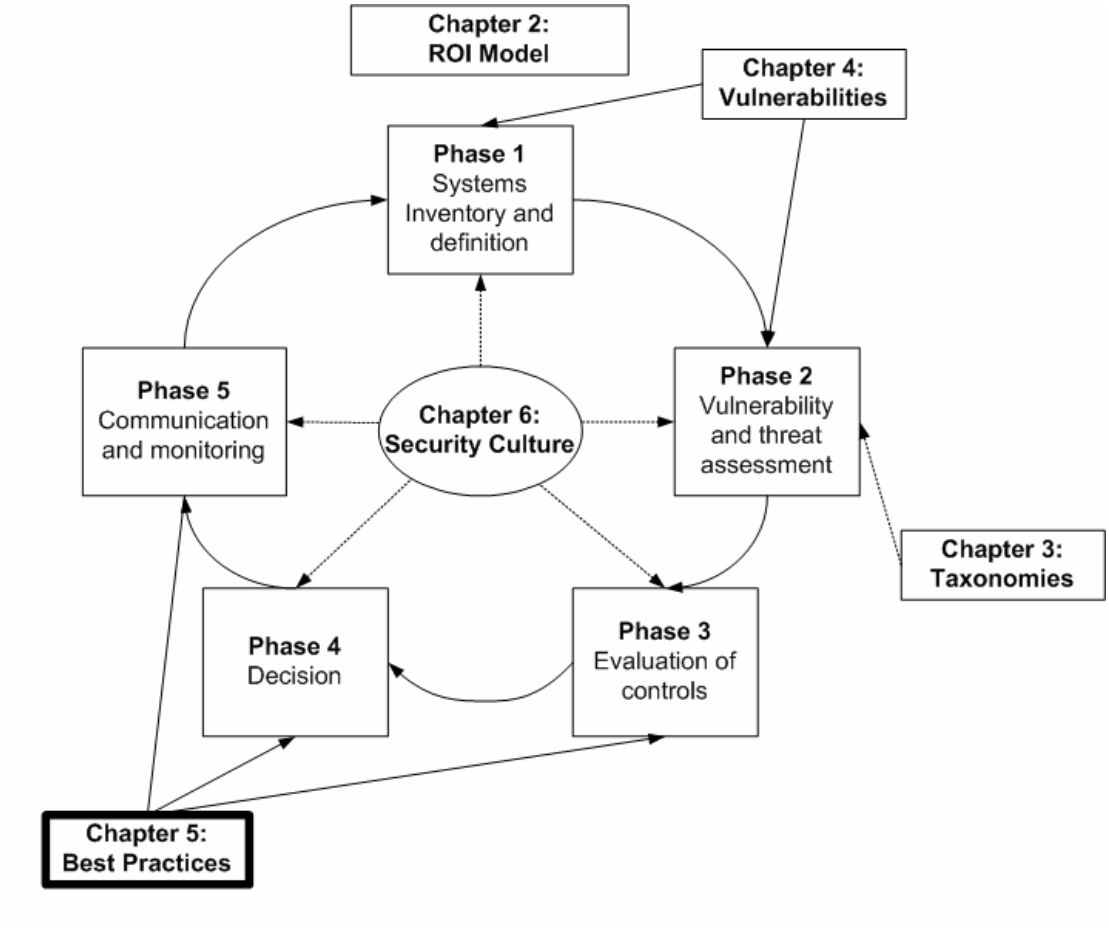

Figure 11. ROI on E-Security Model, Highlighting Best Practices

5.2 Best practices for group 1 vulnerabilities

5.2.1 Access control

Policy is the most important issue to be addressed. The components of the best practices for policy include:

- An effective *policy* must involve all the stakeholders who either follow and use the policy or are affected by its use. The *stakeholders* include employees and end users who are responsible for the data. These end users should be involved in creating the policy, and participating in the audit on the processes. They should be given the ability to take corrective action. When the policy has been created, the individuals who are actually doing the work need to be integrated in policy deployment. It is important that these stakeholders understand the policy, function, etc… Therefore, their insights must be taken into account when designing and implementing policies.
- Management defines the policy and information owners define the procedure. The policy should require the use of a user ID/password and the information owners should define who has access and at what level.
- *Responsibility* for the access control of various pieces of information should be addressed with policy. The business owner has responsibility for defining who should have access.

Business managers are critical because they are responsible for the data they own. They integrate other stakeholders' insight and intention into their actions and procedures.

- *Data ownership* is structured by functional process. A multifunctional perspective to security policy is needed.
- Procedures represent the *deployment* of policy. Every piece of information needs an "owner" and it is the owner that defines who has that access and in what manner. This aspect needs enforcement for accountability of security.
- Policy should address a validation of access list.
- *Human error* is an issue that policy should address. A human error may lead to granting access to individuals who should not have the access rights. This could be attributed to inexperienced, new IT personnel, or other factors. How do we catch these errors?
    - Access lists should be reviewed.
    - Look for trends and activity logs that look irregular, such as looking for actions on the weekends.
    - Intrusion detection systems need to be scanned to look for anomalies.
    - Sometimes, the employees will alert organization. This is linked to the culture and education of the organization. The employees should know what is appropriate and not appropriate, and the consequences of inappropriate access.
    - There should be a system to track errors. Calls may be logged at help desk. Notification and resolution of the problem are logged, but not activity of resolution/solution.
    - Profiling is an appropriate way to handle lists of access rights. Administrators need to associate groups within groups and hierarchy of groups. Companies need to have access control groups, groups of security professionals who have task loads that include monitoring access control for the organization. These groups would maintain and give access to people/groups in the organization. The system administrators have the highest level of control, so they may have the priority of monitoring access control. For example, every person must enter the system under one identity (individual) in an effort to minimize the number of identities.
- *Management* does not regard security as an area that requires supervisory support for employees. Supervisory support for security tends to be an "add-on" or afterthought. Security needs to be recognized as a business enabler, i.e. a required business function.
- IT personnel audit both technical logs and business logs. This does not occur in private, external audits. As a result, we need to *audit the internal auditor*.
- *Think like a hacker* and identify low, medium, high risk of being caught hacking into the system. A result of this thinking is the need to identify the critical business systems, as well as the controls or the backups needed if a breach is in place.
- Need to realize that there is a large risk associated with exposing any system element to the Internet.

5.2.2 Patch management

Patch management is not an easy issue to grapple with because there are always a lot of patches to fix, not all patches are significant, and there are a lot of machines to patch. Patches may be thought of as a "losing battle" because before implementing a patch, you have to test it. The only efficient method with dealing with the shear volume of patches is to *prioritize* them and test/implement them appropriately. The best practices for patch management include:

- Using the free services of email updates for new patches.
- Using an outsourced company, such as external auditing services. They know the configurations on the servers, so they do the upfront matching, as well as prioritizing patches.
- Need stratification of vulnerabilities. We may do this through Internet vs. non-Internet exposed applications, server, network, etc…
- Look at news and links, as well as the community of security (FBI, white hat hackers) in order to identify the 'critical' patches that can protect systems from breaches, worms, viruses, etc…
- Once patches are identified, it becomes a *management* issue:
    - Change control process should be managed. The process of implementing a patch is organization-wide, and requires appropriate management.
    - This generally does not need the involvement of the end users, unless it is an application patch. This is because the end users are linked to the client/application, and should not be directly or indirectly involved with the change of those particular components.

5.2.3 Anti-virus protection

End-users used to play a more active role in anti-virus protection, but this is decreasing. The processes are becoming more automated, and the best practices identified reflect that change:

- Anti-virus protection needs to upgrade in a timely manner. This is the biggest issue facing companies right now.
- Problems arise when people dial into the system from a personal machine. Awareness of this aspect of the system is critical for monitoring anti-virus protection.
- It would be helpful to take the end users out of the anti-virus protection process, but this is not always possible. We must remember that laptops that are used may or may not be connected to the network. Personal machines (laptop or PC) that connect to the network also present large problems and complexity is added when we are unaware of what is on the machine, making it impossible to control the variables on the machine.
- *Training* may be more effective when a mechanism is highlighted. People need to know what is important and whom to contact. This is especially true with a hybrid attack of both technical and social engineering tactics.
- Viruses are introduced on diskettes that have been worked on at home, and then brought back to work. Or, viruses may be introduced by accessing hotmail accounts from work. To remedy this, we may:
    - check to make sure that anti-virus protection is turned on.
    - check to make sure end-users receive their signature files.
    - allow end-users to call someone (a security analyst) when they feel something is wrong. This creates good corporate citizens, letting them know what to do, and who to call when trouble arises.
- Culture. We need to "Practice Safe Computing". Automation of security can eliminate only some of the human and organizational issues. Security has become one of the priorities of business, as a result of automation.

5.3 Best practices for group 2 vulnerabilities

5.3.1 Password management

Password management is a multifaceted problem. There are multiple passwords for a single user, associated passwords, and single passwords (those that allow access to anything). There needs to be a balance in the number of passwords and the complexity of password. Some best practices for dealing with the intricacies of password management are as follows:

- Tokens work well, but there is a user acceptance factor. Tokens are important for those with root access. Other technologies include: biometrics, smart cards, etc…
- One single sign-on for both the network and business systems.
- Degree of authentication. If you have mission-critical data, a single factor password scheme (all lower case, no numbers) will not be adequate. You need multiple levels of passwords, which are determined by the assets to be protected.
- Changing passwords is a key practice. Passwords should be changed on a regular basis. Some useful techniques are reversed words and setting complexity of the password.
- People write down their passwords (common and pervasive in organizations). A helpful technique may be encouraging good passwords though games and engaging activities, even though password policy is mandated. An example of this may be employee password "cracking" day, where there is competition for hard-to-crack passwords.
- There should be a minimum length requirement for all passwords.
- Sharing passwords is not right. Sharing passwords amounts to sharing an identity and in that respect, both individuals may be compromised. There is a loss of accountability when this happens. There should be a policy of not sharing passwords.

5.3.2 Backup

Similarly, the backup vulnerability is multi-faceted. Since backup is done on all servers, the problems that arise are multidimensional. Some best practices for backup:

- Policy for backups should be such that, if a business area purchases a new server then that area is responsible for backups of the system.
- Individuals are responsible for backing up their personal data. It is not appropriate to use a PC as a repository for data.
- What you backup and how often you do it depends upon what can be afforded to lose. This needs to be calculated and those issuing the times and amount of backups need to be made aware of these issues.
- Security policy should address tapes that need to be labeled with confidential data and be stored off site. There are some business processes that require instantaneous back up.
- Policy and procedures need to be in place for setting up policy for all computers, including laptops.
- Business recovery rehearsals/restore processes need to be tested to see if what should be restored is actually restored. This should be part of the business plan for increasing security.

5.3.3 Application design

An important aspect of application design is its integration into the existing architecture. If application is not integrated, there is a potential point of failure.

- Application design should take into account in the "front end", or upfront design requirements. Some consequences of not planning the design requirements may be "building a door when you need a window", that is a creating system architecture that does not fit the need of the current system usage. The need in this context is to build security exits within the design that allow changes in application, as well as other components of the system.
- If these elements are not within the design, a checklist may be one way to accomplish this task. There could be a "walk-through" (this is speaking to the door/window analogy above). A security checklist would address this partly (business needs), like reliability and confidentiality of data.
- Use applications that test application security.
- Organizations tend use the same designers or vendors because there are many different ways to accomplish the test applications, and organizations want to be consistent.
- There are issues of malicious intent: someone who intentionally puts in a back door, as well as errors of omission. A code walk-through can help deal with this.

5.3.4 Asset classification

Confidential data may be exposed if the data is not properly classified. How can we prevent this from happening?

- Business owners should classify the data based upon criticality.
- Some useful classifications of assets:
    - Confidential
    - Internal use only
    - Public
    - Historical
- Documents are retained or deleted. In order to decide what is kept or deleted, one should consult the organization's attorney, or obtain outside legal counsel. For the most part, the data owner is responsible for keeping or eliminating the information.

5.4 Conclusion

For the vulnerabilities with the highest criticality, group 1, policy, human error, management practices, auditing, risk management, training, and culture were identified as areas were best security practices may take place. For best practices of group 2, significant areas identified by the workgroup include usability practices related to tokens, authentication, sign-on, passwords; as well as policy, recovery practices, and issues related to formulating the specifications for application design requirements.

CHAPTER 6 – SECURITY CULTURE

6.1 Introduction

Organizational culture is manifested at many levels and can therefore be studied and analyzed at different levels. The basic levels constitute the "surface-level" components to culture (i.e. artifacts). As these are recognized and understood, we may analyze the deeper values and underlying assumptions to culture.

The issues identified in security culture permeate all areas of the ROI model (see Figure 12). Because security culture is subjective and qualitative, there are indirect relationships to all phases of the ROI model, as indicated by a dashed line.

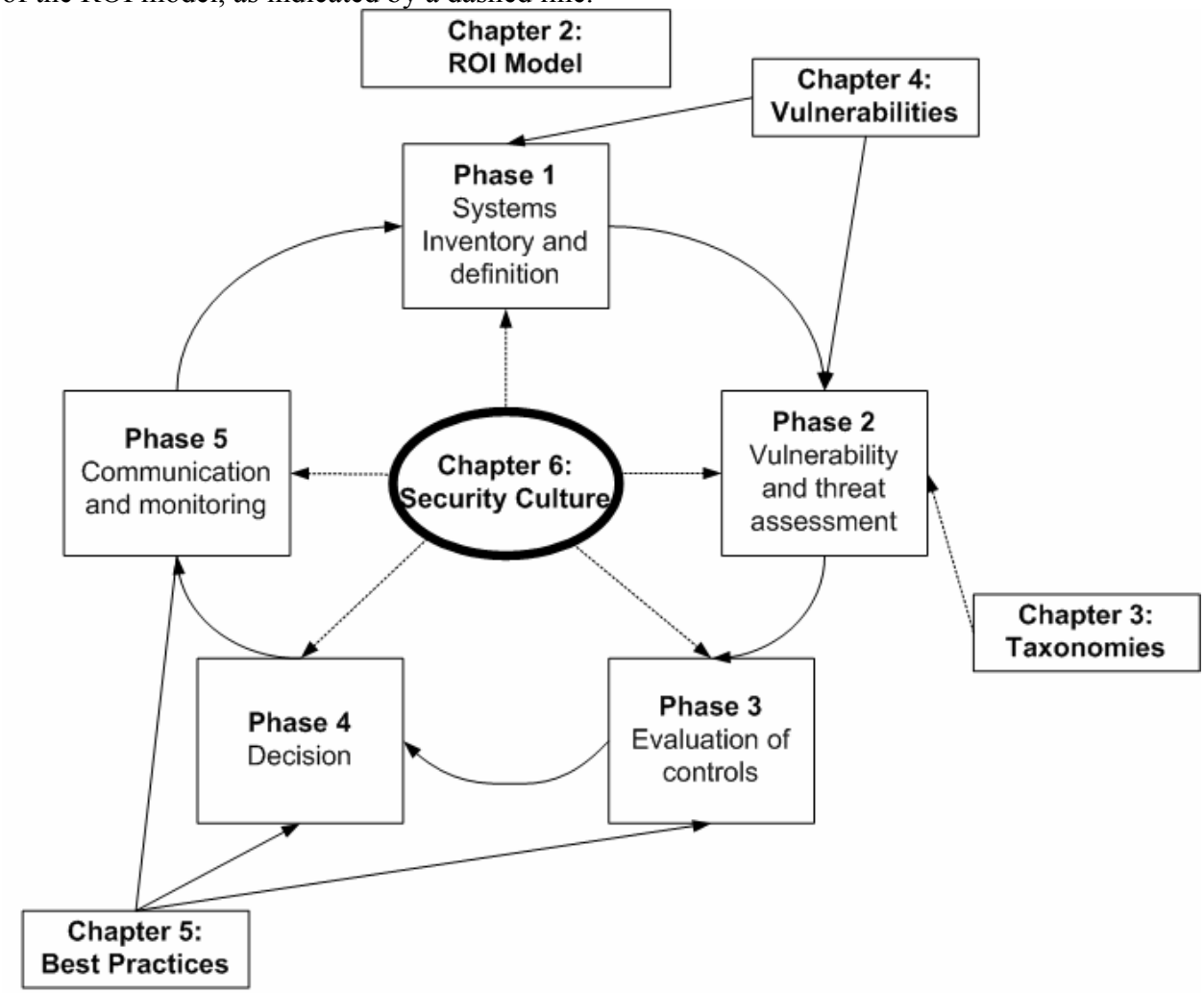

Figure 12. ROI on E-Security, Highlighting Security Culture

6.2 Measuring security culture

There are several ways to measure the security culture of an organization. One indirect measure of security culture may be done through incident reporting. For example, the amount of

passwords violations (e.g., weak passwords, passwords not changed frequently) may be measured. The amount of inappropriate materials downloaded from the Internet may also be a possible indirect measure of security culture.

Documentation of security practices within the organization is an important element of security culture. For example, marketing, human resources, and information security management need to document and articulate what a secure environment means. One may also use posters, which would be used to convey security-awareness attitudes. Employee interactions and communications through the company's intranet, distribution of reading materials at employee meetings and in the cafeteria, etc… may be good measures of security culture. Security culture is difficult to measure, but one may try to create an open environment by facilitating questions and comments on security policy through many channels.

6.3 Dimensions of security culture

Employee participation is an important dimension of security culture. If there is resistance to change, participation could alleviate some of this. *Training* on security policy and security practices that are job-specific (separate from "overall" security training) is an important element to employee participation. Awareness and understanding of the "critical moments" or "events" the end user needs in security may be very revealing to security needs or mechanisms that need to be in place to create better security. These moments may be the reveal the context of an end user or administrator error, why and what precipitated the error or mistake. These critical moments may take place in training, during the use of the technological system, customer interactions, or some other aspect that relates directly to the usage of the technological system.

Hiring practices include extensive background checks, involvement of the employee handbook in training, making sure that new employees know the policies on the onset of employment, or when there is a new or different security policy. There should be attestation between employee and employer, and agreements with third-party workers, on security policy and practices.

The *reward system* is another dimension of security culture, although there is a flipside: sanctions need to be in place for damaging behavior. With a reward system, the attitude that needs to be cultivated is appreciating security because it keeps your job and the organization "safe". Security at the organization needs to be connected to the employees so that they understand the importance of it. Security is linked to their livelihood, i.e. their employment at the organization. Employees need to be intrinsically motivated and care about security. This is tied to the understanding of the how security is important. Employees need to understand the benefits of security. This is a *mechanism* that drives security culture.

Management commitment is an important element of security culture. Security needs to be enforced and management needs to be the enforcers of that movement. There should be a visible display policy enforcement (e.g., memos, signs in the organization, management presence at security meetings) and no individual or group should be exempt of following security policies. Management needs to lead by example and deliver the message of security to the employees. Further, management should have the correct security factors established so that when the decision makers of the organization are allocating resources to security, they have the correct and most current information to allocate those resources appropriately.

Communication and feedback are pervasive and critical to improving security. For organizations that have their corporate policy on their intranet site, creating links where employees can comment or question the policy can be helpful. Other good practices for communication and feedback from employees include emailing and calling security managers. The committee on company policy can then take the employee comments and change or integrate them accordingly.

Trend analysis of security breaches and vulnerabilities may be useful for communication and feedback mechanisms. Identifying trends in security breaches and vulnerabilities may be revealing to areas of the organization where security is especially weak. When trying to identify these weaknesses in the organization, it is critical to realize that every function of the organization needs to be communicated to in their context and language. However, having a common dialogue around security is critical.

Physical security is the invocation of computer and information security. When the physical security comes to the attention of the organization, it helps extend foster better employee attitudes toward the awareness of e-security.

6.4 Conclusion

Security culture is pervasive throughout organizations and is often difficult to summarize or measure for levels of effectiveness. The brief discussion above reflects the current thinking on how to measure and identify the dimensions of security culture.

REFERENCES

Brooke, P. (2000). *Risk-Assessment Strategies*. Network Computing. Retrieved, from the World Wide Web: http://www.networkcomputing.com/1121/1121f3.html

Center for Strategic and International Studies (2002). *Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories*. Washington D.C.

Howard, J. D., & Longstaff, T. A. (1988). *A common language for computer security incidents* (SAND98-8667). Alburquerque: Sandia National Labs.

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