December 2006

Information Availability and Security Policy

Andrew Martin
University of Nebraska

Deepak Khazanchi
University of Nebraska

Information Availability and Security Policy

Andrew P. Martin
Information Systems & Quantitative Analysis
College of Information Science & Technology
University of Nebraska at Omaha
am41475@gimail.af.mil

Deepak Khazanchi
Information Systems & Quantitative Analysis
College of Information Science & Technology
University of Nebraska at Omaha
khazanchi@unomaha.edu

ABSTRACT

Information availability is a key element of information security. However, information availability has not been addressed with the same enthusiasm as confidentiality and integrity because availability is impacted by many variables which cannot easily be controlled. The principal goal of this research is to characterize information availability in detail and investigate how effective enterprise security policy can ensure availability.

Keywords

Information Availability, Confidentiality, Integrity, Security Policy.

INTRODUCTION

Today's businesses are highly dependent upon the availability of information resources. While *information availability* (IAV) is well established as an attribute required for information security (INFOSEC), researchers and practitioners were, and remain, most concerned with maintaining *confidentiality* and *integrity* of the information. IAV remains less understood in practice and ignored in research because of the seemingly endless number of potential factors that can impact the availability of information (Hosmer 1996; Parker, 1992). Brinkley & Schell (1995) argue that there exists an "unboundedness of possible causes of a loss of availability." Tryfonas, Gritzalis & Kokolakis (2000) call for availability to be revisited at the macroscopic level because of our ever-growing dependence upon online information. Lipson & Fisher (1999) believe that "the problems of greatest concern today relate to the availability of information and continuity of services."

The simultaneous increase in dependency upon information resources and attacks against those same resources gives credence to the need, now more than ever, for better understanding of the factors that determine IAV. The astounding cost of unavailability ranges from $1 to 3 million per hour depending upon the industry sector (ODI, 2006). Enterprises require that availability be provided with the same certainty associated with confidentiality and integrity. Therefore, this paper has three main objectives: (1) Explain the notion of IAV and its attributes; (2) Identify key determinants of IAV; and (3) Evaluate the impact of one of these determinants (security policy) on IAV using the example of three firms (cases).

INFORMATION AVAILABILITY

Confidentiality is defined as the "assurance that information is not disclosed to unauthorized entities or processes" (Schou, 1996). By controlling access to information and preventing unauthorized disclosure, a system can achieve confidentiality (Brinkley & Schell, 1995). *Integrity* is defined as the "condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed" (Schou, 1996). Integrity focuses on preventing unauthorized modification of information (Brinkley & Schell, 1995). In contrast to confidentiality and integrity, *availability* is the "timely, reliable access to data and information services for authorized users" (Schou, 1996). More broadly, *availability is about information being accessible as needed, when needed, where needed. The objective of availability is to enable access to authorized information or resources* (CEC, 1991). According to Viles & French (1995), most users expect a "100-100 Web: 100 percent availability for all servers and 100 millisecond latency to every server." This expectation is nearly impossible to sustain, given the many threats to availability.

Components of Information Availability (IAV)

It is reasonably well established that availability has three components: *Reliability*, *Accessibility*, and *Timeliness*. *Reliability* is "the probability of a system performing its purpose adequately for the period of time intended under the operating conditions encountered" (Reibman & Veeraraghavan, 1991). Users do not want to depend upon a system that cannot be trusted to consistently execute their requests. Broadly speaking, *accessibility* is "the degree to which a system is usable by as many people as possible without modification" (http://www.wikepedia.org). There are several access control policies, such as

Mandatory Access Control (MAC) and Discretionary Access Control (DAC) which are supported with access control services such as Role Based Access Control (RBAC) (Sandu, 1996). *Timeliness* is the responsiveness of a system or resource to a user request. Traditionally IAV has mostly been measured by the amount of time an information resource is either processing or not (uptime and downtime) (Wood, 1995).

DETERMINANTS OF INFORMATION AVAILABILITY (IAV)

In Figure 1, each block on the far left represents an IAV factor that impacts the availability of an information resource or the data stored within an information resource. Each factor influences one or more of the attributes of availability, thereby contributing to the overall availability of the information resource. A discussion of each factor and its impact to the enterprise follows.

Security Policy

An enterprise-wide security policy is the foundation for INFOSEC activities and establishes the framework for information processing and use of IT devices within an enterprise. "A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow" (Dekker, 1997).

Most security policies do not address IAV (NRC, 1991; Hosmer, 1996). In fact authors of policies generally concentrate on confidentiality concerns. A system security policy should address who is using the system and the enterprise's expectations of users. Access control mechanisms can be defined and user privileges established. A security policy impacts the reliability of an IS by establishing the thresholds within which the system operates. Current and future architecture and design decisions should be based upon the organization's strategic plan and the enterprise security policy. Furthermore, the level of reliability that the organization also desires may impact the amount of preventative maintenance that occurs, the level of system monitoring and auditing, and evaluation of system effectiveness.

Operational Controls and System Monitoring

By implementing operational controls within the system, security professionals can set limits that protect the organization's information. Operational controls "are those system rules and guidelines that are necessary to manage the day-to-day activities that occur within an enterprise's information resources" (Weber, 1999, p. 291). Operational controls are created to implement security policy, thereby providing a mechanism for enforcing the security policy. Monitoring system performance provides the stakeholders of the enterprise with measurements of how the information resources are operating (Weber, 1999). Real-time monitoring can be used to identify unauthorized activity and can be a powerful tool in protecting the system. According to Hawkins, Yen, & Chou (2000), the best intrusion protection is constant monitoring for intrusions by utilizing the best protection the organization can afford.

Operational controls and system monitoring can work together to enforce security policy and provide security professionals the capability of defending the system at the desired level. Operational controls affect reliability, accessibility, and timeliness by placing appropriate limits, as deemed necessary within the security policy, on users, applications, hardware, data storage, and support functions.

Auditing and System Effectiveness Evaluation

According to Weber (1999, p. 10), auditing IT resources is a "process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently." Auditing is used to verify that the operational controls within the system are successfully implemented and to analyze system behavior to detect misuse or abuse within the system (NRC, 1991). Auditing differs from monitoring in that auditors analyze historical data, whereas monitors trigger alarms based upon real-time activity.

A system effectiveness evaluation is a specific type of audit that not only analyzes the reports and logs, but takes a macro view of the system, the organization, and its personnel to determine how well the system meets the needs of the organization (Weber, 1999). This type of evaluation is especially important for availability, in that the availability is a significant dynamic of several factors that a system effectiveness evaluation measures (*ibid*). Auditing and system effectiveness evaluations provide independent assessment of reliability and timeliness factors within the system. These evaluations may show trends of inappropriate or unauthorized behavior on the system that is not being caught through real-time monitoring.

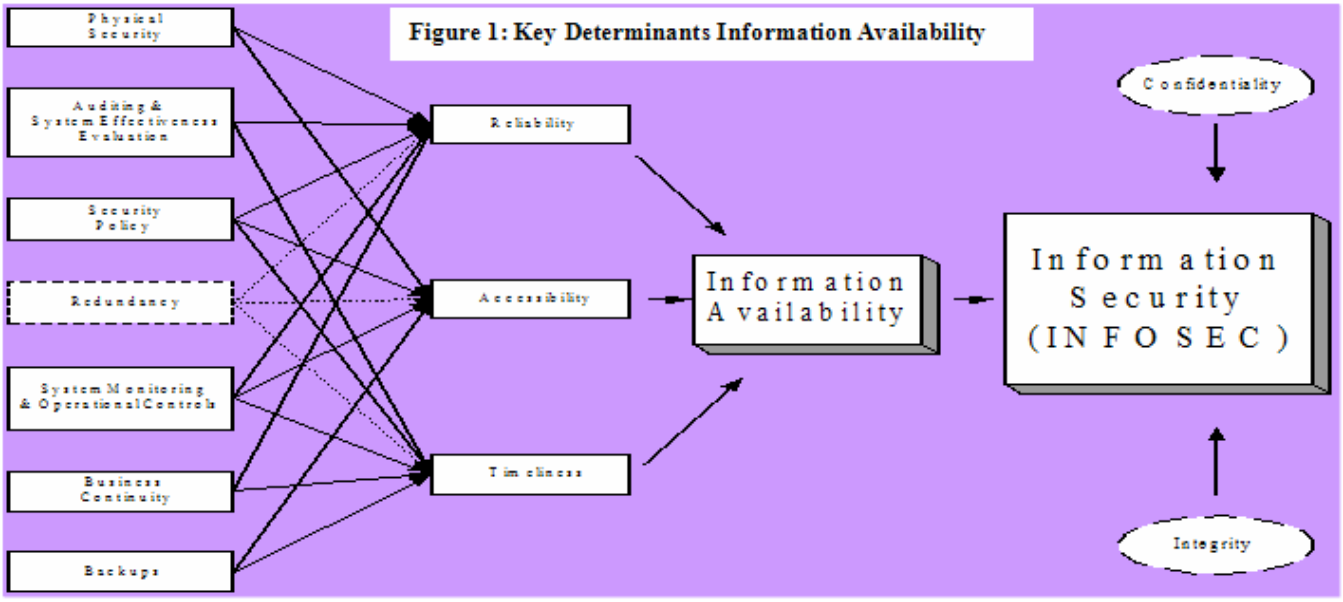

Figure 1: Key Determinants Information Availability

Physical Security

Physical security is a critical prerequisite of IAV. If an organization does not provide physical security to its systems, then unauthorized personnel would have unchallenged access to the organization's systems. The traditional point of view looks at protecting building sites and equipment from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (NCES, 1998). While information is not directly protected through physical security, the information resides on hardware that computer security experts are charged to protect, therefore warranting the attention of both information and security professionals.

Securing the physical hardware and the communications pathways within the enterprise is an important step in assuring the availability of the system. If the device containing the data a user is requesting is unavailable because the device has been stolen, the power to that device has been cut, or the cable connecting the device is disconnected, the impact to the user or process making the request is the same as if the requestor was not authorized to access that data. Bois (2002) aptly asserts "…it is vital that we acknowledge that people seeking to do harm to our information infrastructure will not stop if they cannot get to us via the Internet."

Backups

Backups provide a copy of the data, applications, and O/S settings that are stored within a computer. By having backups, an enterprise can minimize the downtime an enterprise experiences following an event that may leave a storage device damaged or erased (Murphy, 1996). Additionally, backups have become necessary because the data stored within the enterprise is valuable (Parrish, 2001). If the situation arises where information is lost, then a set of backups will greatly reduce the amount of downtime and loss felt by the organization. Backups for both the system and user are required to provide maximum restorable capability to the enterprise. Physical security of the backup media is crucial, requiring the same level of security for the backup capability as other critical applications (Parrish, 2001).

Backups address timeliness and accessibility by providing the enterprise the capability to restore lost files in a timely manner. Without backups, the system would need to be recovered by starting with blank storage.

Business Continuity

Business continuity is a key component of any enterprise's plan to maintain operations in the event of a catastrophic event such as a natural disaster or a network attack. Yet, only 20% of existing continuity plans are workable when tested (Brunetto & Harris, 2001; Kelly, 2000). Business continuity impacts the timeliness and accessibility of a system by providing a systematic and known process for restoring operations in the least time possible. Without a tested continuity plan, the organization has no "insurance" that operations will ever be restored to their pre-event state (Facer, 1999; Wilson, 1997).

SECURITY POLICY AND IAV

The six factors identified earlier can influence IAV by impacting how a request made to an information resource is successfully executed. Each factor plays a role in the success of this complex process, but the enterprise's **security policy** provides direction for how each segment of the IT infrastructure will be implemented, operated, maintained, and when necessary terminated.

In order to address the question of *how (and if) security policies of organizations address IAV and how this impacts IAV*, we conducted three case studies using Yin's (1994) process. The three firms represented in study were as follows:

- **Company 1:** A regional grocery store chain located in the southern United States and Mexico that employs over 55,000 people in over 300 locations and has annual sales in excess of $10 billion. This company is committed to its customers by ensuring that zero outages occur as a result of a security breaches. The firm has an informational website but does not engage in consumer e-commerce. The company's focus is retail sales of groceries, pharmaceuticals, health and beauty products, and a limited selection of housewares, paper goods and chemicals, newspapers and magazines, flowers, and outdoor cooking products. This firm also produces a line of food products.
- **Company 2:** A large member-owned Fortune 500 company that owns and manages more than $65 billion in assets and offices throughout the United States and Europe. It offers members banking, investment, personal property and casualty, and life insurance services. In 2001, this firm posted revenue of $9 billion. Approximately 15% of that revenue is attributed to the company's Internet presence. The firm also maintains a Corporate Intranet which is available to employees and contains several online documents and tools that employees use on a daily basis. This firm employs over 20,000 employees worldwide, with 2,600 personnel in the IT department, and 45 specifically assigned to system security, but holds every employee responsible for security.
- **Company 3:** A national telecommunications provider, offering local and long distance telephone service; dial, dedicated, switched and digital subscriber line (DSL) services; and managed services to customers. The company employs approximately 180,000 employees across the United States and reported $43 Billion in revenue in 2002. It maintains an extensive Internet presence, which includes both informational sites and e-commerce applications. Customers have a variety of options when viewing the company's main webpage, including viewing bills, news releases, or the company's earnings report, as well as requesting new service, troubleshooting telephone problems, or querying the company's online telephone directory, and customers can register to receive e-mails (e.g., new service information, bill-pay reminder, or a reply to a question). In addition to its public presence, employees have access to a myriad of information and services via a corporate Intranet.

Case Study Approach

Following Yin (1994), first, the enterprise security policy or policies of each firm were examined to assess whether the security policy addressed IAV and its enablers using a "document review agenda" set forth in advance. Second, semi-structured interviews were conducted with security personnel from each organization using an *a priori* list of thirty-five questions as a starting point for the discussion.

Data collected from the interviews has been combined with the analysis of each organization's documents to develop a narrative case history for each organization studied. How each firm addresses IAV is examined in terms of the accessibility, reliability and timeliness and the six factors that influence them.

Case Narratives

Company 1

This company's corporate security policy does not mention availability at all, nor does the policy provide specific direction or guidance to the reader as to how availability should be provided. Reliability, however, is included as a function that must be assured. As seen in Figure 2, Company 1 hierarchically organizes its 22 information security policy documents, where specific guidelines and directions are documented in operating procedures that address specific pieces of hardware or software systems.

Reliability: Company 1 ensures reliability by architecting an infrastructure that includes frame relay (FR) and satellite connectivity to all facilities. The entire infrastructure from circuits to printers is redundant. Stores have dual servers, and servers and cash registers are connected to uninterruptible power supplies (UPS). Company 1 has a primary and backup data center, each has generator backup and the two facilities are connected via a SONET backbone. All critical applications have redundant backup with automatic failover. Servers are load-balanced and redundant for each of the application platforms

within the enterprise. Not only is Company 1 committed to assuring reliability in its current infrastructure, their strategy plans to double the current infrastructure capacity within 3 or 4 years. Furthermore, any new piece of hardware or software must go through a certification process to ensure that corporate standards are met.

Accessibility: Company 1 grants access to information based upon the role (RBAC) the employee is fulfilling for the business. Applying the law of least privilege, only information that an employee may need to perform the duties the employee is assigned are made available. It should be noted that any employee movement is not automatically updated within the IS. Due to the manual request that must be made to the Information Security Office, there is a strong possibility that an employee's role may not be updated when the employee changes jobs. Company 1 also recognizes that information may be released to outside parties who must request access to information through the Public Affairs Department.

Timeliness: Timeliness is not addressed in Company 1's security policy. By architecting the infrastructure with redundant components and connectivity, reduced latency is achieved as a byproduct of reliability. Metrics of system "uptime" are taken mostly of the enterprise servers which are concentrated at the data center.

Company 2

Company 2 has high uptime requirements of its IT resources. This company's Internet presence, and the applications made available to users, requires 100% uptime to deliver on the company's promise to its users. This company has built an INFOSEC policy pyramid, as seen in Figure 3, to link the corporate security policy with technical procedures for specific systems. The top layer of the pyramid is the corporate security policy with the corporation's key security metrics filling the next layer. These two documents address INFOSEC from a business perspective. The third layer, the corporation's security guidelines, begins to discuss security in technical detail, but also include business requirements.

The final layer of the pyramid is individual procedures, which apply to specific information resources. The company's data center and alternate facility are located within 200 miles of each other. Both are unmarked buildings, with on-site security personnel.

Reliability: Company 2 addresses reliability through a combination of network planning, information security, and disaster recovery actions. The company's guidelines state requirements, such as dual, non-duplicated paths within the city where the data center is located and separate upstream providers for both voice and data traffic. The same requirement exists for the alternate data center. Furthermore, its two data centers are connected via an OC-12 connection and the backup data center can automatically assume the workload in the event that an outage occurs at the primary data center. Both data centers are hardened, stand alone facilities with the capability to feed and lodge personnel for an extended period of time. To further enhance the enterprise's reliability, Company 2 has developed extensive business continuity plans, which would be executed during an event (e.g., natural disaster; physical or cyber attack; or power outage). These continuity plans are reviewed every 60 days to ensure that modifications to the physical and logical network have been recorded in the continuity plans. Scenario-based exercises are regularly executed at 6-8 week intervals.

Auditing agencies regularly inspect the performance and operation of Company 2's IT resources. The company's Internal Audit Division, which is separate from the IT Company, analyzes how the system the performance level, run security scans, check data integrity, and review system logs. External agencies (e.g., Securities and Exchange Commission (SEC) and the Federal Deposit Insurance Company (FDIC)) also audit Company 2.

Accessibility: Company 2 currently addresses accessibility through role-based access control (RBAC) and an industry-leading Information Management System (IMS). Employees are granted access based upon the principle of least access, which is based upon the employee's position. If an employee moves from one job to another, then the losing manager triggers a manual process to revoke current privileges and the gaining manager requests new access privileges required to work in the new position. Members are required to log-on to the Internet site, which initiates the member's session. Once logged-on, the traffic from the company's Internet site pass through the IMS, a transaction monitor which makes a member's information accessible. Members who use the company's Internet site may access account information, request services, and in some cases conduct business transactions without visiting a physical office or speaking to a company representative.

Company 2 has a robust backup capability. Backups are written at the Backup Data Center and stored off-site. Backups are handled by a leading industry backup application, which controls the backup process. Company 2 does not take a single-minded attitude toward backups. Each system has specific backup requirements that are defined when the system is brought online. Those requirements are programmed into the backup system, thereby providing consistent control of the backup process. In addition to data files, the company's Database (DB) and system logs are also backed-up. By including logs in the backup schema, Company 2 can recreate the stored data and any transactions that occurred since the last backup and the loss of data.

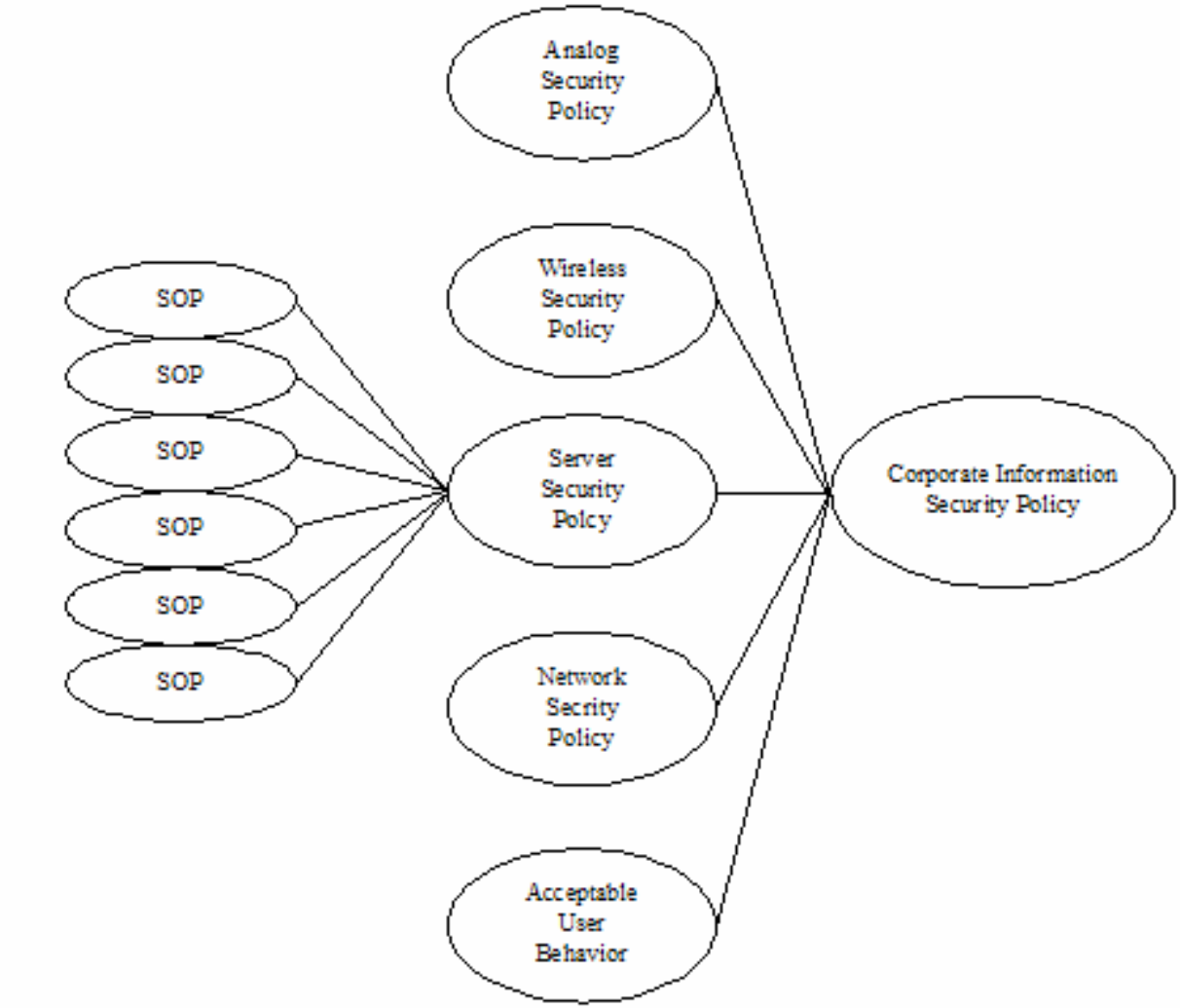

Figure 2: Company 1 Security Policy Hierarchy

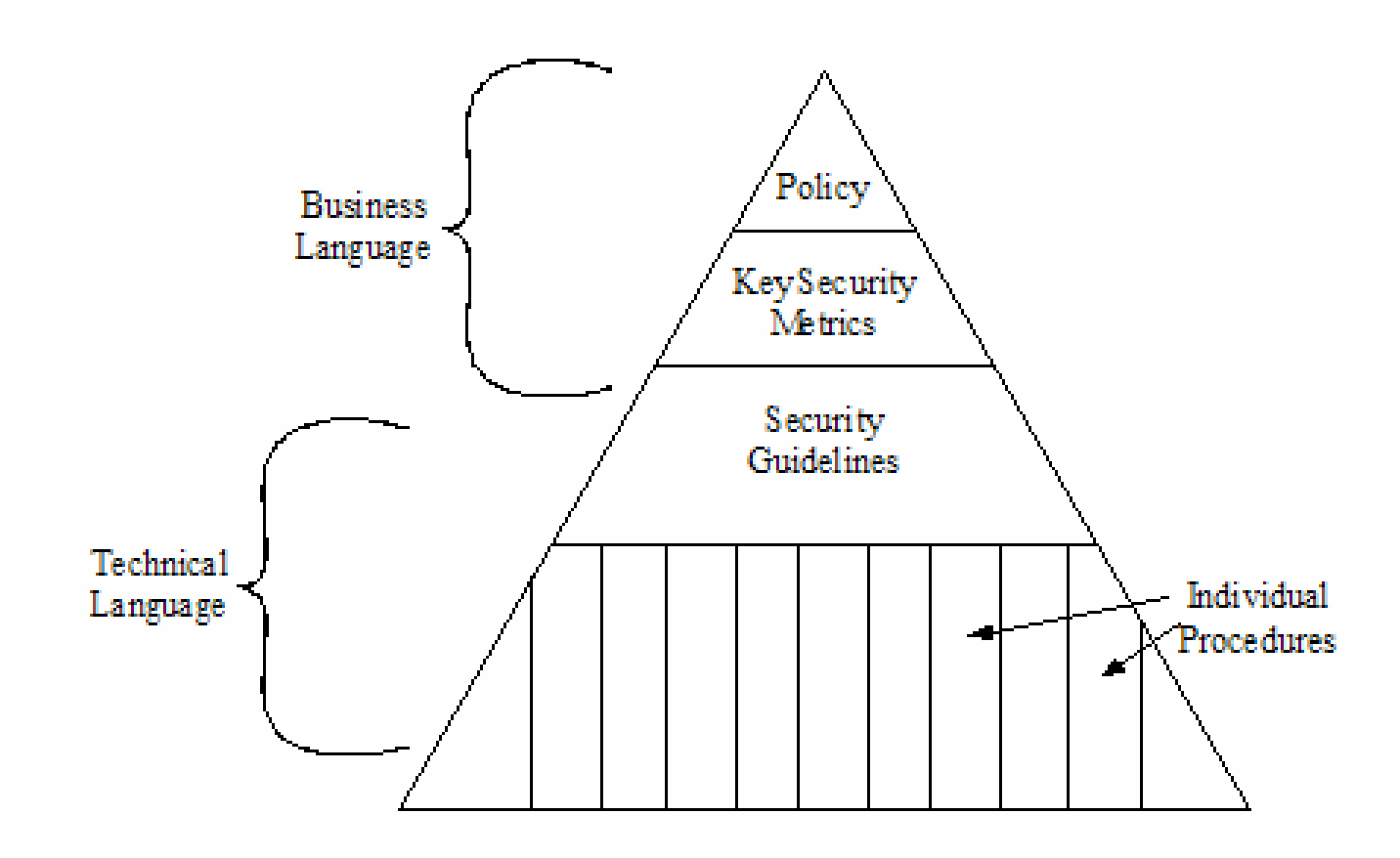

Figure 3: Company 2 Security Policy Pyramid

Timeliness: Company 2 addresses timeliness by monitoring, in real-time, certain aspects of circuits, hardware, and software. Each IS has system-level response time objectives (e.g., end-to-end or application to application). Several IT resources are designed using an N-tiered model. By architecting systems in this way, Company 2 has enhanced the capabilities of its information resources, but has increased the complexity of the applications operating within the enterprise. To effectively measure timeliness, the components of each IS are measured separately. These separate response times are then summed to provide a high-level response time. Company 2 is then able to identify poor performance at a more granular level and make the correct adjustment to keep the response times below the maximum response time stated in each system's system-level objective.

Company 2 balances real-time monitoring with after-the-fact auditing of system and event logs. The business decides how to strike this balance by analyzing the business requirements and associated risks. The greater the risk assessed, the more real-time monitoring is used. Alarms are based upon a programmed threshold for each IS. Company 2 also audits system and event logs to analyze user behavior and for the purpose of post-event analysis. By employing real-time monitoring, Company 2 can address timeliness and defend the enterprise. This coupled with auditing can address system faults to prevent future problems.

Company 3

IT services in Company 3 have been consolidated into a separate business unit. Day-to-day security is maintained by system administrators and operations personnel who monitor the public and private networks that Company 3 operates. At Company 3, INFOSEC is a part of the company's "Code of Business Conduct" (hereinafter referred to as "the Code"). This document states the boundaries within which employees of Company 3 must act. Included in the Code are clauses about the corporate expectation of privacy, use of company property (including information), ethics, and equal employment opportunity. As seen in Figure 4, Company 3 has written Executive support for CIS and these executive documents state that INFOSEC is critical to the success of the business. It is worth noting that the policy provides the company's confidentiality, integrity, and availability definitions. Additionally, this policy explicitly states that non-availability could be a characteristic of company information if the company's information is not protected. While *availability* is defined in Company 3's security policy, the policy is written at an executive-level. The technology used to accomplish the goals stated in the policy is documented in the company's INFOSEC standards. INFOSEC guidelines address how to use the technology to accomplish those policy goals.

Reliability: Company 3 addresses reliability by clustering and consolidating data storage and processing and by employing redundant circuitry throughout its logical and physical network. The company has strategically located regional data centers which are controlled by an on-site security detail, with access card and biometric access devices installed at points of entry to computer rooms. Additionally, Company 3 has identified a comprehensive list of hardware and software documentation (i.e., business benefits, technologies used, backup and application recovery contacts and requirements, and field support impact) which IT personnel use to maintain each IT resource. Company 3 employs multiple firewalls throughout the enterprise, each of which is dedicated to a certain class of user (e.g., affiliates, business partners, employees).

Company 3 conducts systematic backups at all its data centers. In addition to backups at the data center level, Company 3 has implemented an application which enables employees to backup critical files residing on a desktop PC. In the event that a data center experiences an event resulting in downtime, each data center is linked to another data center, which acts as its backup. Additionally, each data center maintains offline backup storage for itself and the data center to which it is linked.

As a national telecommunications provider, Company 3 is very concerned about disaster recovery and business continuity. As a result, Company 3 has a workgroup within the company's Asset Protection Division dedicated to planning the response to an unforeseen event. Before any IT resource is added to the enterprise, a continuity plan is developed and tested. Enterprise-wide tests of the company's continuity plans are conducted annually.

Accessibility: Company 3 addresses accessibility through RBAC and the rule of least privilege. Employees are granted access based upon the needs of their position and requirements of Federal Regulations. Company 3 has a standardized User ID and utilizes an industry standard directory service. This enables developers to verify the identity of the user. This does not, however, allow all users to access all IT resources. For some IT resources, ITO grants access; for others the administrator or owner of the IT resource grants access. Company 3 tracks access controls manually. If an employee changes positions, the employee will request access to any new IT resources that are required to complete work in the new position. For auditing purposes, all access requests are documented and the accountability trail maintained. Additionally, Company 3 maintains several classifications of information, which define the level at which that information can be released.

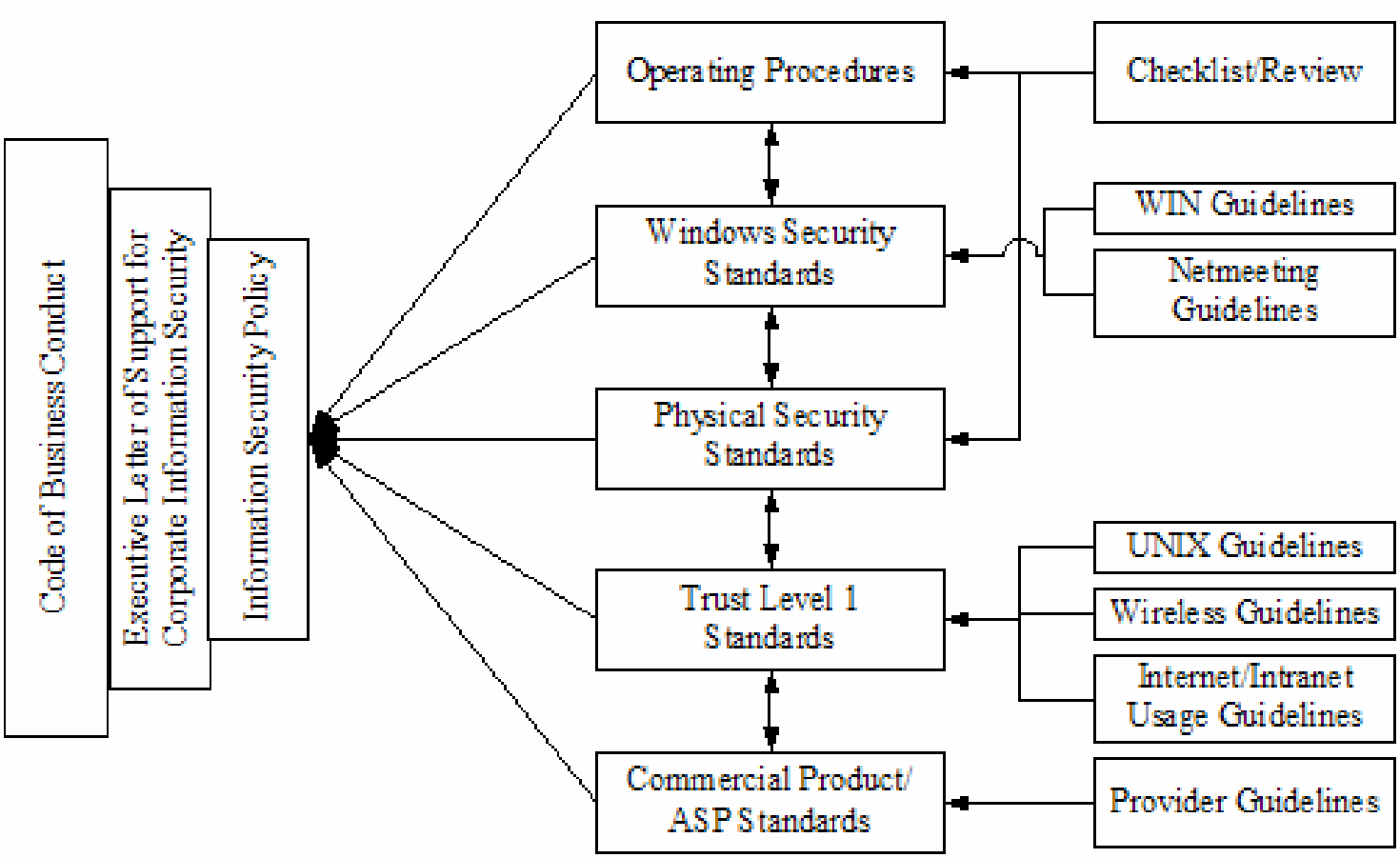

Figure 4: Company 4 Security Policy Diagram

Timeliness: Timeliness is addressed through the Systems Operations Center (SOC), where monitoring throughout the logical and physical network is conducted. Company 3 employs a number of alarms which are activated based upon the rules applied to each alarm. Periodically, the need for each alarm is reviewed to ensure that the cost of alarming the network is commensurate with the risk of loss. Company 3 applies specific standards to its various IT resources. How each standard is applied is dependent upon the criticality of the resource and the risk to the business. These factors are determined as part of the design process, and timeliness metrics are made available to the IT staff through the Availability Management group.

Company 3 has an active Auditing group. This group not only audits IT systems, but the entire business. Audits are conducted when irregularities within the business arise. During these audits, the supporting IT resources are analyzed. Any identified IT or INFOSEC findings are included in the report which is provided to the President of the business unit, and applicable sections are sent to the personnel responsible for that function (e.g., INFOSEC findings are sent to the appropriate CIS consultant).

SUMMARY OF FINDINGS

Based on our understanding of factors that influence IAV and the related analysis of the data collected from three firms, we can draw the following conclusions.

Ø *Whether an organization's security policy addresses IAV or not, business requirements are driving IT professionals to provide IAV.*

IAV was absent from Company 1's security policy; the word 'availability' was included in Company 2's security policy; and defined in Company 3's security policy. Regardless of how IAV was addressed in the company's security policy, the business requirements of all three companies had identified IAV. Furthermore, information is being used by each company to bring the business closer to both customer and other businesses. By using IT to connect geographically dispersed locations, the companies interviewed have leveraged consolidated storage plans to decrease operating costs and enhance the services that each company can provide. These applications are not driven by INFOSEC considerations, but by business requirements. The INFOSEC literature reviewed for this paper indicates that IAV is not being addressed because unavailability has infinite causes. Conversely, businesses have embraced the possibilities (and the enhanced revenues) which effective IAV brings.

Ø *Security policies provide broad INFOSEC goals, which may include IAV, but do not provide sufficient detail to address IAV in a day-to-day context.*

After reviewing each company's security policy and interviewing the company's INFOSEC professional(s), it is clear that each company did not desire to have detailed security policies. Applying a hierarchical approach to the policies, which all three companies did, allowed each company to secure executive support for INFOSEC goals and develop more granular documentation (i.e., standards, guidelines or procedures) for use by personnel charged with day-to-day control of the information enterprise. The degree to which IAV is addressed in the security policy does not necessarily correspond with the level of IAV that is demonstrated by each company.

Ø *Of the three components of IAV, reliability is an obvious requirement in all cases. Timeliness and accessibility, however, do not receive the same attention.*

The companies participating in this research had all architected highly redundant infrastructures. Each company had done this to remove as many single points of failure as possible. Furthermore, Companies 1 and 3 addressed IAV through redundancy, but neither addressed timeliness. Company 2 also addressed IAV through redundancy and had detailed timeliness metrics which provided additional granularity to Company 2. None of the companies addressed IAV through the context of accessibility. In general, timeliness seems to be addressed through system performance parameters rather than through security policy. For example, Company 2 recorded response times to provide metrics which could be analyzed to address timeliness.

Ø *Given the large showing of redundant IT components in the participating companies, there may be cause to add 'Redundancy' as a determinant of IAV.*

Each of the participating companies had redundant hardware and software, communications pathways, and data centers. Each company also placed a great deal of confidence in having redundancy to provide IAV in the event of an outage (e.g., natural disaster, manmade catastrophe, accidental or malicious action, or hardware or software failure). Therefore, after

reviewing the data collected for this paper, we believe that 'Redundancy' should be included as the seventh determinant of IAV in our model displayed in Figure 1. Past research in this area has shown that *redundancy* provides an organization the ability to reconstruct information elements that may be corrupted or damaged and minimize unavailability by utilizing redundant capabilities or restoring the capabilities of the IS (Jajodia *et al*., 1999). Additionally, having redundant connectivity that has adequate capacity for the traffic load of the organization is an imperative for many organizations today (Hutt *et al*., 1995).

Ø *The ability to provide adequate IAV is impeded by resource constraints and the need to balance IAV with the other security attributes (i.e., confidentiality and integrity), and economic and political considerations.*

Past research shows that there is greater importance attached to confidentiality and integrity as compared with IAV. Our study provides some support for the notion that there is a division between INFOSEC requirements and business requirements. Furthermore, we find that IAV is addressed from a business perspective and not from a security perspective. It is apparent that the ability to deliver adequate IAV has to be balanced with other security attributes and business requirements. Also, IAV may need to be considered separately from confidentiality and integrity and potentially a separate IAV policy may be needed within organizations to overcome the potential threats to availability.

CONCLUDING REMRKS

In this paper we have developed a detailed understanding of information availability (IAV) an important attribute of modern information security. Based on past literature, we provide a detailed list of factors or determinants of information availability and its attributes (reliability, accessibility and timeliness). We evaluate the impact of a firm's security policy on IAV and discuss some key findings. It is important to note that we intentionally focused our attention in this research on how one determinant of IAV, security policy, impacts IAV. This is because we felt that without a well-developed security policy, an enterprise is ill-prepared to ensure that information resources with be available and that the data is correct. However, we believe that further research needs to be conducted on how the other determinants influence IAV and in what way the interactions between the various determinants impacts IAV and INFOSEC.

REFERENCES

1. Bois, J. (2002, April 4). Protect yourself. Retrieved from http://rr.sans.org/physical/protect.php. SANS Institute (http://www.SANS.org).
2. Brinkley, D. L. & Schell, R. R. (1995) *Concepts and terminology for computer security*. In. M. D. Abrams, S. Jajodia & H. J. Podell (Eds.), *Information security: An integrated collection of essays*, 11-39. Los Alamitos, CA: IEEE Computer Society Press.
3. Brunetto, G. & Harris, N. L. (2001) Disaster recovery: How will your company survive? [Electronic version]. *Strategic Finance*, 82(9), 57-61.
4. CEC -- Commission of the European Communities (1991). *Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria: Version 1.2* [Electronic version]. Luxembourg: Office for Official Publications of the European Communities.
5. Dekker, M. (1997) Security of the Internet. *The Froehlich/Kent Encyclopedia of Telecommunications*, Vol. 15, 231-255. Retrieved May 21, 2002 from http://www.cert.org/encyc_article/tocencyc.html.
6. Facer, D. (1999) Rethinking: Business continuity [Electronic version]. *Risk Management*, 46(**10**), 17-18.
7. Hawkins, S., Yen, D. C., & Chou, D. C. (2000) Awareness and challenges of Internet security. *Information Management & Computer Security*, 8(**3**), 131-143.
8. Hosmer, H. H. (1996) Availability policies in an adversarial environment. *Proceedings of the 1996 Workshop on New Security Paradigms*, USA, 105-117. Retrieved April 10, 2002 from http://doi.acm.org/10.1145/304851.304876.
9. Hutt, A. E., Bosworth, S., & Hoyt, D. B. (Eds.). (1995) *Computer security handbook* (3rd edition). New York, NY: John Wiley & Sons, Inc.
10. Jajodia, S., McCollum, C. D. & Ammann, P. (1999) Trusted recovery [Electronic version]. *Communications of the ACM*, 42 (7), 71-75.

11. Kelley, J. (2000) Business continuity: Battling high-tech exposures [Electronic version]. *Risk Management*, 47(**5**), 31-33.
12. Lipson, H. F. & Fisher, D. A. (1999) Survivability--A new technical and business perspective on security [Electronic version]. *Proceedings of the 1999 workshop on new security paradigm*, Canada, 33-39.
13. Martin, A. (2003) Key determinants of information availability: a multiple case study. Unpublished MS in MIS Thesis, University of Nebraska at Omaha.
14. Millen, J. K. (1992) Resource allocation model for denial of service. *Proceedings of the Symposium on Research in Security and Privacy*. USA, 137-147.
15. Murphy, M. (1996, February 1) Backup strategy. Retrieved May 14, 2002 from http://www.linuxjournal.com/article.php?sid=1208.
16. NCES -- National Center for Education Statistics. (1998, September 22) *Safeguarding your technology: Practical guidelines for electronic education information security* [Electronic version] [Handbook]. In: Szuba, T. and the Technology and Security Task Force of the National Forum on Education Statistics. Retrieved June 20, 2002, from http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=98297
17. NRC -- National Research Council (1991) *Computers at risk: Safe computing in the information age*. Washington, D.C.: National Academy Press.
18. ODI -- Ontrack Data International (2006) Cost of Data Loss. Retrieved January 12, 2006 from http://www.ontrack.com/understandingdataloss/.
19. Parker, D. B. (1992) Restating the foundation of information security. *Proceedings of the Eighth International Conference on Information Security*, Netherlands, 139-151.
20. Parrish, S. (2001, August 30) Security considerations for enterprise level backups. Retrieved June 7, 2002 from http://rr.sans.org/backup/enterprise_level.php.
21. Reibman, A. L. & Veeraraghavan, M. (1991) Reliability modeling: An overview for system designers [Electronic version]. *Computer*, 24(**4**), 49-57.
22. Sandu, R. (1996) Access control: The neglected frontier [Electronic version]. *Proceedings of the First Australasian Conference on Information Security and Privacy*, Australia, 219-227.
23. Schneier, B. (2000) *Secrets and lies: Digital security in a networked world*. New York, NY: John Wiley & Sons, Inc.
24. Schou, C., Editor (1996) *Information Systems Security Organization (ISSO) Glossary of INFOSEC and INFOSEC related terms*, Vols. I & II. Idaho: Idaho State University.
25. Tryfonas, T., Gritzalis, D. & Kokolakis, S. (2000, August) A qualitative approach to information availability. Proceedings of Information Security for Global Information Infrastructures (IFIP TC11). *Sixteenth Annual Working Conference on Information Security*, USA, 37-47.
26. Yin, R. K. (1994) *Case study research: Design and methods*. (2nd Ed.). Thousand Oaks, CA: SAGE Publications, Inc.
27. Viles, C. L. & French, J. C. (1995) Availability and latency of world wide web information servers. *Computing Systems*, 8 (1), 61-91.
28. Weber, R. (1999) *Information systems control and audit*. Upper Saddle Creek, New Jersey: Prentice-Hall, Inc.
29. Wilson, K. (1997, September 2) Contingency and recovery planning: Checklist for information systems. Retrieved on June 6, 2002 from http://socrates.berkeley.edu:2001/em/checklist.html.
30. Wood, A. (1995) Predicting client/server availability [Electronic version]. *Computer*, 28(4), 41-48.