HANDBOOK OF RESEARCH ON
INFORMATION SECURITY AND ASSURANCE

JATINDER N. D. GUPTA & SUSHIL K. SHARMA
Handbook of Research on Information Security and Assurance

Jatinder N.D. Gupta
*The University of Alabama in Huntsville, USA*

Sushil K. Sharma
*Ball State University, USA*
Table of Contents

Preface ...................................................................................................................... xxiv

Acknowledgment .................................................................................................... xxviii

Section I  
Enterprise Security

Chapter I  
Ransomware: A New Cyber Hijacking Threat to Enterprise ........................................ 1  
Xin Luo, The University of New Mexico, USA  
Qinyu Liao, The University of Texas at Brownsville, USA

Chapter II  
E-Commerce: The Benefits Security Risks, and Countermeasures ............................... 7  
Joon S. Park, Syracuse University, USA  
Jillian K. Lando, Syracuse University, USA

Chapter III  
Information Warfare: Survival of the Fittest............................................................ 18  
Pamela Ajoku, University of Pittsburgh, USA

Chapter IV  
Evolution of Enterprise Security Federation ......................................................... 29  
Gaeil An, Electronics and Telecommunications Research Institute, Korea  
Joon S. Park, Syracuse University, USA

Chapter V  
A Holistic Approach to Information Security Assurance and Risk Management in an  
Enterprise .............................................................................................................. 42  
Roy Ng, Ryerson University, Canada

Chapter VI  
An Integrative Framework for the Study of Information Security Management Research .......................................................... 55  
John D’Arcy, University of Notre Dame, USA  
Anat Hovav, Korea University, Korea
Chapter VII
Information Systems Risk Management: An Audit and Control Approach ......................................................... 68
Aditya Ponnam, Louisiana State University, USA
Britta Harrison, Louisiana State University, USA
Ed Watson, Louisiana State University, USA

Section II
Security Approaches, Frameworks, Tools, and Technologies

Chapter VIII
Distributed Denial of Service Attacks in Networks ......................................................................................... 85
Udaya Kiran Tapakula, Macquarie University, Australia
Vijay Varadharajan, Macquarie University, Australia

Chapter IX
Firewalls as Continuing Solutions for Network Security .................................................................................. 98
Andy Luse, Iowa State University, USA
Anthony Townsend, Iowa State University, USA
Kevin Scheibe, Iowa State University, USA

Chapter X
An Immune-Inspired Approach to Anomaly Detection .................................................................................. 109
Jamie Twycross, University of Nottingham, UK
Uwe Ackelae, University of Nottingham, UK

Chapter XI
Cryptography for Information Security ............................................................................................................ 122
Wasim A. Al-Hamdani, Kentucky State University, USA

Chapter XII
Memory Corruption Attacks, Defenses, and Evasions ...................................................................................... 139
Carlo Bellettini, Università degli Studi di Milano, Italy
Julian L. Rrushi, Università degli Studi di Milano, Italy

Chapter XIII
Design and Implementation of a Distributed Firewall ....................................................................................... 152
Dalila Boughaci, LRIA – USTHB, Algeria
Brahim Oubeka, LRIA – USTHB, Algeria
Abdelkader Aissioui, LRIA – USTHB, Algeria
Habiba Drias, LRIA – USTHB, Algeria
Belaid Benhamou Technopôle de Château-Gombert, France

Chapter XIV
A Formal Verification Centred Development Process for Security Protocols .................................................. 165
Tom Coffey, University of Limerick, Ireland
Reiner Döjen, University of Limerick, Ireland

Chapter XV
Edge-to-Edge Network Monitoring to Detect Service Violations and DoS Attacks ........................................... 179
Ahsan Habib, Siemens TTB Center, Berkeley, USA
Chapter XVI
A “One-Pass” Methodology for Sensitive Data Disk Wipes ................................................................. 193
  Doug White, Roger Williams University, USA
  Alan Rea, Western Michigan University, USA

Chapter XVII
Securing E-Mail Communication with XML Technology ................................................................. 202
  Lijun Liao, Horst-Görtz Institute for IT Security, Germany
  Mark Manulis, Horst-Görtz Institute for IT Security, Germany
  Jörg Schwenk, Horst-Görtz Institute for IT Security, Germany

Chapter XVIII
Aspect-Oriented Analysis of Security in Distributed Virtual Environment ....................................... 218
  Li Yang, University of Tennessee at Chattanooga, USA
  Raimund K. Ege, Northern Illinois University, USA
  Lin Luo, Florida International University, USA

Chapter XIX
Information Availability .......................................................................................................................... 230
  Deepak Khazanchi, University of Nebraska at Omaha, USA
  Andrew P. Martin, University of Nebraska at Omaha, USA

Chapter XX
Formal Analysis and Design of Authentication Protocols ............................................................... 240
  Siraj Ahmed Shaikh, United Nations University (UNU), Macau, SAR China

Chapter XXI
Access Control Frameworks for a Distributed System ..................................................................... 254
  Rajeev R. Raje, Indiana University-Purdue University Indianapolis, USA
  Alex Crespi, Indiana University-Purdue University Indianapolis, USA
  Omkar J. Tilak, Indiana University-Purdue University Indianapolis, USA
  Andrew M. Olson, Indiana University-Purdue University Indianapolis, USA
  Carol C. Burt, 2AB Inc., Helena, AL, USA

Chapter XXII
Implications of FFIEC Guidance on Authentication in Electronic Banking ...................................... 266
  Manish Gupta, State University of New York, Buffalo, USA
  JinKyoo Lee, Oklahoma State University, USA
  H. R. Rao, State University of New York, Buffalo, USA

Chapter XXIII
Disruptive Technology Impacts on Security ..................................................................................... 279
  Sue Conger, University of Dallas, USA
  Bret J. L. Landry, University of Dallas, USA
Section III
Security Policies and Procedures

Chapter XXIV
Internal Auditing for Information Assurance ................................................................. 292
Sushma Mishra, Virginia Commonwealth University, USA
Amita Goyal Chiu, Virginia Commonwealth University, USA

Chapter XXV
IT Continuity in the Face of Mishaps ............................................................................. 301
William H. Friedman, University of Central Arkansas, USA

Chapter XXVI
Business Continuity and Disaster Recovery Plans ..................................................... 308
Yvette Ghormley, Saint Leo University, USA

Chapter XXVII
Security Policies and Procedures ................................................................................. 320
Yvette Ghormley, Saint Leo University, USA

Chapter XXVIII
Enterprise Access Control Policy Engineering Framework ....................................... 331
Arjmand Samuel, Purdue University, USA
Ammar Masood, Purdue University, USA
Arif Ghafoor, Purdue University, USA
Aditya Mathur, Purdue University, USA

Chapter XXIX
Information Security Policies: Precepts and Practices .............................................. 341
Sushil K. Sharma, Ball State University, USA
Jatinder N. D. Gupta, The University of Alabama at Huntsville, USA

Chapter XXX
A Guide to Non-Disclosure Agreements for Researchers ........................................ 347
Paul D. Witman, California Lutheran University, USA
Kapp L. Johnson, California Lutheran University, USA

Chapter XXXI
Assurance for Temporal Compatibility Using Contracts ........................................ 360
Omkar J. Tilak, Indiana University-Purdue University Indianapolis, USA
Rajiv R. Raja, Indiana University-Purdue University Indianapolis, USA
Andrew M. Olson, Indiana University-Purdue University Indianapolis, USA

Chapter XXXII
Spatial Authentication Using Cell Phones .................................................................... 372
Arjan Durresi, Indiana University-Purdue University Indianapolis, USA
Section IV
Mitigating Security Risks

Chapter XXXIII
Plugging Security Holes in Online Environment
Sushil K. Sharma, Ball State University, USA
Jatinder N. D. Gupta, The University of Alabama in Huntsville, USA
Ajay K. Gupta, Gsecurity, Inc., USA

Chapter XXXIV
Six Keys to Improving Wireless Security
Erik Graham, General Dynamics C4 Systems, USA
Paul John Steinbart, Arizona State University, USA

Chapter XXXV
Human Factors in Information Security and Privacy
Robert W. Proctor, Purdue University, USA
E. Eugene Schultz, High Tower Technologies, USA
Kim-Phuong L. Vu, California State University, USA

Chapter XXXVI
Threat Modeling and Secure Software Engineering Process
Wm. Arthur Conklin, University of Houston, USA

Chapter XXXVII
Guarding Corporate Data from Social Engineering Attacks
Christopher M. Botelho, Baylor Health, USA
Joseph A. Cazier, Appalachian State University, USA

Chapter XXXVIII
Data Security for Storage Area Networks
Tom Clark, Brocade Communications, USA

Chapter XXXIX
Security Awareness: Virtual Environments and E-Learning
Edgar Weippl, Vienna University of Technology and Science, Austria & Secure Business, Austria

Chapter XL
Security-Efficient Identity Management Using Service Provisioning (Markup Language)
Manish Gupta, State University of New York, Buffalo, USA
Raj Sharman, State University of New York, Buffalo, USA

Chapter XLI
A Strategy for Enterprise VoIP Security
Dwayne Stevens, Community Trust Bank, USA
David T. Green, Governors State University, USA
Chapter XLII
Critical Success Factors and Indicators to Improve Information Systems Security Management

Jose M. Torres, TECNUN University of Navarra, Spain
Jose M. Sarriegi, TECNUN University of Navarra, Spain
Javier Santos, TECNUN University of Navarra, Spain

Chapter XLIII
Privacy, Societal, and Ethical Concerns in Security

Rebecca H. Rutherford, Southern Polytechnic State University, USA

Chapter XLIV
An MDA Compliant Approach for Designing Secure Data Warehouses

Rodolfo Villarroel, Universidad Católica del Maule, Chile
Eduardo Fernández-Medina, Universidad de Castilla-La Mancha, Spain
Mario Piattini, Universidad de Castilla-La Mancha, Spain
Juan Trujillo, Universidad de Alicante, Spain

Chapter XLV
Survivability Evaluation Modeling Techniques and Measures

Hai Wang, The Pennsylvania State University, USA
Peng Liu, The Pennsylvania State University, USA

Chapter XLVI
The Last Line of Defense: A Comparison of Windows and Linux Authentication and Authorization Features

Art Taylor, Rider University, USA

Chapter XLVII
Bioterrorism and Biosecurity

M. Pradhan, Indiana University-Purdue University Indianapolis, USA
Y. Xia, Indiana University-Purdue University Indianapolis, USA

About the Contributors

Index
Chapter XIX
Information Availability

Deepak Khazanchi
University of Nebraska at Omaha, USA

Andrew P. Martin
University of Nebraska at Omaha, USA

ABSTRACT
This chapter describes the concept of information availability (IAV) which is considered an important element of information security. IAV is defined as the ability to make information and related resources accessible as needed, when they are needed, where they are needed. In the view of the authors, this notion encompasses more than just making sure that the information technology (IT) infrastructure is technically adequate and continuously available, but it also emphasizes other often-ignored attributes of IAV, such as appropriate policies and procedures, an effective security policy, and the establishment of a workable business continuity plan. Thus, the goal of the chapter is to define IAV in the context of information security and elaborate on each of these first and second order determinants of information availability.

INTRODUCTION
As the Internet has matured, enterprises have leveraged information technology (IT) to enhance their operations and improve the services to which consumers have access. The marketplace has embraced these new capabilities, and many consumers now depend upon these services on a daily basis. To meet consumer demands, many businesses now require critical information systems (IS) be online 24 hours per day, seven days per week, and 365 days per year. Due to this increased dependency, the availability of critical IT resources has assumed new importance. While availability is not a new attribute of information, it has dramatically grown in its importance because of the criticality of systems that are now operating in a distributed computing environment. According to recent estimates, the cost of unavailability is astounding and ranges from $1 to 3 million per hour depending upon the industry sector (Ontrack Data International, 2006). Enterprises require that availability be provided with the same certainty associated with confidentiality and integrity. Therefore, proactive steps need to be taken to mitigate risks that could result in unavailability and procedures need to be in-place to respond to an event that threatens to degrade availability.

Security professionals have developed several protocols, tools, and techniques in an attempt to achieve three generally accepted information attributes (i.e., confidentiality, integrity, and availability), thereby resulting in enhanced Information Security (INFOSEC) (Jonsson, 1998). A system’s effectiveness is improved by INFOSEC in that the attributes provided offer defensive capabilities (Maconachy, Schou, Ragsdale, & Welch, 2001). These defensive capabilities are necessary, because information has real value (Denning,
1999) and an organization cannot afford to stand by while its information is made unavailable by natural disaster, hardware or software malfunction, or accidental or intentional loss of resources or data (Hutt, Bosworth, & Hoyt, 1995, pp. 16).

While Information Availability (IAV) is well-established as an attribute required for INFOSEC, few security researchers and practitioners have chosen to address IAV with the same enthusiasm as the other security attributes. INFOSEC researchers and practitioners were, and remain, most concerned with maintaining confidentiality and integrity of the information. According to Hosmer (1996), information availability remains mostly misunderstood and unresearched because of the seemingly endless number of potential factors that can impact the availability of information. Hosmer argues that the current availability paradigm is inadequate and emphasizes that social threats as well as technical threats add to the multifaceted nature of IAV. Furthermore, communications protocols were designed to make information and resource sharing possible; INFOSEC emerged afterwards. IAV was treated as a function of bringing-up an IS and in terms of a user having access to that system. Initially, access was controlled by physical barriers and obstacles. As networking became more popular (and anyone with a computer, a modem, and the knowledge of the operating system (O/S) could remotely access an IS), the need for INFOSEC emerged. IAV was a prerequisite; therefore, INFOSEC researchers and practitioners needed to develop methods and procedures of maintaining confidentiality and integrity. This security paradigm was necessary, but never truly sufficient. For example, if an IS did not have enough modems, then users would receive a busy signal. If the IS was offline, then users could not access the IS. Users accepted the technological constraints of the time, but as technology has improved dramatically over the past decade, and IT resources have become more reliable and pervasive, it seems that the user’s tolerance level for downtime has decreased.

The need to address IAV is both past due and necessary, particularly in the context of the information security challenges of today. The paradigm needs to shift (and is to some extent already shifting) from one that assumes IAV to one that provides sustainable IAV—unavailability is not an option in today's context. To achieve this end, a new understanding of IAV and the factors that impact it can help INFOSEC practitioners analyze how each factor can be addressed within the context of their enterprise, and determine whether or not to initiate changes that will achieve IAV for the organization’s critical logical and physical IT resources. Therefore, this chapter has two main objectives: (1) describe the notion of IAV as it relates to information security and identify key first and second order factors that impact Information (IAV) based on an analysis of the a priori academic and practitioner literature; and (2) discuss implications for research and practice.

DEFINING INFORMATION AVAILABILITY

Initial research efforts in the area of INFOSEC have focused upon the most needed component: process management. Soon after, access control emerged as a necessary service. “The original motivation for putting protection mechanisms into computer systems was to keep one user’s malice or error from harming other users,” (Lampson, 1971). The reference monitor, which “controlled sharing of system resources” (Anderson, 1972), was quickly adopted as the basis for assuring that system resources were protected (Brinkley & Schell, 1995). The publications of Bell and LaPadula in 1973 established the first mathematical model for specific access classifications that would satisfy a specific security conditions (LaPadula, 1996). The model concentrates on confidentiality (Schneier, 2000). Further research expanded the reference monitor to the trusted computing base (TCB) which has continued as the premise for modern secure or trusted systems (NRC, 1991).

Confidentiality has been the primary goal of INFOSEC, because there has been and continues to be a desire for systems to be “trusted”, thereby only granting access to users who are authorized to receive the requested information (NCSC, 1992). By controlling access to information and preventing unauthorized disclosure, a system has achieved confidentiality (Brinkley & Schell, 1995). In this chapter, we adopt the definitions of availability, confidentiality and integrity shown in Table 1 (Schou, 1996). The objective of information availability is to enable access to authorized information or resources to those who need them (CEC, 1991). Thus, for our purpose, IAV is the ability to make information and related physical and logical resources accessible as needed, when they are needed, and where they are needed. This notion encompasses more than just making sure that systems and related infrastructure is technically adequate and
continuously available, but it also highlights the need to address other often-ignored concerns of IAV such as appropriate policies and procedures, an effective security policy, and the establishment of a workable business continuity plan.

FACTORS IMPACTING INFORMATION AVAILABILITY

It is reasonably well-established in literature and practice that IAV has three first order determinants: Reliability, Accessibility, and Timeliness (Jonsson, 1998). Reliability refers to the degree to which a system performs its purpose for the period of time intended under the operating conditions encountered (Reibman & Veeraraghavan, 1991). For example, a space shuttle’s onboard computer and related applications need to work on tasks without interruption and errors in a consistent way. Users do not want to depend upon a system that cannot be trusted to consistently execute their requests. Since a system cannot be reliable if it is not available and secure, the notions of reliability, availability and information security are intricately linked.

Broadly speaking, accessibility refers to the degree to which a system is usable by as many people as possible without modification and is characterized in terms of the ability of users to have physical access to the system, the nature of users’ interface with the system, and the ability to physically retrieve potentially relevant information (Culnan, 1985). Authentication is a critical element of accessibility and has been approached from technical, conceptual and organizational levels (Siponen & Oinas-Kukkonen, 2007). At the technical level, there are several access control approaches, 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) (Sandhu, 1996). At the conceptual level, Siponen and Oinas-Kukkonen (2007) use the example of Access Matrix (Lampson, 1971) which can be utilized to illustrate which users/processes/security subjects have access to which security objects. At the organizational level, measures to achieve secure access include biometrics, security policy (users’ following security guidelines), applying extrinsic deterrence, and ethical responsibility (“employees are responsible for fulfilling the organizational security mission”) (Siponen and Oinas-Kukkonen, 2007).

Timeliness is the responsiveness of a system or resource to a user request. In fact, traditionally IAV has mostly been measured by the amount of time an information resource is either processing or not (uptime and downtime) (Wood, 1995). Users and organizations alike desire instant response to their requests; without good IAV, that desire may not be adequately met.

Second Order Determinants of Information Availability (IAV)

Within the logical and physical domain, redundancy (Hutt et al., 1995; Jajodia, McCollum, & Ammann, 1999; Parker, 1992) and thorough system backups (Dennning, 1999; Hutt et al., 1995; Parker, 1992), preventative and corrective maintenance (Hutt et al., 1995), and disaster recovery plans (Hutt et al., 1995) increase the availability of IT resources in the event that a threat is realized. The danger in assuming that an information resource (e.g., data file, router or switch, telecommunications pathway, and so on) will be available is that it is forgotten until that resource is unavailable, at which time, the resource must be immediately restored. Researchers have proposed to quantify availability in terms of latency (Tryfonas, Gritzalis, & Kokolakis, 2000), mean time to fail (MTTF) and mean time to restore (MTTR) (Sun & Han, 2001), maximum waiting time (MWT) (Gligor, 1984), finite waiting time (FWT) (Yu & Gligor, 1990), and probabilistic waiting

Table 1. Definitions of the components of information availability from the ISBO Glossary of INFOSEC and INFOSEC Related Terms Vol. 1 (Schou, 1996)

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Timely, reliable access to data and information services for authorized users.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Assurance that information is not disclosed to unauthorized entities or processes.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.</td>
</tr>
</tbody>
</table>
Information Availability

It is reasonably well-established in literature and practice that IAV has three first order determinants: Reliability, Accessibility, and Timeliness (Jonsson, 1998). Reliability refers to the degree to which a system performs its purpose for the period of time intended under the operating conditions encountered (Keltman & Veenaraghavan, 1991). For example, a space shuttle’s onboard computer and related applications need to work on tasks without interruption and errors in a consistent way. Users do not want to depend upon a system that cannot be trusted to consistently execute their requests. Since a system cannot be reliable if it is not available and secure, the notions of reliability, availability, and information security are intrinsically linked.

Broadly speaking, accessibility refers to the degree to which a system is usable by as many people as possible without modification and is characterized in terms of the ability of users to have physical access to the system, the nature of users’ interface with the system, and availability to physically retrieve potentially relevant information (Collins, 1985). Authenticity is a critical element of accessibility and has been approached from technical, conceptual, and organizational levels (Siponen & Oinas-Kukkonen, 2007). At the technical level, there are several access control approaches, 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) (Sandhu, 1996). At the conceptual level, Siponen and Oinas-Kukkonen (2007) use the example of Access Matrix (Lampson, 1971) which can be utilized to illustrate how every (security) subject has access to which security objects. At the organizational level, measures to achieve secure access include biometrics, security policy (users’ following security guidelines), applying extrinsic deterrence, and ethical responsibility (“employees are responsible for fulfilling the organizational security mission”) (Siponen and Oinas-Kukkonen, 2007).

Timeliness is the responsiveness of a system or resource to a user request. In fact, traditionally IAV has mostly been measured by the amount of time an information resource is either processed or available (or downtime) (Wood, 1995). Users and organizations alike desire instant response to their requests; without good IAV, that desire may not be adequately met.

Second Order Determinants of Information Availability (IAV)

Within the logical and physical domain, redundancy (Hutt et al., 1995; Hurdia, McColm, & Aumann, 1999; Parker, 1992) and thorough system backups (Denny, 1991; Hutt et al., 1995; Parker, 1992), preventative and corrective maintenance (Hutt et al., 1995), and disaster recovery plans (Hutt et al., 1995) increase the availability of IT resources in the event that a threat is realized. The danger in assuming that an information resource (e.g., data file, network switch, telecommunications pathway, and so on) will be available is that it is forgotten until that resource is unavailable, at which time, the resource must be immediately restored. Researchers have proposed to quantify availability in terms of latency (Tryfonas, Grkalzis, & Kokolakis, 2010), mean time to fail (MTTF) and mean time to restore (MTTR) (Sun & Han, 2011), maximum waiting time (MWT) (Gillies, 1964), finite waiting time (FWT) (Yu & Gilger, 1990), and probabilistic waiting time (PWt) (Miller, 1992). Each metric assesses the amount of time an information resource is unavailable, but from a different perspective. According to Viles & French (1985), most users expect a “100-100-Web: 100 percent availability for all servers and 100 millisecond latency to every server; “ is to say that users desire fast response to a request. This expectation is nearly impossible to sustain given the numerous threats to availability.

In Figure 1, each block on the far left represents an IAV second order 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 first order attributes of information availability, thereby contributing to the overall availability of the information resource and impacting information security. A discussion of each factor and the impacts it has on the enterprise follows.

Security Policy

An enterprise-wide security policy is the foundation for INFOSEC. It defines how the enterprise will protect its information resources. The security policy establishes the framework for information processing and use of IT devices within an enterprise. According to Dokker (1997), 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 service, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow.

Without a well-developed security policy, the enterprise is ill-prepared to ensure that information resources will be available and that the data is correct. Due to the increased use of information technology, many organizations have established security policies. Most security policies do not address IAV (Hosmer, 1996; NRC, 1991). In fact, authors of policies generally concentrate predominantly on confidentiality concerns. Distributed Denial of Service (DDoS) attacks specifically challenge availability with immediate and potentially lasting effect and relatively little risk to the attacker. In fact, during such an attack, limiting availability may be the countermeasure to best protect the system. If the security policy does not address availability, the correct actions may not be taken in a timely manner, thereby increasing the potential exposure of the IS and the risk of permanent damage to system.

Table 1: Definitions of the components of information availability from the ISO/IEC Glossary of INFOSEC and INFOSEC Related Terms Vol. 1 (Sekou, 1996)

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Timely, reliable access to data and information services for authorized users.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Assurance that information is not disclosed to unauthorized entities or processes.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Condition that exists when data is exchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.</td>
</tr>
</tbody>
</table>

Figure 1: Factors impacting information availability
A system security policy should address who is using the system and the enterprise’s expectations of users. The enterprise can establish guidelines for appropriate use of the provided information resources by identifying the characteristics of an authorized user. Access control mechanisms can be defined and user privileges can be established. Furthermore, all users should understand their privileges and be aware that system monitoring is used to ensure that online actions are being monitored. In addition, users should be told about the consequences for misuse of the provided information resources and the procedures for reporting suspect or odd behavior. A security policy impacts the reliability of a system 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.

Security policy can influence accessibility by setting the access control policies for the system. By doing so, the data contained within the system can be appropriately shared with those users who are authorized, and denied to those who are not. Additionally, physical access to the system is of great concern. Protecting the perimeter (e.g., the campus, the building, the floor on which the computer room resides, or the walls of the computer room) via physical and technological methods is the first line of defense to ensure that authorized users can physically access the system.

**Operational Controls and System Monitoring**

Creating system security policies that address the availability of resources for the enterprise is a major step toward assuring availability, but the policies require enforcement. If the rules, practices, and procedures set forth in the security policy are not enforced, there is less reason to develop them in the first place. 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). Operational controls are created to implement security policy, thereby providing a mechanism for enforcing the security policy. There are several areas where operational controls are implemented. According to Weber (1999), tools are most commonly established for computer and network operations, production systems, data storage, technical support, and any outsourced operations. There are several commercial tools that can aid in establishing the required controls that are not inherent within the hardware or software components. Monitoring system performance provides the stakeholders of the enterprise with measurements of how the information resources are operating (Weber, 1999). Moreover, if security personnel have access to real-time monitoring, they can identify potentially unauthorized activity and implement real-time defensive countermeasures to minimize the system’s exposure to potential loss. According to Hawkins, Yen, and 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, pp. 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. Both functions are important and necessary since monitors cannot investigate every anomaly within the system. To that end, thresholds are defined so that the monitoring application will alarm appropriately. Auditors, on the other hand, analyze automatically generated logs and reports of system activity and can identify further trends that may not immediately impact the
system, but over time could expand and threaten the availability of the system or even the security of the enterprise.

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. 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. The results of a system effectiveness evaluation can be used to determine whether or not there is sufficient availability to meet the demands of the enterprise, as well as provide stakeholders with measurements to evaluate how efficiently the system operates within the organization. While the system effectiveness evaluation is based upon user perceptions, the attitudes of the users will significantly determine the success or failure of the system (Weber, 1995).

Auditing and system effectiveness evaluations provide independent assessment of reliability and timeliness factors within the system. The findings of the auditors can be used to determine whether or not the enterprise has sufficient bandwidth within the infrastructure to support the enterprise's information services and users. These evaluations may show trends of inappropriate or unauthorized behavior on the system that is not being caught through real-time monitoring. If that occurs, policy makers and stakeholders have additional information needed to reevaluate the organizational strategy, security policy, monitoring thresholds, and operational controls. Audits are the check and balance to preserve IAV and the enterprise's confidentiality and integrity.

**Physical Security**

Physical security is a critical prerequisite of IAV. According to the NCES (1998), physical security involves "protecting building sites and equipment from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage". 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). Within the context of availability, physical security is extremely important. 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 computer 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. That request cannot be fulfilled, thereby negatively affecting the productivity of the requestor and any other requestor attempting to contact the unavailable device. Bois (2002) makes the point that "...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. "Without good physical security, the information resources will be attacked, and there will be loss.

Accessibility is impacted if the infrastructure or hardware that facilitates a user's making a request for information and the corresponding response is unavailable. There are several possible reasons why a device may be unavailable, from scheduled maintenance, device or connectivity problems to a malicious attack. Regardless of the reasons behind the unavailability, the end result is the same. Accessibility either is degraded, or completely eliminated for a period of time. Furthermore, the longer the device remains unavailable, the less reliable the system appears to be to the user.

**Backups**

Backups provide a copy of the data, applications, and O/S settings that are stored within a computer to facilitate recovery if necessary (Schou, 1996). 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). Backups do not protect information; other mechanisms should be in place to protect information. If the situation arises where information is lost, then a set of backups will greatly reduce the amount of downtime and cost of loss felt by the organization.
Backups for both the system and user are required to provide maximum restorable capability to the enterprise. The system is most likely stable, therefore system backups need to be made when the system is initially installed, and subsequent system backups need to be created after changes to the system have been made (Murphy, 1996). User files, on the other hand, are modified quite often, making frequent backups, quite possibly daily, necessary (Murphy, 1996). 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 provide a safety net for the enterprise, but the backups must be current, possess integrity, and be available for the system administrator to restore files from the backup media.

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. This process could be quite time consuming. Furthermore, without proper configuration documentation, there is no guarantee that the system will be recreated in exactly the same way.

**Business Continuity**

Business continuity is also known as contingency planning or continuity planning or disaster planning and 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. It also includes planning for backup operations and post-disaster recovery, to ensure the availability of critical resources (Schou, 1996). Yet, only 20% of existing continuity plans are workable when tested (Brunetto & Harris, 2001). In developing continuity plans, the planners need to understand the organization and analyze the dependencies within the enterprise and with vendors who interact with the organization (Kelly, 2000). Once the dependencies are identified, the areas that could suffer loss and the cost of loss should be estimated (Wilson, 1997). Here, the risk assessment and inventory used to develop the enterprise's security policies can be utilized to develop continuity plans. The security policy and business strategy should identify the requirements for continuity and be included as part of the organization's continuity plan.

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” (Facer, 1999) that operations will ever be restored to their pre-event state.

**Redundancy**

Redundancy relates to the ability of an organization to reconstruct an information element to its last state before disruption and having capabilities to connect to its information resources despite disruptions (Jajodia et al., 1999). The goal of redundancy is to minimize unavailability by utilizing redundant capabilities for restoring the capabilities of an organization’s systems (Jajodia et al., 1999). Backing up data provides an extra copy of data, which is restorable in case of failure, sabotage, or natural disaster (Denning, 1999, pp. 384). Furthermore, since failure of any component is possible, the impact of each component being unavailable should be assessed and a redundant equivalent must be available (Hutt et al., 1995). 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).

Based on anecdotal research conducted by the authors, it is clear that redundant systems components are essential to IAV. Our research shows that organizations maintain redundant hardware and software, communications pathways, and data centers (Martin & Khazanchi, 2006). Each company we researched 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).

**CONCLUDING REMARKS**

In this chapter, we have developed a detailed understanding of information availability (IAV) an important attribute of modern information security processes. Based on past literature, we have developed a detailed list of factors that impact information availability and its first order attributes - reliability, accessibility and timeliness.

**Implications for Research**

The technological advances that have enabled businesses to reliably offer applications and services to in-
ternal and external customers through a distributed IT architecture are critical to any business. We believe that given the significance of business requirements upon IAV, there may be justification to separate IAV from information security. Organizations seem to address IAV from a purely operational perspective rather than a broader INFOSEC perspective. Whereas INFOSEC professionals are charged with implementing policies geared toward confidentiality and integrity, business operations personnel have developed infrastructures that support varying levels of IAV. Furthermore, the tools for providing confidentiality and integrity are different from those tools that provide IAV. There also seems to be differing perspectives when discussing confidentiality and integrity and IAV. Therefore, we believe that further empirical research needs to be conducted on the impact of IAV on information security and the antecedents of reliable, accessible, and timely IAV. There is also a need to better understand how IAV models might be adjusted to address the specific needs of smaller businesses.

Implications for Practice

In practice, there is reason to believe that IAV has been an area of great interest. This interest stems from business requirements that are consistent with the business objective of earning profit. Practitioners need to continue to address IAV, but engage researchers in discussions about IAV to better understand its impact on information security. Furthermore, practitioners may consider implementing IAV policies independent of confidentiality and integrity issues in the broader context of information security. By doing so, more focused attention could be devoted to studying how to best provide IAV to meet a business’s IAV requirements. Finally, organizations need to develop practical models for addressing IAV that at a minimum address issues of reliability, accessibility and timeliness of information systems and services in the context of all the factors discussed in this chapter—security policy, redundancy, operational controls and systems monitoring, auditing and system effectiveness, backups, physical security, and business continuity.

REFERENCES


Information Availability


**KEY TERMS**

**Accessibility**: The degree to which a system is usable by as many people as possible without modification and is characterized in terms of the ability of users to have physical access to the system, the nature of users' interface with the system, and the ability to physically retrieve potentially relevant information.

**Auditing**: 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.

**Backup**: Copy of files and programs made to facilitate recovery if necessary.

**Business Continuity Planning**: 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. It also includes planning for backup operations and post-disaster recovery, to ensure the availability of critical resources.

**Information Availability (IAV)**: The ability to make information and related physical and logical resources accessible as needed, when they are needed, and where they are needed.

**Operational Controls**: System rules and guidelines necessary to manage the day-to-day activities that occur within an enterprise's information resources.

**Physical Security**: Protecting building sites and equipment from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage.

**Redundancy**: Having an information element stored redundantly or having the ability to reconstruct an information element (Jajodia, et al., 1999).

**Redundancy**: The ability of an organization to reconstruct an information element to its last state before disruption and having capabilities to connect to its information resources despite disruptions. The goal of redundancy is to minimize unavailability by utilizing redundant capabilities for restoring the capabilities of an organization's systems.

**Reliability**: The degree to which a system performs its purpose for the period of time intended under the operating conditions encountered. **Security Policy**: A documented high-level plan for organization-wide computer and information security.

**Systems Monitoring**: Monitoring system performance provides the stakeholders of the enterprise with measurements of how the information resources are operating and allows security professionals to identify potentially unauthorized activity and implement real-time defensive countermeasures to minimize the system's exposure to potential loss.

**Timeliness**: The responsiveness of a system or resource to a user request. In fact, traditionally information availability has mostly been measured by the amount of time an information resource is either processing or not (uptime and downtime).