Corporate Vital Defense Strategy:
A framework for Information Assurance

Bel G. Raggad, Ph.D.
School of Computer Science and Information Systems
Pleasantville, NY 10570
braggad@pace.edu

This study is sponsored by the American Institute of Management and Information Technology and Pace University's School of Computer Science and Information Systems, New York.

Abstract

The article proposes the corporate vital defense strategy (CVDS) as a security and information assurance framework, similar to the DoD's Defense-in-Depth strategy. The article identifies 60 types of (default) functional security information systems defined in terms of 1) DoD's attack models (probe; infrastructure; factory; and authorized-access models), 2) Whitten, Bentley, and Barlow's entities (data; people, activities, technology; and networks) induced to cause the attack, and 3) Cohen's security disruptions (information leakage; information corruption; and service denial) produced.

Studying these default functional security information systems not only can help planning automatic information security solutions, as shown in the article.

Keywords: Vital Defense Strategy; Attack Model; Attack Entity; Disruption; Security Information System.

Introduction

In order to support their operational missions, companies need to guarantee the availability of information, efficient information technologies, and a reliable connectivity. Unfortunately, connectivity relies on commercial information resources and networks that are not fully secure.

There are however IA technology solutions that can provide adequate protection of their information. The effectiveness of these solutions should be evaluated based on their impact on operational missions. Full security is not possible, but adequate security can be achieved when IA technology solutions are adopted while balancing risk with cost and performance with operational impact.

Corporate Vital Defense Strategy (CVDS)

The IA technology solutions should be defined with sufficient details to recognize fundamental security services, security technologies, security strategies, interoperability, key management infrastructure, and public key infrastructure.

The corporate vital defense strategy should provide a holistic approach in assuming four main roles:

1. Defend enclave;
2. Defend the Data Processing (DP) environment;
3. Defend infrastructure support.

Corporate Information Assurance Technology Framework (CIATF)

A company needs to have a framework to support the company's information assurance (IA) needs. The company needs to adopt a clear and deliverable profile of IA strategies. This strategy profile is called Vital Defense Strategy (VDS). The planning, design, and implementation of the VDS should be completed in a well defined framework called Corporate Information Assurance Technology Framework (CIATF).

The company should continuously have a clear security mission, and testable policies and regulations. The CIATF contains guidelines on how to acquire, develop, and effectively implant security solutions. The security policy can be satisfied through a balanced implementation between technical security solutions and non-technical countermeasures. The CIATF provides case studies where tradeoffs between cost and risk can yield adequate security. Cases where practical solutions cannot fully satisfy security policies are also explained in the CIATF.

The CIATF identifies a range of risk management methodologies that apply to divers activities, networks, technologies, conceptual resources, and software systems. The risk management methodologies should be the foundation for additional security assessment models through which the certification and accreditation activities are processed.

The CIATF should periodically review and redefine security concepts and diverse roles and functions and new technologies so that current IA technology solutions can be evaluated. Security assessment models should be reviewed, and revised as IA security technology changes. New risk assessment models should be developed.

How to defend the corporate enclave as required in the CVDS?

The CIAFT provides structure and sufficient design information on three major areas: the protection of network access originating at the enclave; the protection of remote access conducted by traveling users and remote users; and the protection of interoperability across security levels. The protection of network access should diversify the IA technology by considering, for example, firewalls, intrusion detection systems, vulnerability scanners, and virus detection.

Defending the enclave also includes defending external connections as required by the CVDS.

How to defend DP as required in the CVDS?

The defense of the DP environment requires that end-user workstations, servers, applications, and operating systems be protected. CIATF should include explicit information details of how security requirements of divers DP elements are designed. For example, the components of a DP element that should be protected are identified, analyzed before their security solutions are designed and implemented. End-user applications in the CIATF can include secure emailing, secure web browsing, file protection, and mission specific applications.

How to defend the infrastructure support as required in the CVDS?

Defending the DP environment, its networks, and its enclave remains useless if the infrastructure support itself is not secure. Imagine, agents at the company and its partner's enclaves are all using compromised keys, invalid certificates, or weak cryptographic models. The CIATF cannot help in implementing the company's VDS if the infrastructure support is not adequately secured.

Defending the infrastructure support is obviously a consequential element of the company's CIATF. At least two major areas should be planned: the KIM/PKI (key management infrastructure/public key infrastructure), and the D&R (detection and respond).

The first area concerns the technologies, services, and processes used to manage public key certificates and symmetric cryptography.

Information Security Methodology:

An information security methodology (ISM) is a systems approach that produces a user's security needs. The ISM consists of three main phases, as in Churchman's systems approach (Preparation effort; Solution effort; and Implementation effort), which provide a detailed security analysis of the user's system. This analysis should satisfy all integral requirements defined in the CIATF. The ISM which is beyond the scope of this article is described in great details in AIMIT’s series of information security.

User security should be studied throughout its entire life cycle. The preparation effort is conducted first to understand mission needs, system policies, system regulations, system standards, and threats to owners. The solution effort is concerned with the security design. This phase includes the identification of possible security solutions defined in the CIATF, the definition of choice attributes based on which security solutions are retained, and the selection process. The implementation phase consists of the implantation of security solutions, and their review process.

A good security solution is one that grants the required protection for the security needs stated in the system security policy. Risk assessment is always requisite before the design and after the implementation of a security solution. It is needed at the design process to evaluate how much risk is involved, and after the implementation process to ensure that the adopted security solutions are actually working as desired. The security solutions adopted should only be adequate enough to satisfy a balance between cost and harm effected on system owners.

The certification task is a review process that aims at assuring that the security solutions are technically feasible. This is however a continuous process that lives as long as the system lives. The certification process stays alive in order to ensure the system is satisfying operational and security needs and is adequately evaluating relevant threats.

It is very common however that the review process revisits the initial security attributes processed to produce an ISM. Often, the system security policy also needs to be reassessed. When the former revisits generate definitive differences or deviations from findings accepted at the preparation effort, then the system security solutions may need to be redesigned.

Classes of attacks:

Attacks are better organized in terms of 1) the identity of the entity carrying the attack, 2) their effects on system owners, and 3) the models employed in the attacks. The effects of attacks on systems owners are commonly called security disruptions [1].

Identities of entities carrying the attacks

There are however only 5 possible acting entities that can have the capability of rooting an attack: 1) an activity, 2) a person, 3) a network, 4) a technology, and 5) a data resource. These entities were introduced first by Whitten, Bentley, and Barlow (1996) in systems analysis and design, and used by the author in diverse publications under the term business computing components.

These entities consist of people, activities, technology, data, and networks [4].

People: the role people play in an information system includes who will input data; who will receive output; and so forth.

Activities: The sequence of steps, data flows, security controls an information system environment are defined. The processes and security controls should be defined and documented.

Technology: technology is studied at any phase in the life cycle of the information system.

Data: Data and information flows are defined at any phase of the system life cycle.

Networks: Network requirements at every location of the business area are studied.

Security disruptions resulting from attacks

Security disruptions are organized as in Cohen 1995 [1], into 3 main groups: information corruption (C), information leakage (L), and information denial (D).

An attack employs a model to induce an entity to produce one or more security disruptions [1]. Causal links between entities and security disruptions are depicted in Figure 1.

Attack models

Attacks have models that combine people, data, knowledge, hardware, software, and other resources in order to achieve a specific objective which is usually to cause harm to system owners. The attack models are organized in 4 categories: Probe models, Infrastructure models, Authorized access models, and Factory models.

Probe attack models

Probe attack models are concerned with passive attacks that are designed to identify opportunities that can be explored to cause harm to system owners. A probe model takes the form of any other method conformant with the attack opportunity the attacker is exploring [3].

Infrastructure attack models:

Infrastructure attack models are concerned with attacks that are designed to induce entities to cause harm to system owners, by affecting an infrastructure attribute. An infrastructure attack model can be generic as introducing ,malicious code, copy traveling data, an attempt to break a security feature; or core as attacking a network backbone [3].

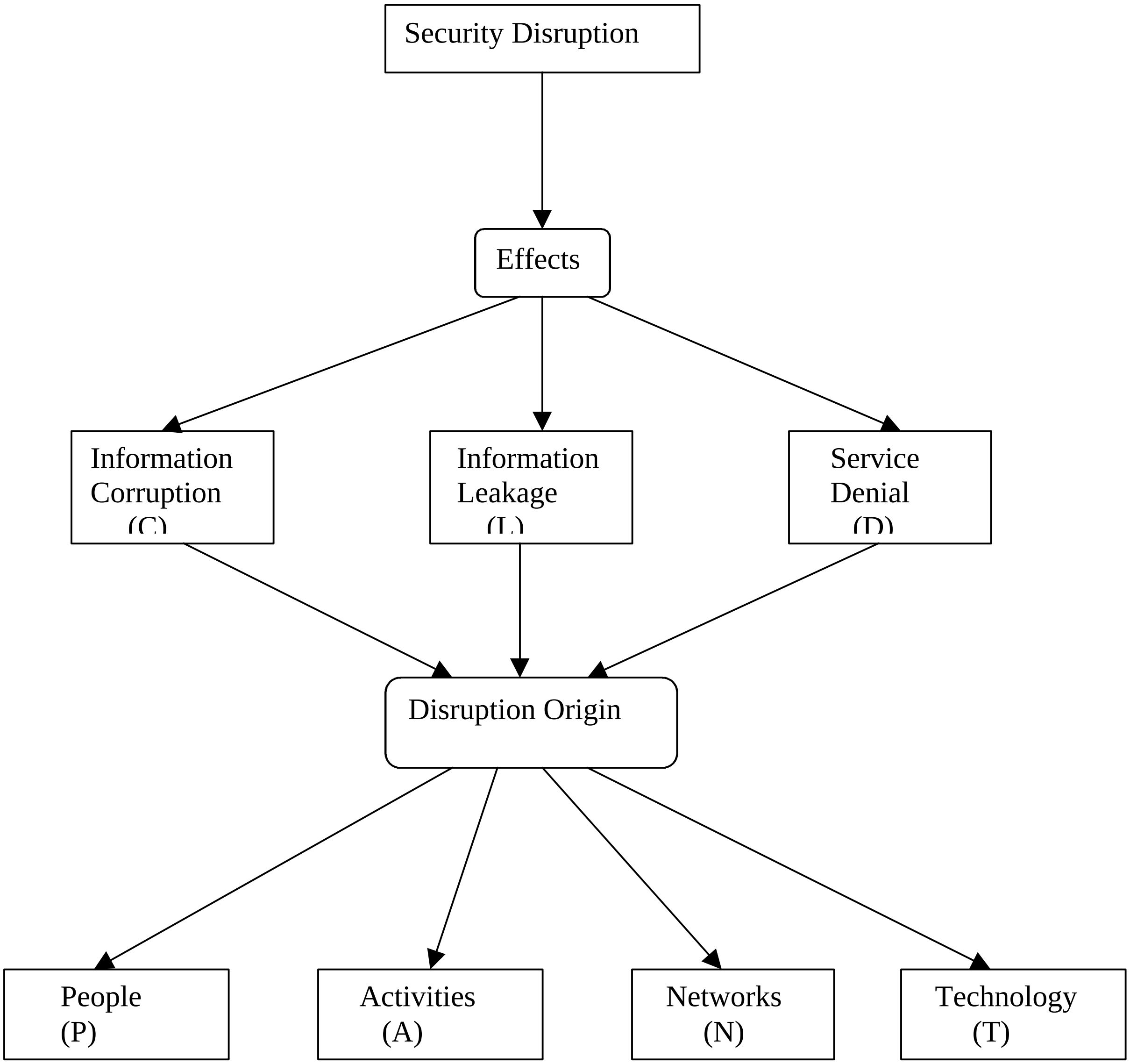

Figure 1: Security disruption classes defined by (Effect, Origin) pairs

Factory attack models:

Factory attack models are designed to induce an entity to indirectly cause harm to system owners by carrying the modification or the substitution of hardware or software at the factory, or during the distribution process.

Factory attack models may be designed to embed malicious code through shrink wrapped software, user swapping media, or path created to import information from an external network. Attacks are usually characterized by the malicious modification of hardware or software between the time the hardware or software is developed and the time they are installed and used. An example would be an entity (a user) with remote access capability who configures his/her computer when the computer is left unattended without any physical protection. The same attack would take place if the software is shipped through a network or a physical means [3].

How to develop a security information system?

A security information system is studied in terms of the following three dimensions: 1) attack model; 2) security disruption produced; and 3) the entity induced to cause the attack. In this manner, the effect of the disruption on the business area in terms of information corruption (C), leakage (L), or denial (D) will be understood. The business information components at the origin of the security disruption which may be people (P), activities (A), technology (T), data (D), or networks (N) will be known. The models used in future attacks are well defined in terms of their categories: probe models, infrastructure models, authorized access models, and factory models.

In the hierarchy of classes, for each attack model, there are therefore 15 classes defined by the effect and the origin of the security disruption [1]. Since there are 4 attack models, this hierarchy identifies 4*15=60 types of security information systems. This article will refer to these systems as Default Functional Security Information Systems (DFSIS).

For a fixed attack model associated with the company’s security threats and vulnerabilities, described in the PPs for various components of security information systems, as shown in the company’s CVDS, the DFSISs are studied in terms of the following situations:

1. Corrupted People (CP):

   CP is a security disruption class where the effect is information corruption and the origin is people at the business area.

2. Corrupted Activity (CA):

   CA is a security disruption class where the effect is information corruption and the origin is an activity at the business area.

3. Corrupted Technology (CT):
   CT is a security disruption class where the effect is information corruption and the origin is technology at the business area.
4. Corrupted Data (CD):
   CD is a security disruption class where the effect is information corruption and the origin is data at the business area.
5. Corrupted Network (CN):
   CN is a security disruption class where the effect is information corruption and the origin is a network at the business area.
6. Leaking People (LP):
   LP is a security disruption class where the effect is information leakage and the origin is people at the business area.
7. Leaking Activity (LA):
   LA is a security disruption class where the effect is information leakage and the origin is an activity at the business area.
8. Leaking Technology (LT):
   LT is a security disruption class where the effect is information leakage and the origin is technology at the business area.
9. Leaking Data (LD):
   LD is a security disruption class where the effect is information leakage and the origin is data at the business area.
10. Leaking Network (LN):
    LN is a security disruption class where the effect is information leakage and the origin is a network at the business area.
11. Denying People (DP):
    DP is a security disruption class where the effect is information denial and the origin is people at the business area.
12. Denying Activity (DA):
    DA is a security disruption class where the effect is information denial and the origin is an activity at the business area.
13. Denying Technology (DT):
    DT is a security disruption class where the effect is information denial and the origin is technology at the business area.

14. Denying Data (DD):

    DD is a security disruption class where the effect is information denial and the origin is data at the business area.

15. Denying Network (DN):

    DN is a security disruption class where the effect is information denial and the origin is a network at the business area.

Default objectives for the DFSISs:

The default objective of a DFSIS is the solving of the security problem or the enforcement of the security directive for which the system is initiated. Unless information system owners approve a new objective, the security information system maintains its default objective.

A security information system is initiated to solve a security problem or to enforce a security directive cited in security policies. The objective of the security information system may be defined as the objective of the class where the security problem belongs. If it is initiated by a security directive, then the default objective of the security information system will be that of the security directive.

Since a security disruption may reside in different classes, then a security problem may also reside in different classes. The security information system may hence have multiple default objectives. Table 1 provides default objectives for security information systems associated with the 15 security disruption classes defined earlier.

A simple security information system is a system that is initiated by security problems or security directives members of only one class. The selection of the problem may be done using frequency distribution of security situations. Classes are ranked with respect to the frequency percentage of those security situations residing in classes. Classes of corrupted networks, leaking networks, denying networks, corrupted people, and denying activities are ranked 1, 2, 3, 4, and 5 respectively.

One may rank security situations according to their number of residences. A situation related to the highest number of residences is selected first. Every security situation is carefully examined to identify the class where the security disruption resides. Even though, the number of classes associated with one situation may indicate that the security information system should be initiated using these classes and their respective default objectives, it is important to think of a threshold beyond which a security situation is considered as a security problem that leads to the initiation of the new security information system.

The first simple security information system that is a candidate for initiation will have as an objective as the minimization of information corruption originating at networks of the business area.

Security information systems with multiple classes

A security information system may be a simple system with one default objective, or a more complex system with multiple default objectives. The complexity of the security information system depends on the number of default objectives involved.

Obviously, its is possible that a security disruption causes any combination of damage, for example, at the same time information corruption and information leakage. It is also possible that a security disruption originates at more than one business information component, for example, people and technology both cause the same damage, say, information corruption.

Corporate Security Evaluation Environment under Common Criteria

The company data processing environment either acquires products from vendors identified by their users, or develop systems using vendor products and components made in-house. Functional security information systems, including the 60 types defined earlier, are developed to integrate with these in-house systems and trusted vendor products.

The CVDS requires that all information resources are evaluated whether they are IT products purchased from vendors or systems developed to satisfy user requirements. For this purpose, a company should maintain a long queue for TOEs that are scheduled for evaluations and re-evaluations.

Conclusion

The article introduced 60 default functional security information systems, defined in terms of 1) DoD's attack models (probe; infrastructure; factory; and authorized-access models), 2) Whitten, Withny, and Barlow's entities (data; people, activities, technology; and networks) induced to cause the attack, and 3) Cohen's security disruptions (information leakage; information corruption; and service denial) produced.

Automatic information security solutions can be developed. Some of the automatic security solutions are already provided as a part of the IDS literature. The CVDS should contain risk and vulnerability assessment that can identify and prioritize the default functional security information systems which should be initiated. The CVDS should also describe categories of PPs required by the company's user community, and diversified STs for systems produced and security product acquired.

he development processes for the default functional information systems proposed are beyond the scope of this article but will be described in details in AIMIT's series on information security. Because of the pre-defined specifications of these systems, their STs will be easier to write, and their evaluation processes easier to conduct.

Table 1: Default objectives for security information systems associated with the 15 security disruption classes.

Security Disruption Class	Default Objective
1. Corrupted People (CP):	Minimize information corruption at the business information component: People
2. Corrupted Activity (CA):	Minimize information corruption at the business information component: Activity
3. Corrupted Technology (CT):	Minimize information corruption at the business information component: Technology
4. Corrupted Data (CD):	Minimize information corruption at the business information component: Data
5. Corrupted Network (CN):	Minimize information corruption at the business information component: Network
6. Leaking People (CP):	Minimize information Leakage at the business information component: People
7. Leaking Activity (CA):	Minimize information Leakage at the business information component: Activity
8. Leaking Technology (CT):	Minimize information Leakage at the business information component: Technology
9. Leaking Data (CD):	Minimize information Leakage at the business information component: Data
10. Leaking Network (CN):	Minimize information Leakage at the business information component: Network
11. Leaking People (CP):	Minimize information Leakage at the business information component: People
12. Leaking Activity (CA):	Minimize information Leakage at the business information component: Activity
13. Leaking Technology CT):	Minimize information Leakage at the business information component: Technology
14. Leaking Data (CD):	Minimize information Leakage at the business information component: Data
15. Leaking Network (CN):	Minimize information Leakage at the business information component: Network

References

1. Cohen, F.B., Protection and Security on the Information Superhighway, John Wiley and Sons, 1995.
2. Connolly, J. L., and B. S. Abramowitz, The Trust Technology Assessment Program and the Benefits to U.S. Evaluations, *Proceedings of the 11th Annual Computer Security Applications Conference*, pp. 157-161, New Orleans, LA, December 1995.
3. NSA, Solution Development and Deployment, and Technical Directors, Information Assurance Technical Framework, Release 2.0.2, 1999.
4. Whitten J.L., Bentley, L.D. and V.M. Barlow, Systems Analysis and Design Methods, Irwin, 1996.

Biography:

Dr. Bel G. Raggad is currently a professor of computer science and information systems, at Pace University, New York. He obtained his Ph.D. in 1989 from Pennsylvania State University, University Park. His current area of research includes Possibilistic Reasoning, Data Mining, and Information Security. Dr. Raggad has about a 100 publications, in proceedings and scholarly journals, including the Journal of Computer Information Systems, Information Processing and Management, Management Decision, Logistic Information Management, Industrial Management and Data Systems, etc. He is currently the President of the American Institute of Management and Information Technologies, and the Editor-in-Chief of the Journal of eBusiness and Information Technologies.