PUBLICATION

The Art of Balancing Information Security and Information Sharing

Michael Cartney

December 2001

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman	*Managing Director*
Anthony G. Oettinger	John C. B. LeGates

Michael Cartney, Lieutenant Colonel, USAF, is chief, satellite communications operational plans, policy and procedures, Command Control Systems Directorate, North American Aerospace Defense Command, U.S. Space Command. In his previous assignment as director of the Global Command and Control System for the chairman, Joint Chiefs of Staff, he managed the daily operations and security of over 10,000 networked workstations located across more than 750 sites worldwide. He prepared this report while serving as an Air Force National Defense Fellow with the Program in 1999–2000.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-78-X **P-01-4**

December 2001

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

- Anonymous Startup
- AT&T Corp.
- Australian Telecommunications Users Group
- BellSouth Corp.
- The Boeing Company
- Booz Allen & Hamilton Inc.
- Carvajal S.A. (Colombia)
- Center for Excellence in Education
- CIRCIT at RMIT (Australia)
- Commission of the European Communities
- Critical Path
- CyberMedia Convergence Consulting
- CyraCom International
- DACOM (Korea)
- ETRI (Korea)
- eYak, Inc.
- Fujitsu Research Institute (Japan)
- GNB Technologies
- Grupo Clarin (Argentina)
- Hanaro Telecom Corp. (Korea)
- Hearst Newspapers
- High Acre Systems, Inc.
- Hitachi Research Institute (Japan)
- IBM Corp.
- Intel Corp.
- Korea Telecom
- Lee Enterprises, Inc.
- Lexis-Nexis
- Eli Lilly and Co.
- Lucent Technologies
- John and Mary R. Markle Foundation
- McCann North America
- Microsoft Corp.
- MITRE Corp.
- Motorola, Inc.
- National Security Research, Inc.
- National Telephone Cooperative Assoc.
- NEC Corp. (Japan)
- NEST–Boston
- Nippon Telegraph & Telephone Corp (Japan)
- NMC/Northwestern University
- Research Institute of Telecommunications and Economics (Japan)
- Samara Associates
- Siemens Corp.
- SK Telecom Co. Ltd. (Korea)
- Strategy Assistance Services
- TRW, Inc.
- United States Government:
  - Department of Commerce
    - National Telecommunications and Information Administration
  - Department of Defense
    - Defense Intelligence Agency
    - National Defense University
  - Department of Health and Human Services
    - National Library of Medicine
  - Department of the Treasury
    - Office of the Comptroller of the Currency
  - Federal Communications Commission
  - National Security Agency
  - United States Postal Service
- Upoc
- Verizon

Acknowledgements

The author gratefully acknowledges the following people who reviewed and commented critically on the draft version of this report. Without their consideration, input, and encouragement, this study could not have been completed:

Robert A. Beck, Jr.
Alan D. Campen
James R. Clapper, Jr.
Craig M. Cook
Peter H. Daly
Fred R. Demech, Jr.
Albert J. Edmonds
Seymour E. Goodman
James J. Hearn
David Komar
Martin C. Libicki
R. Thomas Marsh
Peter G. Neumann
LouAnna Notargiacomo
Charles Popper
Richard T. Reynolds
Linda M. Schlipper
H. Gordon Thigpen
Steve Welke
Marilyn Z. Wellons
John L. Woodward

These reviewers and the Program’s Affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor should they be blamed for any errors of fact or interpretation.

I would also like to thank my wife Harriett and my son Byron for their support, and Hong Shik Jung for his friendship and advice while both of us were with the Program.

The views, opinions, and conclusions expressed in this paper are those of the author and should not be construed as an official position of the Department of Defense or any other government agency or department.

Executive Summary

Today’s global, high-tech, information-oriented environment forces all organizations to face the enormous challenge of finding the most appropriate balance between sharing information and securing it against harmful disclosure or potential threats. In the military, security often conflicts with operational effectiveness. In the intelligence community, protecting sources and methods may undermine confidence in an information product. In industry, guarding trade secrets and customer privacy may prevent the introduction of e-commerce innovations. Rapidly growing demands for both information sharing and information security mean that achieving a better balance between information sharing and security (IS&S) has become critical to business survival.

This study suggests ways in which organizations can improve their design and practice of IS&S by using an approach that remains rooted in, and focused on, the practical aspects of *how* (business culture) and *why* (business value) organizations conduct business. It offers an original framework that provides organizations with the tools and concepts they need to identify, define, focus, and address influences on IS&S, including business objectives, stakes and stakeholders, technology, trends, and vulnerabilities. Because the framework identifies business value as the common denominator for measuring expectations, analyzing options, and assessing influences, it can help organizations to balance information security against sharing. It can also enable managers to determine the appropriate level of IS&S effort within the overall business model. Finally, the study outlines an approach to managing IS&S that is both inclusive, in that its scope reflects the potential contribution of information to organizational effectiveness, and specific, in that it goes beyond attractive theories to specific, business-related measures and directly incorporates IS&S into the overall process of managing an enterprise.

The framework does not seek to prescribe solutions regarding IS&S. Instead, it allows organizations to ask and examine key questions that many approaches to IS&S often leave unanswered or incomplete. Because the study defines the term *business* in a generic sense, to mean *getting something accomplished*, and *operations* and *operational aspects* to mean *the activities required to accomplish something*, the resulting framework applies in all settings—from small startup companies to the U.S. government. By inserting its own specific terminology, any organization can customize the tools provided in this study to identify the most appropriate balance between sharing and security in its own setting.

Contents

Illustrations

Figures

Tables

Chapter One

The Framework at a Glance

Information sharing is like breathing—you have to do it to survive. How well you do it affects your strength, but if you overdo it you will pass out. And you have to be careful what you breathe.

Gen. Robert T. Marsh, USAF (Retired),
Chairman, President's Commission on Critical
Infrastructure Protection[1]

As we wire the world and our lives, we add new vulnerabilities that will be exploited. As a country and a society, we have no desire to stop, or even slow down, the dramatic technological improvements that the information revolution offers. Nonetheless, as we incorporate new systems into our lives and as we become increasingly dependent upon them, we must be prepared to protect ourselves.

Project Air Force, 1999[2]

Balancing the need to share information against the need to protect it is an age-old dilemma facing the military, the intelligence community, and industry. In the military, maintaining operational security (OPSEC), which keeps antagonists from learning the details of a military mission, often conflicts with effectiveness. In the intelligence community, protecting intelligence sources and methods may undermine confidence in the information provided. In industry, guarding trade secrets and customers' privacy may prevent the introduction of innovations in electronic commerce, or "e-commerce."

When is an information environment so open that openness jeopardizes vital interests? To what extent should security be allowed to impede effectiveness? Who are the stakeholders, and what are the stakes? What are the tradeoffs? Where does technology fit in? How can an organization—whether a branch of the U.S. government or a private corporation—determine the best balance between sharing and protecting information? Every organization faces the enormous challenges embodied in these questions. Today's global, high-tech, information-oriented

[1] Interview by the author with Gen. Robert T. Marsh, Washington, D.C.: The Pentagon, Dec. 16, 1999.

[2] Zalmay M. Khalilzad, "Defense in a Wired World: Protection, Deterrence, and Prevention," in *Strategic Appraisal: The Changing Role of Information in Warfare*, edited by Zalmay M. Khalizad and John P. White (Santa Monica, Calif.: The RAND Corp., 1999), 403' also [On-line]. URL: http://www.rand.org/publications/MR/MR1016/ (Accessed Feb. 27, 2001.) The mission of Project Air Force is "to conduct an integrated program of objective analysis on issues of enduring concern to Air Force leaders." The RAND Corp., "About Project Air Force," [On-line]. URL: http://www.rand.org/paf/about.html (Accessed Feb. 27, 2001.)

environment, with its constantly increasing demands to share as well as to protect information, amplifies their complexity and importance.

This report offers a framework for an approach to information sharing and security (IS&S) that organizations can develop to ask and answer these difficult questions for themselves, a task that involves weighing crucial but often conflicting requirements. It focuses only indirectly on the questions. Instead, organizations can adapt the framework to their own needs and to their particular individual and cultural identity. The framework provides ideas and tools for examining related questions such as the following:

- Why share information?
- Why secure (that is, protect) information?
- What influences decisions when there is business value in sharing information easily as well as business value in restricting the free flow of the information?
- How much sharing is too much sharing?
- How much security is too much security?

The proposed framework uses the term *business* in a generic sense, to mean *getting something accomplished*, and *operations* and *operational aspects* to mean *the activities required to accomplish something.* It therefore becomes applicable to all types of organizations—from small, startup information-technology companies considering what to tell potential strategic partners to the U.S. government deciding what military intelligence information to share with allies and potential coalition partners. By plugging in specific terminology, any organization can tailor the framework to make it relevant to its particular business—whether that business be diplomacy, manufacturing, finance (including sales and e-commerce), education, consulting, or any other type of business activity.

The original framework developed in this project, and described here, offers insights into how to identify and analyze the important influences that shape an effective approach to IS&S, including the organization’s culture, objectives, stakes and stakeholders, technology, trends, and vulnerabilities (see **Figure 1-1**). By providing organizations with the tools and concepts needed to identify, define, focus, and address these influences, it can enable them to practice the art of balancing information sharing against information security. Organizations can use the framework to identify and then develop IS&S objectives and to make informed decisions about ways to implement a viable IS&S strategy (see **Figure 1-2**).

Most important, this report investigates the benefits of using a framework for IS&S that remains rooted in, and focused on, the operational aspects of *how* (culture) and *why* (value) organizations do business. It does so by:

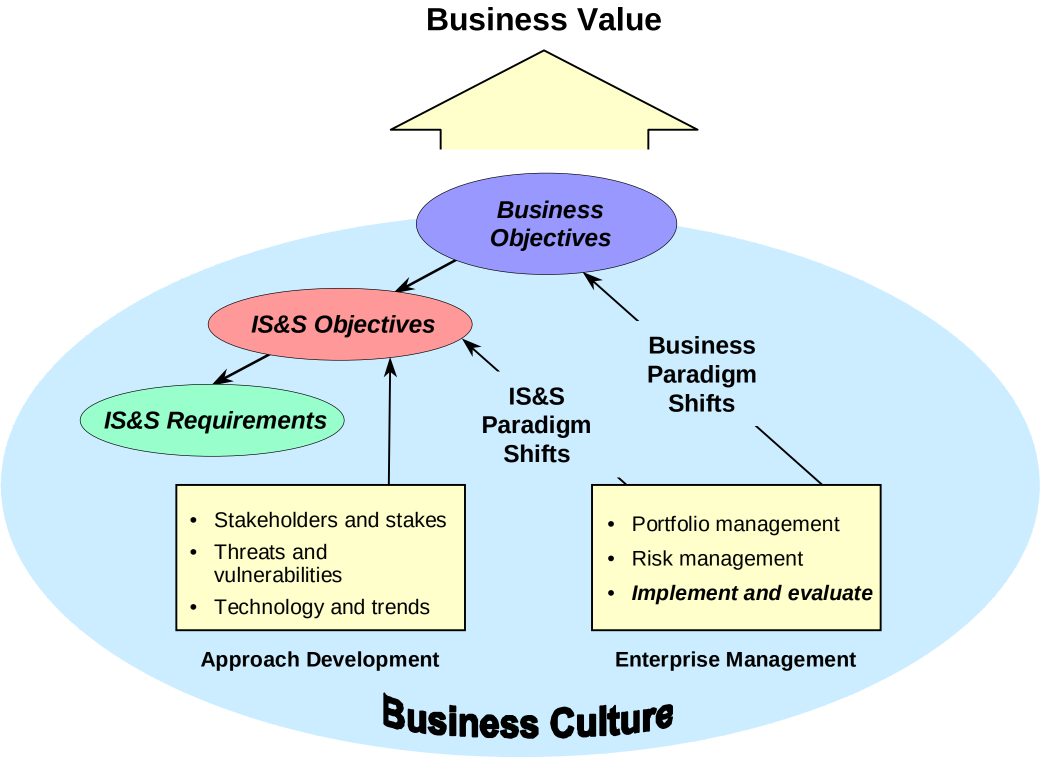


Figure 1-1

Influences on an Approach to IS&S

- linking the objectives of IS&S to overall business objectives and to the way organizations manage these objectives on the basis of business value;

- recognizing the essential role of business culture;

- developing an IS&S approach by examining and weighing influences and options based upon business value;

- emphasizing organization-wide understanding of IS&S to promote support and participation in implementing the approach chosen; and

- evaluating and managing IS&S efforts from the perspective of achieving overall business goals.

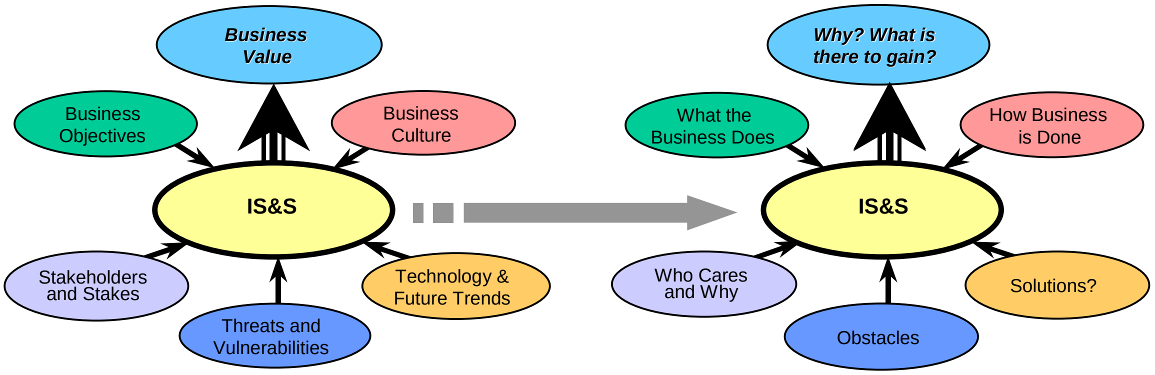


Figure 1-2
Model for Developing an Approach to IS&S

By using business value as the common denominator for analyzing and assessing influences, the framework helps organizations to balance security against sharing and enables them to position security and sharing efforts within their overall business model.

Business culture pervades all aspects of IS&S. Even the wording of a question or task implies whether the organization primarily shares or secures information; that is, if its approach to sharing and security is permissive or restrictive. Each organization's particular culture determines which approach is "correct" for that organization. The report suggests that each organization can develop a usable and appropriate approach by recognizing the context of business culture and its impact on every aspect of the approach to IS&S.[3]

Throughout, two examples illustrate how the proposed framework could apply in different settings and highlight certain aspects of how it might be used. Because of the author's background and expertise, the focus is on automated data processing (ADP) systems, but both the framework and the concepts discussed can apply to government and business information systems in general. The two short case studies are neither exhaustive nor conclusive about specific organizations and their IS&S approaches. However, within a narrow focus and within the constraints of a discussion at the unclassified level, the description of each example is complete and accurate. Senior leaders representing key stakeholders from both organizations used in the examples have reviewed, contributed to, and commented on the report. The **Appendix** provides additional information on both settings.

[3] See Charles Popper, *A Holistic Framework for IT Governance* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-1, January 2000), 1, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/popper\popper-p00-1.pdf

1.1 Presidential Decision Directives 62 and 63

Concern over possible information attacks against the infrastructure of the United States—including not only government entities but also such essential privately managed services as the nation's electric power grid and its banking system—prompted the Clinton administration to issue several directives aimed at orchestrating potential responses. Presidential Decision Directive (PDD) 62 and PDD 63 indicate how the challenges posed by information warfare, cyber terrorism, and cyber crime blur the boundaries between the roles and responsibilities of law enforcement agencies, the intelligence community, the departments of State and Defense, state government, local government, and the private sector. To protect the National Information Infrastructure (NII),[4] PDD 63 mandates the establishment of a secure network that enables participating entities of government and business to share information related to detecting, warning of, and thwarting attack; investigating incidents and determining appropriate action; and promoting rapid response and recovery.

The PDD mandate and its implications serve as an example of a "clean sheet" environment. Because work in this area is just getting under way and results are not yet available, this report focuses on the PDDs' objectives and requirements. The example of the PDD setting helps to illustrate some of the underlying issues that arise when information must be shared among a range of vastly different organizations. How does the picture change when one organization's approach to network security must account for another, independent organization's approach to security? The issue is further complicated by the differences in the missions of the organizations, the uses to which they put the information, and their disparate approaches to security. The question, "Is there a feasible approach to connecting the major players and to sharing key information electronically?" provides the basis for the discussion of the pertinent issues in IS&S.

1.2 The Joint Command and Control Infrastructure

As requirements for information and the volume of data grow, as mission response times are shortened, and as "cyber threats" and "information targets" expand, the ability of the U.S. military to implement its concepts for twenty-first century command and control may depend on its ability to balance information security and information sharing. In general, the challenge facing the Global Command and Control System (GCCS), which connects military units around the world via a high-speed, secure network, relates to different levels of confidentiality in organizations that have existed for some time. Unlike PDDs 62 and 63, the GCCS has an established environment, culture, objective, and de facto approach to sharing and security. The challenge facing the GCCS stems from the growing need to share more information at various levels of confidentiality more efficiently within the organization.

[4] The term NII generally refers to the group of services that provide digital communications for the United States and therefore includes infrastructure provided by both private organizations and the federal government.

The Joint Staff, which manages the GCCS, is investigating new business practices that require more and faster access to information. Will its present approach to security still work? To illustrate the framework, this report limits the scope of the question to, "Does the current ADP approach of having separate local area networks (LANs) for separate levels of confidentiality meet the need of the Department of Defense (DOD) need for a common command and control system?" It examines the current GCCS/Global Combat Support System (GCSS) approach of maintaining information at different security classification levels on disjoint, separate networks rather than connecting or bridging the networks and employing a scheme for labeling protected data. The discussion is limited to objectives, stakeholders, stakes, trends, and assessments of whether the current electronic data classification will support the command and control objectives of future warfighters. (See the **Appendix** for detail on the topic of multiple security levels.)

1.3 Scope

This report does not recommend a particular approach to security or suggest directions for either the GCCS or the NII. Instead, it proposes a framework in which these entities, and others, can make and implement decisions about their own IS&S approaches and directions. It draws upon the examples of the PDDs and the GCCS, because these information systems have three features common to all information systems in which sharing and security must be balanced:

- information at differing levels of confidentiality,
- increasing reliance on the quality and quantity of information to be shared, and
- existing and potential threats to that information.

These characteristics make the issues generally applicable to any public or private organization.

To frame the discussion, **Chapter Two** defines and explains the terminology used here. **Chapter Three** examines reasons for sharing or securing information, and **Chapter Four** analyzes IS&S objectives in terms of business value. **Chapter Five** explores the influences that determine an effective approach to IS&S, including stakeholders and their stakes, threats and vulnerabilities, and the technologies and trends related to IS&S that affect the business environment. **Chapter Six** presents some ideas about incorporating IS&S into the overall management processes of an organization, and **Chapter Seven** summarizes the major findings.

Approaches to sharing and securing information, of course, are not worth pursuing unless they support a worthwhile product. This report assumes that organizations have already assessed their information products (current and planned) and concluded that the business value of these products justifies some level of cost for sharing or securing them. Although the report touches briefly on ways in which the proposed framework might contribute to that decision, its primary focus is on ways for organizations to identify feasible and effective IS&S approaches in the context of their own goals and objectives.

Chapter Two

Talking “Eye to Eye”: Creating a Shared Language Framework

The ability to communicate clearly and concisely about a topic depends on the linguistic dexterity and competence of both the presenter and the audience. Effective communication is critical to the success of any effort. Before an organization can embark on a useful examination of IS&S, the parties involved will need a common understanding of several words and phrases that denote certain concepts. Section **2.1** provides the foundation for such an understanding to give organizations the basic tools to remove ambiguity from discussions of information and information products. A common language remains a starting point. Only continued dialogue and vigilance will ensure clear and effective communication.

No distinction is made here among data, information, and knowledge, partly because any distinction will always be subjective. One person’s knowledge is often another’s information, and may only be a data point to a third. What a front-line worker may “know” is often information or even just data to corporate staff, yet the substance is the same. Philosophers as far back as Aristotle and Plato have debated these definitions, but no lasting consensus has emerged.[1] The focus of this report is on helping organizations decide what to share or protect, and how to do so, not on the content that is shared or protected.

2.1 What Is an IS&S Approach?

An *IS&S approach* consists of a set of IS&S objectives together with a plan for influencing the organization’s information process, as well as the substance and bundling of information products to accomplish the objectives. An *IS&S objective* is a measurable concept whose full or partial accomplishment determines whether or not an organization achieves a given goal.

Business goals are defined here as the aims of the organization; one or more *business objectives*, if met, will achieve the goals. Thus, *goals* tend to be abstract, while *objectives* are specific and quantifiable. IS&S objectives focus on enabling the organization to reach its objectives and are therefore to be phrased in a positive way. Once the objectives become clear, the organization’s overall stakes in IS&S become evident (for definitions of the terms *information process*, *substance*, and *format bundling*, see section **2.2**).

[1] William H. Read, *Knowledge As a Strategic Business Resource* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-99-1, January 1999), 1, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/read\read-p99-1.pdf

An IS&S approach addresses the key components of *awareness*, *training*, *technology*, *policies*, and *procedures*:

- **Awareness**. An organization's assurance that its most important resource—its staff members—understand what information must be secured and why, and also understand the consequences to the organization and the individual of releasing or protecting information.
- **Training**. A program that teaches people how to secure information.
- **Technology**. The use of automation and other tools to share or secure information.
- **Policies**. Clear, concise statements describing the organization's philosophy and approach to information security.
- **Procedures**. Step-by-step instructions for how to perform security tasks and actions.

2.2 What Constitutes an Information Product?

Information is a basic resource, like energy and materials.
Without materials there is nothing; without energy nothing works;
and without information, nothing makes sense.[2]
Anthony G. Oettinger

In discussing information, the ability to describe the particular aspect of an information product that is of concern makes it possible to paint the desired picture clearly. According to one portrayal of the elements of information products,

> Media may come and media may go, but the basic substance, format and process building blocks stay on as the tools of choice for expressing change. Thinking explicitly in terms of these building blocks helps avoid entrapment in bundles tied by the exercise of discretion appropriate to the moment in history but whose time may be long gone.[3]

Information products and services are built from a triad of substance, format, and process.[4]

- **Substance** represents the content of the information in a very broad sense: "Data, knowledge, and the rest are kinds of information substance—of greater or lesser value, of greater or lesser cost. Within the broader context of information resources, the concept of substance brings out the essence of information: the thing that either a picture or a thousand

[2] Anthony G. Oettinger, "Building Blocks and Bursting Bundles," in *Mastering the Changing Information World*, edited by Martin L. Ernst (Norwood, N.J.: Ablex Publishing Corp., 1993), 21.

[3] Ibid., 49.

[4] Martin L. Ernst, "The Information Evolution," in *Mastering the Changing Information World*, 7.

words conveys, the thing evoked when speaking of matters that are substantive rather than formal or procedural."[5]

- **Format** concerns the physical materials and/or signals in which substance is, or can be, embodied for subsequent manufacturing and distribution, as well as for eventual absorption and interpretation.

- **Process** includes all the energy-consuming means used to create and manipulate substance, embody it in a format, and deliver it to a user."[6] Frederick Brooks conceptualizes processes as having three components: the architecture (plan), the implementation (concept for carrying out the plan), and the realization (a specific instantiation of the implementation).[7]

  - *Architecture* is the conceptual strategy for achieving the business objectives.[8] People talk about business architectures, information architectures, security architectures, and even information technology architectures as separate, though often overlapping, entities.

  - *Implementation* encompasses the rules and detailed guidance outlining the approach to embodying the architecture in a product.

  - *Realization* is the actual application of materials, energy, and information that represents an instantiation of the implementation.

- **Bundling** is the combination of process, format, and substance that becomes an information product (see **Table 2-1**). Often the name of the product identifies the bundling and provides insight—for example, television news versus newspaper. The terms themselves indicate that even though the substance may be the same, the process and format are different. Which bundling is chosen for any particular piece or category of information product, and how that bundling evolves or is replaced, will be based on four key elements: purpose or use of the information; value of the information; information quality requirements; and environmental considerations.9

These concepts are discussed in **Chapter Five**.

2.3 What Is Information Sharing?

Individuals and organizations share information in a variety of ways and for a variety of reasons. Here the term *information sharing*, as opposed to *information exchange*, is used because *exchange* implies a two-way flow. Information can be shared unintentionally as well as

[5] Ibid., 26.

[6] Ernst, "The Information Evolution," in *Mastering the Changing Information World*, 7.

[7] Gerrit A. Blaauw and Frederick P. Brooks, Jr., *Computer Architecture: Concepts and Evolution* (Reading, Mass.: Addison-Wesley, 1997), 3–31; and Bernard Cohen, *Howard Aiken: Portrait of a Computer Pioneer* (Cambridge, Mass.: The MIT Press, 1999), 144.

[8] Anthony G. Oettinger, in a presentation at Harvard University, October 1999.

[9] Oettinger, "Building Blocks and Bursting Bundles," in *Mastering the Changing Information World*, 33.

intentionally. Here information sharing refers to information shared electronically, orally, as hard copy, and visually.

Table 2-1

Elements and Components of an Information Product

Element	Component	Bundling 1 Feline Stories	Bundling 2: Classified Letter
Substance		Story about Garfield	SECRET letter from Joint Staff J-6
Format	Symbol	Representation of a feline	"SECRET" label on the top of the document
	Pattern	English word "CAT"	Word "SECRET" on the top center of the page
	Token	Transistor in "on" state	Smudge of ink on paper
Process	Architecture	Collection of stories about famous felines stored where anyone has access to them	Classification system that prevents sensitive U.S. government information from falling into wrong hands
	Implementation	Web site with copies of all such stories found in libraries	Classification levels of TOP SECRET, SECRET, and UNCLASSIFIED, with special releasability constraints, handling, protection, and information labeling procedures and processes
	Realization	URL: http://www.cats.com, which contains all scanned stories on cats from the Watertown Public Library on a SUN SPARC Web server in a Sybase database management system (DBMS)	System of labeling, handling, storing, protecting, and discarding U.S. government paper documents

2.4 What Is Information Security?

> *Business is war. Survival of the fittest. In order to survive in today's cutthroat business environment, we must be properly armed. One of the most important arrows in the businessman's quiver is accurate knowledge of his competitors and business environment… Possessing accurate intelligence is like having a flashlight in the dark. It won't remove any obstacles in your path, but it will illuminate them so you don't stumble.*[10]

The importance of protecting information is rising as quickly as the use of information. But what does *information security* mean? The terms used by many different players muddy and undermine efforts to protect information. Industry often uses the terms confidentiality, integrity, availability, and nonrepudiation.[11] Within the DOD, warfighters use OPSEC, the National

[10] R. W. Rustmann, Jr., "The Craft of 'Business Intelligence,'" *Intelligencer* (August 1999), 4.

[11] LouAnna Notargiacomo, Trusted Computer Solutions, Inc., personal communication to author, Dec. 18, 2000.

Security Agency (NSA) and ADP personnel ponder computer security (COMPSEC), and communications technicians strive to improve communications security (COMSEC), even though all these terms have officially merged into one common term, information security (INFOSEC). At the same time, *information assurance* is touted as the protector of the quality and availability of information, while *information protection* and *defensive information warfare* appear to refer to steps taken to limit the effectiveness and impact of threats.

The variety of terms and definitions stems from the different vantage points on problems affecting information security or communications. These differences strengthen the need to make certain that various entities have a common language framework. Most experts agree that information security involves steps taken to ensure that the organization is not prevented from realizing the purpose, value, and quality of its information while also ensuring that an organization’s business advantages are not compromised by external efforts to collect information. Information security is generally discussed in terms of threats, vulnerabilities, and mitigating actions. (See **Chapter Five** for an explanation of these concepts.)

Chapter Three

Why Share? Why Secure?

Is business in the information age about the free and open exchange of information, or is it about the rapid, seamless, and controlled use of information by organizations? Certain entities must be prevented from accessing, manipulating, or interfering with the organization's flows of information. Why? Why is information shared? Why is it secured? What is the motivation for either?

Specific answers usually point to one general answer: "Because it is good for business." Organizations share information because it brings them direct or indirect benefit. Sometimes the benefit of sharing stems from the value of the information, sometimes simply from the act of sharing. By contrast, organizations secure (or withhold) information because some legal, political, or operational advantage results from doing so. Would they expend precious resources on these activities otherwise?

The business value of information depends on the culture of the particular organization. Whatever process the organization uses for IS&S, the goal is always business value, and the process takes place against the backdrop of the business culture (see **Figure 1-1**). Consequently, one of the first steps in developing an approach to IS&S is to define what there is to gain, what the business value is, or, succinctly, the Why.

3.1 Business Value—A Common Thread

The underlying motive for all business activities is to gain or retain business value. Not only is this common motivation essential to identifying, clarifying, and focusing an analysis of influences on IS&S, but it also provides a useful means to compare the effects of different influences accurately.

Unfortunately, no standard definition of *business value* exists. For one type of organization, business value may be as straightforward as improving cash flow and the efficiency and effectiveness of operations; for another it may be as complicated as promoting strategic international relationships. The meaning will depend on the particular organization, its business objectives, and the specific questions or circumstances that it must address at any given time. Understanding the premise that business value is the common thread across influences is crucial.

Decisions may also be based on the value of information, but that raises certain problems. First, as for business value, there is no standard definition of *information value*, yet an organization must ultimately express the value of information in terms of a business value for it to be meaningful. Because business value is broader than information value, different IS&S options or aspects may result from the same or equal information value but from different business values. Although defining and estimating the value of information may help an organization to understand individual elements of various assessments, such as which information products are worth protecting, using this value as the common thread may diminish the quality of the overall analysis.

Second, in addition to enabling comparisons, using business value as the fundamental criterion for decisions about IS&S offers other advantages, such as helping to focus the identification and analysis of influences on activities with the greatest impact on accomplishing business objectives. Another benefit is that an analysis based on business value can spur advocates of IS&S to develop case studies to show advantages, returns on investment, and cost/benefit analyses, along with less tangible aspects, such as customer confidence, reputation, and long-term effects. More important, discussing influences in business terms can help upper management to understand the impact of IS&S on and its importance to an organization.

As an example, antivirus software may be described in terms of business value as an inexpensive and effective way to avoid losing business days to a highly likely near-term threat that could interrupt all operations supported by computer systems (95 percent of a corporation). Antivirus software thus has a 100:1 estimated return on investment ratio. In technical terms, antivirus software can be described as an inexpensive and effective tool to detect and remedy malicious software capable of corrupting databases, interrupting e-mail, and even causing whole computer systems to crash. Which description would upper management be more likely to understand, support, and fund?

The characterization of business value in the context of the PDDs (section **1.1**) is far more complex. Reaching agreement on a definition of business value in a diverse environment that includes federal, state, and local government agencies and private industry would be a major achievement. As the discussion of stakeholders and culture will show (see section **5.1**), these parties have very different views of what is important and of what each is trying to achieve. Even such a generic specification of business value as “gaining or maintaining business opportunities while increasing information sharing and maintaining or increasing information security” may not be one on which all parties might agree. Phrases such as “business opportunities” may mean one thing to one government entity, something entirely different to another, and something different yet to industry. If government wants industry to participate, will it need to formulate goals in terms that accentuate the value to industry and to the voting citizens of the United States, rather than in terms that emphasize benefits to government? Are there advantages to doing so, and would this force government to change the way it thinks, plans, and discusses a particular topic? Perhaps such a formulation would make the initiatives launched by the PDDs less open to criticism such as that of Peter Daly:

> PDD 63 recommends the creation of an elaborate, government-led, public-private partnership structure that would depend heavily on intrasector

> information exchange and centralized government decisionmaking on risk and response. Although the commission's report and the resulting PDD focus on new paradigms and new ways to manage risk, both the commission's recommendations and the requirements of the PDD relate almost exclusively to vestigial concepts of defending the shores and apprehending criminals.[1]

For the GCCS, the chairman of the Joint Chiefs of Staff (JCS) defines business value as moving the military toward "a joint force—persuasive in peace, decisive in war, and preeminent in any form of combat."[2] Specific to the GCCS, the Joint Staff's director for command, control, communications, and computer systems, and the director's four service counterparts, define business value as something that "brings to the warrior an accurate and complete picture of the battle space, timely and detailed mission objectives, and the clearest view of their targets."[3] These criteria are used here in the discussions of the GCCS.

3.2 The Relationship Between Business Culture and Approaches to IS&S

Information security will only pay off if it is designed and managed with the recognition that it must be based upon the culture and politics of the enterprises it is intended to support.[4]

IS&S affects nearly every aspect of an organization. Accordingly, the business *culture*—that is, how an organization works—can affect every aspect of IS&S. When examining the business culture, understanding *why* an organization works as it does is as important as understanding *how* it works. An approach sound in every other respect may be unusable or untenable within a particular organization if it does not take the business culture into account. For instance, the U.S. military installed secure telephone technology to increase security during operations. In peacetime, the rate of use of the secure phone was relatively high. At the start of the next major military operation, however, when the importance of security increased, use of the secure features of the phone dropped significantly.[5] Whether the reduction was intentional, due to perceived time

[1] Peter H. Daly, *Soldiers, Constables, Bankers, and Merchants: Managing National Security Risks in the Cyber Era* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-3, June 2000), 30–31, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/daly\daly-p00-3.pdf

[2] Chairman, Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: Office of the Chairman, Joint Chiefs of Staff, n.d.), 2, [On-line]. URL: http://www.dtic.mil/jv2010/jv2010.pdf (Accessed Dec. 7, 1999.)

[3] Director, The Joint Staff, *C^{4}I for the Warrior* (Washington, D.C.: Office of the Director, The Joint Staff, Command, Control, Communications, and Computer Systems, JCS/J6I, January 1998), 1.

[4] Statement adapted from M. Shrage, "The Real Problem with Computers," *Harvard Business Review* (September–October 1997), 178–188; quoted in Charles Popper, *A Holistic Framework for IT Governance* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-1, January 2000), 1, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/popper\popper-p00-1.pdf

[5] Interview by the author with James J. Hearn, Deputy Director for Information Systems Security, NSA, 1988–94, Dec. 13, 1999.

constraints, or unintentional, this approach to security did not fit into the military's operational culture and was therefore bypassed.

Business culture pervades every organization and its tasks. Even the wording of an IS&S task or question offers an opportunity to reflect the organization's objectives, philosophy, and direction. Is its approach to sharing and security permissive or restrictive? Will the IS&S effort focus on determining what information to share or on identifying the best way to protect the organization's information environment? Will the propensity be toward sharing or toward withholding information? Is the goal to emphasize or de-emphasize security? The difference can be as minor as asking what information *can* be shared versus what information *must* be shared. In a permissive information-sharing environment, *information is shared unless there is a reason not to do so*; in a restrictive environment, *information is shared only when there is a reason to do so*. In a permissive security environment, the default is not to secure information; in a restrictive environment, the default is to secure it. The correct IS&S formulation for a particular business will be a dynamic of the organization's culture. Realistically, it will reflect compromises between an ideal approach and what the organization can afford. The technology exists to implement almost any approach, but organizations will need to make tradeoffs that affect processing speed, throughput, and other factors.

The basic questions about IS&S fall into two categories: (1) those to determine what should be shared and (2) those to determine the best route for security.[6] Although closely related and interdependent, these categories can present vastly different problems. If an organization tries to address both aspects of IS&S in a single question or tasking, it may find it has set itself an overwhelmingly complex job. The complexity derives from differences in the objectives of sharing and security as well from differences among the stakeholders and stakes involved. The motivation for sharing information is to add value, while the motive for security is to avoid losses. The objective of sharing is to maximize the value of information to the organization by disseminating the information, while the objective of security is to minimize liability by addressing threats and vulnerabilities to the information and therefore protecting and safeguarding it.

As a rule, beginning by addressing which information to share provides a useful structure for determining how best to secure the information environment. Few people will argue that knowing what is being shared can determine how to secure it. Because other things will be shared only if they can be shared safely, dependence also flows in the other direction. What is important is to ensure that the questions posed truly reflect the aspect of IS&S addressed.

Just as the IS&S objectives and criteria for success reflect business culture, any change to a cultural aspect of the organization to accommodate a new approach to IS&S may require

[6] Some call the processes involved *information management*—another term whose meaning varies so widely that it is not applied here.

additional steps to take those cultural shifts into account. Linking an IS&S approach to the organization’s culture and environment increases the likelihood that the approach will make sense to the people involved, will be truly relevant to their jobs, and will add value to their work.

3.3 Illustrations

The role of business culture is very different in the settings of the two examples (sections **1.1** and **1.2**). In the PDD setting, the cultures of the various government entities and private corporations vary greatly, with different approaches and philosophies about security, and most relationships have not yet been defined or established. By contrast, military culture, which shapes the GCCS environment, is relatively homogeneous, and approaches to security and information-sharing relationships are established and often of long standing. In both settings, however, highlighting cultural considerations (see **Tables 3-1** and **3-2**) yields benefits.

PDDs 62 and 63 call for federal entities, in particular the DOD and the intelligence communities, to share information with each other, with national, state, and local law enforcement, and with industry. The debate that resulted after the President’s Commission on Critical Infrastructure Protection (PCCIP) released its findings regarding vulnerability to information attacks illustrated the cultural differences of the participating entities. The military views steps to prevent revealing U.S. vulnerabilities as logical and necessary and therefore supported making the findings a classified document. The private sector (industry) views such steps as comparable to taking a car to a mechanic and having the mechanic’s shop tell you the car desperately needs repair without telling you what is wrong, while also saying that the shop will not fix the car—but if you want to fix it, the mechanic might help you to remedy whatever problems you find!

Table 3-1 highlights the differences in approaches to security, uses of information, and methods of collecting information, and in the motivations, interests, and goals of the entities involved in infrastructure protection. In contrast to that wealth of differences, the GCCS is regarded here as a single cultural environment. Although, in general, the DOD is a permissive environment for sharing and security, because the GCCS deals with classified environments, the DOD’s default is irrelevant. What is important is the attempt to identify key enablers and obstacles within the GCCS culture that affect its approach to sharing and security. Section **1.2** and **Table 3-2** present some of the cultural disparities that arise, for example, from the approach of maintaining separate LANs for separate security classifications.

Table 3-1

Cultural Highlights of PDD Participants

Entity	Sharing and Security Environment: Defaults*	Cultural Highlights
Federal Government (Civilian agencies: Dept. of Commerce, Dept. of State)	Share information Not to secure information	Focus: National interest Public confidence paramount to success Criterion for action: Protection of nation and way of life as a whole
Department of Defense	Share information Not to secure information Secure vulnerability information	Focus: National security Jurisdiction: Outside United States only Security requirements established in statute, policy, and doctrine Public confidence paramount to success Criterion for action: Protection of nation and way of life as a whole
National Intelligence Agencies	Not to share information; disseminate information based upon need to know Secure information	Focus: National security Jurisdiction: Outside United States only By statute, highly protective of sources and methods Public confidence paramount to success Motive for action: Provision of strategic and tactical decision support to President, Secretary of Defense, and National Security Advisor
National Law Enforcement	Not to share information Protect information	Focus: Capture and conviction of federal criminals Jurisdiction: Federal and international only (statutes and area) Motive for action: Perceived violation of federal laws
State Law Enforcement	Not to share information Protect information	Focus: Capture and conviction of federal criminals Jurisdiction: Within state only (statutes and area) Security approaches and emphasis controlled by individual states Motive for action: Perceived violation of state laws
Local Law Enforcement	Not to share information Protect information	Focus: Capture and conviction of federal criminals Jurisdiction: Local only (statutes and area) Security approaches and emphasis controlled by individual departments Motive for action: Perceived violation of local laws and ordinances
Industry (banking, communications, energy, transportation)	Not to share information Protect information	Focus: Business value National and international interests Customer confidence paramount Security approaches and emphasis controlled by individual corporations Does not inherently trust government with data Motive for action: Profits versus losses

*Internal and external.

Table 3-2

Cultural Highlights of the GCCS Communications and Computer Environment

Entity	Sharing and Security Environment	Cultural Highlights
Warfighters	Information spread across several computer systems at varying security levels. Voice, hard copy, images, and signal data often handled simultaneously Established policies, procedures, and guidelines for securing and sharing information	Primary producers and consumers of information In peacetime, heavy reliance and close adherence to security policies, procedures, and guidance In war or times of crisis, security constraints may be temporarily outweighed by mission requirements Traditionally, senior management minimally involved in security environment decisions. Heavy reliance on technical and security communities to establish, monitor, and maintain the security environment Often see security as a cost of doing business, not as a business enabler Deployed warfighter depends mainly on SECRET and UNCLASSIFIED access
Intelligence Community	Established and strong adherence to policies, procedures, and guidelines for securing and sharing intelligence information. Secure is default	Role is to develop and provide intelligence information Sees security as paramount to mission success, particularly when it pertains to protection of sources and methods Senior management involvement in security environment Analysts operate predominantly in compartmented-mode security environment
Information Infrastructure Support Personnel	Established and strong adherence to policies, procedures, and guidelines for managing and maintaining information infrastructure and technical ADP security posture	Roles are to provide information infrastructure; serve as custodians for information on that infrastructure; and provide technical expertise Overall responsibility for security of communications and computer systems
National Security Agency/ Central Security Service (NSA/CSS)*	Established and strong adherence to policies, procedures, and guidelines for securing and sharing intelligence information Secure is default	Roles are to provide foreign intelligence information and computer security expertise to DOD; serve as security experts, providing threat and vulnerability information as well as monitoring and assessing security posture of information infrastructure

*Source: National Security Agency. Information consolidated from material available on-line at URL http://www.nsa.gov, including articles include the National Cryptology Strategy for the 21st Century, the NSA Mission, About NSA, and NSA FAQ (Accessed March 10, 2000.)

Chapter Four

IS&S Objectives

The relationship of business objectives to IS&S objectives—
a holistic approach to IS&S.…We are not in the business of protecting
information. We only protect information insofar as it supports the
business needs and requirements of our company.[1]

Balancing IS&S involves three basic tasks:

- determining the purpose of IS&S in the organization (that is, determining the objectives),
- developing an approach, and
- assessing, managing, and adapting to the effects of that approach.

Rather than present the processes and procedures to accomplish these tasks, this report provides the ideas and insights an organization needs to develop to adjust and refine processes already in place and thereby focus those processes on overall business operation (see **Figure 4-1**).

Most organizations initiate an approach to IS&S by establishing objectives based on what the organization wants to accomplish and what results it expects. The requirements for IS&S may be rooted in operations, politics, or law; fulfilling them costs money and consumes resources; and the requirements will affect nearly all aspects of an organization—its people, processes, procedures, technology, and partners. Given this background, what is the basis for developing the organization's IS&S objectives? Typically, the organization's business strategy provides the context for the main value-adding activities and strategies that the IS&S approach is intended to enhance.[2]

In some organizations, however, the objectives of IS&S are based upon and driven by the objectives of the three corporate groups or departments usually involved in constructing an IS&S approach. Unfortunately, these groups—the information infrastructure support staff, the information management staff, and the security staff—do not focus directly on the operational side of an organization. Their objectives, solutions, and metrics make sense to them and fit nicely into their own efforts but may not be wholly aligned with the overall business approach. For example, experts on information infrastructure may use the ease of technical implementation as a

[1] Senior security manager at a major electric utility, quoted in General Accounting Office [GAO], *Information Security Management: Learning from Leading Organizations* (Washington, D.C.: GAO, Executive Guide, GAO/AIMD-98-68 Information Security Management, May 1998), 21.

[2] Ibid., 24. See also Charles Popper, *A Holistic Framework for IT Governance* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-1, January 2000), Chapters Two and Four, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/popper\popper-p00-1.pdf

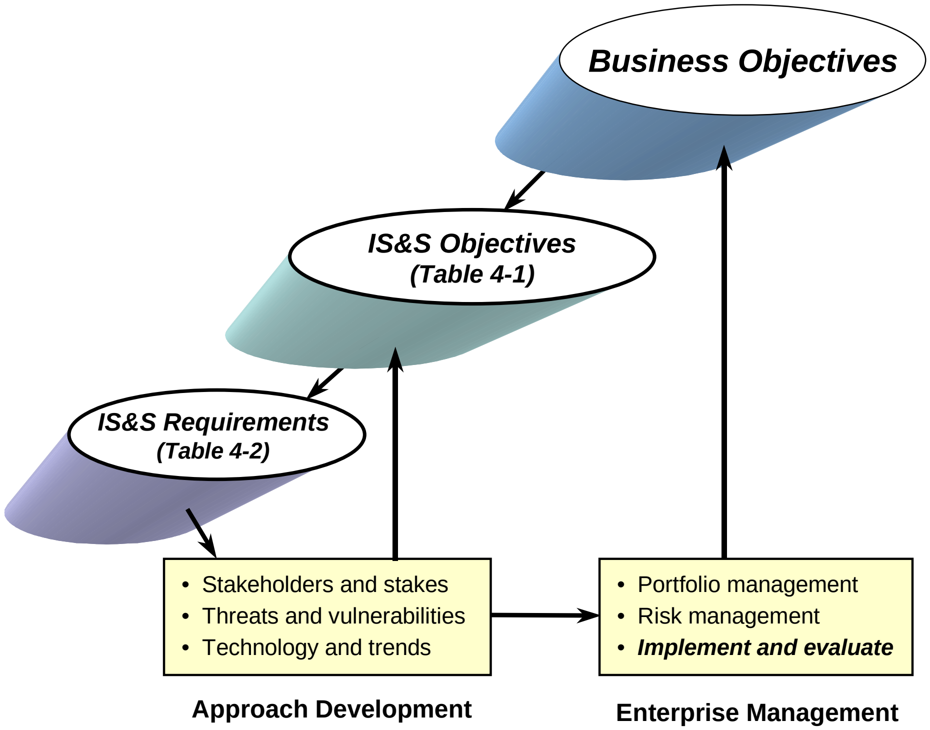


Figure 4-1

IS&S: Developing Objectives and Requirements

key criterion, but the resulting system may be cumbersome for users not concerned with programming. Organizations often complain that security impedes effectiveness or even the ability to conduct business, because it obstructs the flow of information when no compelling security concern outweighs operational concerns.[3] These three corporate groups may not, therefore, be the best source for the organization's IS&S objectives. Would the IS&S objectives support the organization's goals better if they derived from its overall business objectives? Linking IS&S objectives to business objectives may produce IS&S objectives relevant to the overall direction of the organization as well as indicate how the objectives could add value to the organization.

Another problem that faces organizations is knowing when or to what degree IS&S objectives have been achieved. While an organization is developing these objectives, it can also develop criteria to measure whether an objective has been achieved. Such criteria can help to clarify the IS&S objectives and to quantify expectations. "Sufficiently rapidly, sufficiently

[3] Interview by the author with Col. H. Gordon Thigpen, Director, Current Situation Operations Division (CSOD), JCS/J33, Washington, D.C.: The Pentagon, Dec. 15, 1999.

accurately, and sufficiently economically," to use Claude Shannon's terminology:[4] these criteria are usually used to measure technical aspects of communications, rather than to address their success or failure from the perspective of the organization. Adding business-oriented criteria for success (CFS) can enhance the emphasis and clarity of the objectives by keeping the focus on the business value of IS&S.

An organization's use of rigorous metrics—sometimes known as CFS or measures of performance (MOPs)—improves not only the evaluation of the IS&S approach but also the later analysis of how the approach affects the organization's business objectives. For example, the military goes through a process called *security accreditation* to verify that the security environment for a classified system meets DOD standards for information protection. Through this process only the security level of a particular environment is evaluated, not whether the security constraints impede or even halt business operations. Similarly, monitoring an employee's compliance with security guidance does not provide information on how the guidance affects a timely flow of information.

If an organization expects that a new approach to IS&S will act as an enabler,[5] it can use CFS or MOPs to document its expectations, which might include building customer confidence, increasing users' trust, increasing system reliability, or heightening employees' awareness of business objectives by highlighting what the organization considers important. **Table 4-1** offers a fairly simple conceptual tool for summarizing IS&S objectives in relation to overall business objectives. It shows the status, from the perspective of business value, of progress toward an objective, and, when appropriate, can indicate recommended actions. An assumption of the table is that the CFS are presented as part of the objectives. Such a summary presentation offers senior management a quick overview of the direction, status, and benefits of the IS&S effort while simultaneously indicating its relation to overall business concerns. (In this table, as in all those in this report, shading indicates cells that individual respondents would fill in with specific information.)

Once the IS&S objectives have been captured, then the organization needs to identify the associated information to be shared, secured, or shared securely. Identifying them allows the organization to lay out the requirements for the approach to IS&S. Again, identifying the business value while capturing the requirements for the IS&S approach can broaden an understanding of the approach and help to prioritize its component aspects. As more information on culture, stakeholders, trends, and vulnerabilities comes to light, the organization may need to revisit, update, and refine a table like **Table 4-2** more frequently than other kinds of charts.

[4] Quoted in Irwin Lebow, *Understanding Digital Transmission and Recording* (Piscataway, N.J.: Institute of Electrical and Electronics Engineers [IEEE] Press, 1998.), 75; see Claude Shannon, *Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1949).

[5] GAO, 2.

Table 4-1

Sample Information Sharing and Security (IS&S) Objectives

Business Objectives	Sharing and Security Role/Objectives	Business-Value–Based Assessment/ Recommendation
Increased sales Lower production costs per item Increased market share	Enable achievement of business objectives by providing an economically, technically, and critical resource-feasible information sharing environment that is sufficiently secure and enhances operating efficiency. Measures of performance: 1. Enable achievement of business objectives a. Sufficiently flexible to adopt and adapt to new business practices b. Enable consumers to access the data they need when they need it easily and quickly 2. Sufficiently secure a. Acceptable vulnerability mitigation level against information attacks b. Acceptable vulnerability mitigation level against information espionage c. Acceptable vulnerability mitigation level against inadvertent compromise of internal information quality or information exposure d. Acceptable levels of IS&S training and awareness 3. Economically feasible. Within cost constraints 4. Technically feasible. Acceptable availability of needed security technology and of support personnel with required skill set 5. Critical resource feasible. Achievable and supportable with the ADP support personnel, bandwidth, and consumer personnel available	*At the beginning of the IS&S approach development process, use this area to highlight how well the current environment meets the objectives.* *Once the process is completed, highlight recommendations and justifications here.*

Table 4-2

Sample Information Product Requirements

IS&S Objective	Information or Information Product*	Sharing Opportunities	Security Requirements	Issues/ Recommendations

*Note: For further discussion of information products and other terms, see section 2.2.

Using the approach shown in Table 4-1 in the context of the PDDs, **Table 4-3** summarizes the objectives of federal, state, and local agencies in sharing information with industry. The business objectives shown in Table 4-3 were derived from PDD 63[6] and the National Plan for Information Systems Protection, version 1.0[7] and from discussions with General Robert T. Marsh, formerly chairman of the PCCIP. The private sector could apply the recommendations relevant to culture and wording (see section **3.2**) and present the objectives for such areas as the following:

- protect investment;
- ensure proper response while protecting privacy, privileged information, reputation, and customer confidence; and
- assure affordability and feasibility.

Given the objectives shown in Table 4-3, the organization can then consider what information products are best suited to accomplish them. **Table 4-4** gives an example of this for the PDD setting.

The IS&S objectives of different stakeholders vary widely in relation to different business objectives. Developing a chart such as **Table 4-5** to capture the stakeholders' objectives in alignment with their business objectives allows the organization to identify varying perspectives on the issues. The information can then be summarized and portrayed as shown. (For a discussion of capturing information in the context of stakeholders and stakes, see **Chapter Five**.)

As an example, the issue of multiple networks for multiple levels of security provides a focus when modeling the objectives of military guidance[8] and direction[9] for dominant battlespace awareness and information superiority. Warfighters' objectives for IS&S may include the ability to access all data sources from a single workstation (see **Table 4-6**), while the objective of the intelligence community is to ensure that timely and accurate intelligence information is available to the warfighters (**Table 4-7**).

[6] The White House, White Paper on the Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (Washington, D.C.: Office of the President, May 22, 1998), [On-line]. URL: http://www.whitehouse.gov/WH/EOP/NSC/html/nschome.html#doc (Accessed Sept. 2, 1999.)

[7] National Plan for Information Systems Protection: Defending America's Cyberspace—An Invitation to a Dialogue, Version 1.0 (Washington, D.C.: Office of the President, Jan. 2000), [On-line]. URL: http://www.whitehouse.gov/WH/EOP/NSC/html/nschome.html#doc (Accessed Jan. 30, 2000.)

[8] Chairman, Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: Office of the Chairman Joint Chiefs of Staff, n.d.), 2, [On-line]. URL: http://www.dtic.mil/jv2010/jv2010.df (Accessed Dec. 7, 1999.)

[9] Director, The Joint Staff, *C4I for the Warrior* (Washington, D.C.: Office of the Director, The Joint Staff, Command, Control, Communications, and Computer Systems, JCS/J6I, January 1998), 1.

Table 4-3

Summary: PDD Sharing and Security Objectives

Business Objective	Sharing Role/Objectives	Security Role/Objectives	Business Value-Based Assessment/ Recommendation
Protection of national interests by deterring attacks, protecting, responding, and recovering	1. Make threat intelligence information readily available to those that need it 2. Generate and disseminate attack warning in timely enough fashion to be effective 3. Detect attack with sufficient accuracy, including timeliness, to enable creditable response 4. Share attack information in sufficient quantity and quality to enable the various organizations to accomplish their roles and missions	5. Protect organizational resources 6. Protect public's confidence in overall infrastructure as well as individual participants 7. Deter attacks	Environment yet to be established
Proper response to attacks	8. Obtain investigation information of sufficient quality, including timeliness, to determine scale of attack, identify attacker(s) and support proper law enforcement or military response	9. Adherence to privacy and other information statues and policies 10. Ensure that investigation and pursuit of attackers should not unduly impact victims, or make more victims	Environment yet to be established
Public confidence	11. Enhance public awareness and confidence in information infrastructure protection 12. Increase private sector participation as information infrastructure protection partners with government	13. Avoid "Big Brother" syndrome 14. Ensure government awareness and priority for protection of customer confidence, business reputations, intellectual property and other private sensitivities when accepting and using infrastructure protection information from private sources	"A common interest in anticipating and avoiding events that put public confidence at risk may well be the primary motive force for government and major business sectors to rethink their respective compartmentalized perceptions of risk and, then, to undertake a restyling of the traditional government-business relationship in regard to national security in order to determine risk jointly."*
Conservation and effective/efficient use of critical resources (i.e. analysts, computer techies and law enforcement agencies as well as bandwidth and computing power)	15. Align analytical processes to allow sharing of information collection and analysis, allowing for reduction in similar or duplicative efforts 16. Share information effectively to reduce number of duplicated efforts	17. Ensure that sharing and analysis do not undermine the security and integrity of the various organizational operations	

*Source: Peter H. Daly, *Soldiers, Constables, Bankers, and Merchants: Managing National Security Risks in the Cyber Era* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-3, June 2000), 30, [On-line]. URL: http://pirp.harvard.edu/pubs_pdf/daly\daly-p00-3.pdf

Table 4-4

IS&S Information Needed for PDD Scenario

IS&S Objective	Information	Sharing Opportunities	Security Requirements	Issues and Recommendations
Make threat intelligence information readily available to those that need it	Threat intelligence	List entities with which information needs to be shared and the value of that sharing	List threats and mitigation requirements, including constraints on security	
Generate and disseminate attack warning in timely enough fashion to be effective	Attack warning information			
Ensure attack detection occurs with sufficient accuracy, including timeliness, to enable creditable response	Attack detection information			
Share attack information in sufficient quantity and quality to enable the various organizations to accomplish their roles and missions	Attack characteristics information			
Protect organizational resources				
Protect public's confidence in overall infrastructure as well as in individual participants				
Deter attacks				
Obtain investigation information of sufficient quality, including timeliness, to determine scale of attack, identify attacker(s) and support proper law enforcement or military response				
Adhere to privacy and other information statues and policies				
Ensure investigation and pursuit of attackers do not unduly impact victims, or create more victims				

Table 4-5

Model IS&S Objectives by Stakeholders

Business Objective	Stakeholder/ Stake	Information Sharing Objectives	Information Security Objectives	Current Business Value Assessment	Business Value Assessment of Proposed Changes
Objective 1	Information consumers			How well does the current environment meet the objective?	Assessment of recommended changes
	Information providers				
	Information protectors				
	Information custodians				
Objective 2	Information consumers				
	Information providers				
	Information protectors				
	Information custodians				

Table 4-6

Sample GCCS Objective: Single Workstation Access

Business Objective	Stakeholder/ Stake	Information Sharing Objectives	Information Security Objectives	Current Business Value Assessment	Business Value Assessment of Proposed Changes
Dominant battlespace awareness and information superiority	Common to all stakeholders	Win! Save money and resources			
	Warfighter/ business critical	Single workstation access to information Improve warfighter efficiency and effectiveness	Protect national security information, plans, and operations	The separate, disjoint realization is significantly impacting information accessibility, availability, and reliability. Accessibility and availability cost the organization staff hours and decision accuracy as people have to physically move from workstation to workstation to collect, analyze, assimilate, cross check, and disseminate information. The reliability aspect stems from information being copied to various networks for accessibility reasons, where the information subsequently gets out of synchronization with the source information thereby jeopardizing the quality and value of the information and subsequent decisions.	
	Intelligence community/ business critical	Get timely, accurate intelligence to the warfighter	Protect sources and methods		
	National Security Agency—CSS/ business support	Develop reporting standards that maximize information sharing	Ensure secure operation of information infrastructure		
	Joint Staff/ business support				
	DISA and ADP support personnel/ business support, critical resource constrained	Optimize bandwidth and computational resources to ensure ability to meet warfighter needs	Provide a secure information infrastructure		

DISA = Defense Information Systems Agency

Table 4-7

Example of Information Requirements for the GCCS

IS&S Objective	Information	Sharing Opportunities	Security Requirements	Issues and Recommendations
Obtain single workstation access to information Improve warfighter efficiency and effectiveness	Warfighter information	Access to warfighter data at multiple classification levels from a single workstation	Deployed troops operate mainly at SECRET and UNCLASSIFIED levels Security level for access is determined by the security clearance and need-to-know permissions of the person, the security level of the physical environment, the security level of the workstation, and the security level of the supporting communications	
Get timely accurate intelligence to the warfighter Protect sources and methods	Intelligence products			
Optimize bandwidth and computational resources to ensure ability to meet warfighter needs	All			
Protect national security information, plans, and operations	All			
Ensure secure operation of information infrastructure	All	Security posture data Security effectiveness data Security efficiency data	Trained and cleared support and operational personnel	
Provide a secure information infrastructure	Defense in-depth information		Trained and cleared support and developmental personnel	

Chapter Five

Influences on IS&S

Whether a new organization is creating an approach to IS&S from scratch or whether an existing organization is examining specific issues, the factors to be considered and the options they raise may seem infinite. A helpful starting point is to identify and understand the factors that influence why the information is to be shared or secured (see **Figure 5-1**). Recognizing and understanding the stakeholders and their stakes can help the organization to determine, weigh, and prioritize the factors and options that need to be balanced. Identifying threats and vulnerabilities can indicate specific issues to address. Technology—a double-edged sword—and the dynamics of the business and information worlds simultaneously limit possibilities, provide potential answers, and lead to new questions.

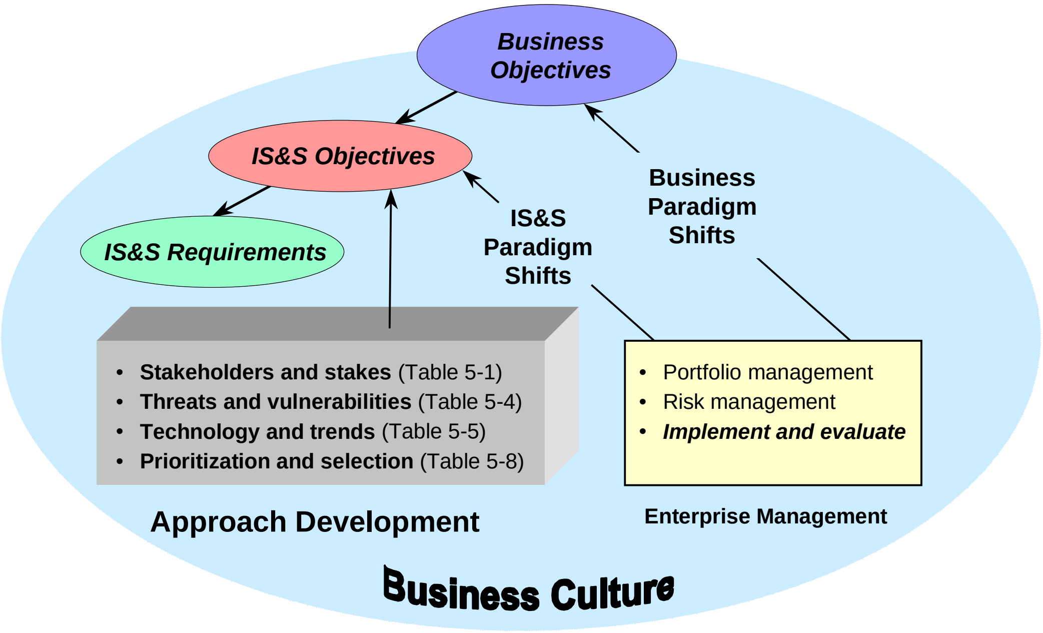


Figure 5-1

Identifying Influences on an Approach to IS&S

5.1 Roles of Stakeholders and Stakes

The advent of the information age will require, as never before, that we take a wider perspective and avoid stovepipes that blind us to changes taking place outside our own sphere of direct responsibility.[1]

Who has a vested interest in an organization’s approach to security? Traditionally, the stakeholders have been consumers and providers of information, and, in some instances, its protectors. Global interconnection and interdependence mean that stakeholders may be located anywhere throughout the world. The information explosion means that copied data are proliferating; it has also led to a worldwide shortage of technical experts to support the information infrastructure. The need to identify the sources and owners of information has become extremely important. So has the need to give greater consideration to the developers, maintainers, and managers of the information infrastructure.

It is not uncommon for an organization to have many stakes in an information product or system, that is, to be simultaneously information consumer, provider, and protector:

- **Consumers** use and exploit the information to realize its business value;
- **Providers** collect, analyze, and disseminate information to consumers; and
- **Protectors** advise about and enforce information security.

Increasing interconnection, either internal to an organization or global, has dramatically increased the number and complexity of stakeholders and stakes and greatly expanded these traditional roles. Businesses now need to deal with:

- **Global consumers**: A special category of information consumers, they are entities outside the organization, other than direct customers, that use the organization’s information. Because of the business benefits of globalization, the IS&S approach needs to consider these consumers in terms of interoperability and information accessibility.
- **Global Providers**: A special category of information providers, they are entities outside the organization that supply information to the organization. Again, because of the business benefits of globalization, the IS&S approach needs to consider these providers in terms of compatibility, interoperability, and information availability.
- **Global Protectors**: A special category of information protectors, they are entities outside the organization that protect proprietary information as it travels between organizations. The IS&S approach needs to consider these protectors in terms of compatibility, interoperability and information vulnerabilities.

[1] Andrew W. Marshall, “Foreword,” in *Strategic Appraisal: The Changing Role of Information in Warfare*, edited by Zalmay M. Khalizad and John P. White (Santa Monica, Calif.: The RAND Corp., 1999), 2, [On-line]. URL: http://www.rand.org/publications/MR/MR1016/ (Accessed Feb. 27, 2001.)

For example, in both policy and practice, the U.S. military emphasizes being as forthcoming as possible with the news media about military operations. With the obvious restriction on discussion of operational details that might help the enemy, the armed services have traditionally allowed the media to interview military personnel and to show them performing wartime tasks. In the age of globally connected information, the military has found it must take new stakeholders into account: members of the military and their families. During the crisis in Kosovo in 1999, a routine interview with an aircrew in which pilots' names were mentioned resulted in hate mail and death threats sent to the pilots' homes, because supporters of Serbia easily found information about the pilots on the Internet.[2]

This example illustrates the way that an organization must take its culture into account in designing an approach to IS&S. From an overall military perspective, threats to one or several members of an aircrew and their families are of little significance. But, even setting aside their effect on the warfighters' morale, the culture of cherishing individual rights means that few in the United States or the U.S. military would find physical or psychological harm to a warfighter's family acceptable.

In a common business paradigm, security is viewed as a cost of doing business, one over which the organization has relatively little control. The unquestioning adoption of this notion has meant that:

- security has come to be seen as separate from core operations, which has led to creation of separate departments to handle security;
- it has come to be treated as an "add-on," rather than a "built-in" function of information systems;
- a failure in communication has occurred among operators, information providers, and information protectors; and
- employers and employees have become apathetic about enforcing business constraints in the name of security.

These attitudes have come about because basing IS&S objectives on the objectives of the security community implies that security is the dominant factor in the balance of sharing and security, which propagates the paradigm of security as a cost (see **Chapter Four**). Although there may be merit to having a separate pool of security experts, should they make the final call between business and security tradeoffs? Perhaps information security personnel need to act like good lawyers, who do not try to set policy on the basis of law unless a course of action is clearly illegal but, instead, carefully outline all the legal risks and allow the decisionmakers to weigh risks against potential benefits. Security experts need to follow this model.[3]

[2] Interview by the author with Lt. Gen. John Woodward, JCS/J6, Dec. 14, 1999.

[3] Charles Popper, personal communication to author, May 2, 2000.

One approach to countering the traditional paradigm would be to involve key stakeholders, at the appropriate levels, in identifying and assessing vulnerabilities; developing and implementing the security architecture; and putting the security approach into practice. Information consumers and providers have the largest business value stake in eliminating information vulnerabilities; moreover, their business processes will be affected profoundly by the way security is actually implemented, and their staffs will carry the bulk of the load in working with the resulting system. Finally, the overall business environment and the organization's profits will be affected by the efforts traded away to accomplish IS&S.

5.1.1. Information Ownership

Decisions about IS&S raise questions concerning the information *owner*, often called the information *originator* by the intelligence community. What role should the information owner have in deciding with whom to share information? What *should be* the owner's role in setting security requirements and verifying security approaches? Most important, who *is* the information owner? Traditionally, the entity with ultimate jurisdiction over the information is considered the owner and has the authority to make decisions pertaining to IS&S requirements. By contrast, an information *source* is simply the entity, either internal or external, from which an organization obtains a given piece of information.

In the global market, where information is duplicated and distributed worldwide, identifying information ownership is essential, not least because failure to meet the owner's expectations of security may prompt the owner to rescind the right to use the information.[4] Decisions on sharing information ought to consider not only the immediate environment but also the environment to or from which information passes, and to take the following questions into account:

- Who is responsible for information security?
- Who is legally liable if security fails or information is compromised?
- As an environment is secured, should the approach to security allow for external data sources or for external data consumers?
- How do laws and regulations on sharing technology apply to an international corporation that shares data across national boundaries?
- What burden does a security approach put on an organization's customers?
- If an organization shares information with a business partner, with whom may that partner then share that information?
- If the organization accepts information from a source, has the recipient accepted liability for that information?
- What does the provider of the information expect in return?

[4] The evolving legal framework in this area is beyond the scope of this paper.

If an organization copies a database onto its network, who owns the information in the duplicate database? Is the owner the original source of the information, the holder of the information, or the provider of the information? If the source is to remain the owner, will the receiving organization allow the source to dictate what it can and cannot do with the information? If the owner is external to an organization, who represents the owner's interests? If the organization passes the information to outside entities, what will be the information owner's position on these issues?

In the private sector, on-line purchasing offers an example. When a consumer gives credit card information in an e-commerce transaction or to a Web site, who owns that information? What are the rights and obligations of each party? What rules govern subsequent sharing of that information? In the military, when sensitive intelligence information is duplicated on several networks to allow faster access, who decides if the security environment on a particular military network is adequate? Who is responsible if the information is compromised, if it is out of date, or if it has been corrupted? In the context of the PDDs, if commercial entities share information on security intruders and cyber attacks with government agencies, who owns that information and determines what can be done with it?

Answers to these questions are not straightforward. In some instances, statutes and regulations outline them, but the culture and dynamics of the particular organization also influence them greatly. If the organizations involved lack a common understanding of ownership, key decisions may be flawed because they will be based upon bad assumptions. Enormous advantages can result for an organization that establishes guidelines early on to address questions of information ownership, even if the guidelines are later amended or exceptions granted. Establishing guidelines, assigning or acknowledging the owner of information, and clearly stating what ownership entails, can prevent future confusion and misunderstandings.

5.1.2 Information Infrastructure Operation and Maintenance

In addition to information consumers and providers, the communities responsible for operating and maintaining the information infrastructure also have a large stake in the amount of human and financial resources needed to support various sharing and security approaches. These resources represent recurring, long-term commitments. Because personnel with the necessary technical skills are increasingly difficult to find, the cost and availability of experts directly affect the economic and technical feasibility of IS&S approaches. On the other hand, the scarcity may prompt organizations to invest in skilled personnel and advanced training programs, benefiting the organization in the longer term and turning a problem into an opportunity.

Information technology (IT) providers include commercial software and hardware vendors, communications vendors, and internal resources. Information infrastructure developers are responsible for the initial realization and subsequent upgrading of the organization's information infrastructure. Understanding the business directions of these entities, as well as their capability and willingness to provide IS&S technology and configurations, is a key consideration in formulating IS&S architecture, implementation, and realization.

Information infrastructure maintainers ensure the proper operation of the information handling and processing tools. Ordinarily viewed as the organization's automation support organization (or just the "computer services" department), the maintainers need to have both the human resources and the tools to accomplish their portion of the IS&S approach.

5.2 IS&S Implementation: An Example

Devising a general model that meets the needs of all, or even most, stakeholders and situations is a daunting if not impossible task in which one vital—and feasible—step, as described above (section **5.1**), is to identify the stakeholders and their stakes. Presenting decisionmakers with an organized analysis of the major players and their interests can help frame the issues, even if the results do not automatically point to a particular IS&S approach.

Suppose a "Feline Stories" Web site were expanded to sell books on cats. Customers could view descriptions of the merchandise and prices and use credit cards to submit their orders. The site would automatically order books from wholesalers. The site—the owner, in this instance—would pay the books' vendors and charges the customer's credit card for the books, adding a small surcharge and taxes; the site would also retain customer information to ease subsequent purchases. **Table 5-1** provides a sample of the stakeholders and their stakes.

Identifying and charting in a single table the stakes of the various stakeholders helps an organization to recognize and address the many sides of the sharing and security issue. Charting this new information, as shown for the PDDs in **Table 5-2**, eases identification of conflicts internal to and between stakeholders and documentation of recommended remedies. It allows stakeholders and managers to visualize the effects of recommendations and the tradeoffs to be considered in decisions.

An organization needs to understand each stakeholder's opportunities and risks. Just as important is recognizing the potential consequences of each security approach for each stakeholder. Pulling your finger out of the dike and running may mean you only get wet, but it may ultimately flood the village. Because the global marketplace means that one entity can have far-reaching effects on others, capturing and quantifying each stakeholder's contributions and requirements can help an organization to clarify and prioritize the stakes. Organizations can then incorporate these stakes into criteria for success, highlighting expectations.

Table 5-1

Stakeholders and Stakes for Feline Stories Web Site

Stakeholder Type	Sample Stakeholders	Stakes in Sharing	Stakes in Security	Contentions	Recommendations
Consumers	Potential customers (descriptions and pricing information)	Easy access to book information.	Trust in book descriptions and prices	The more secure the Web site, the less user friendly it may be if it requires passwords, special client software, etc.	Make site as secure as possible without requiring specialized client software or passwords for read-only access to site
	Wholesaler (ordering and shipping information)	Ability to fill orders properly and make money	Trust in order and shipping information		
	Accounting department (ordering and billing information)	Ability to manage revenues, pay taxes, pay salaries, ensure orders are filled as ordered			
	Future business department (sales information)	Ability to expand business by analyzing buying trends			
	Infrastructure support (number of site users, volume of orders, sensitivity of information provided)	Maintaining optimum infrastructure configuration and efficient operations. Ability to trouble shoot and recover from problems	Web server sizing and security		
Providers	Customers		Ease of order entry, protection of credit card data from fraud, disclosure of credit information, etc.		
	Wholesalers		Customer orders and customer confidence		
Owners		Profits and sales	Direct losses to business and cost of security		
Protectors	Infrastructure support		Resource required to accomplish security approach		
	Business		Legal privacy requirements,* business relation-ships—reputation and customer satisfaction		

*Under "Stakes," detailed information on legal requirements is outlined in GAO Executive Guide, *Information Security Management: Learning from Leading Organizations* (Washington D.C.: General Accounting Office, GAO/AIMD-98-68, May 1998), 10–11.

Table 5-2

Summary: Sharing and Security Stakes for PDD Attack Detection and Response

Stakeholder Class	Stakeholder	Stakes in Sharing	Stakes in Security	Contention Assessment
Information Consumer	Federal government National, state and local law enforcement Critical Infrastructure Assurance Office (CIAO)/Computer Emergency Response Team (CERT) Other sites that are vulnerable to similar attack	Ability to determine if national attack Ability to pursue and prosecute criminals Situational awareness Situational awareness	Rapid response to national security threat Deterrence of additional attacks Ability to coordinate wide-spread attack response Ability to preempt attack on their site	Federal government ability to monitor/ respond versus the "Big Brother" syndrome National response versus individual (or limited number of) corporation's reputation/ customer confidence Avoid advertising a terrorist's success versus notifying public of threat/vulnerability "The one common denominator is public confidence. Government and business both derive viability from it, view it as a critical asset, and–most important–will go to great lengths to retain it."*
Information Provider	Site(s) being attacked	Call for assistance, ability to warn others	Loss of customer confidence if attack information revealed by government	Warning other sites versus losing customer confidence Getting help versus losing customer confidence
Information Protector	Security software vendor for attacked site(s) Attack response support for attacked site(s)	Loss of customer confidence in product Ability to receive countermeasures in timely fashion	Ability to develop/ deploy countermeasures Jobs at stake?	Vulnerability aware-ness for customers versus vulnerability awareness for attackers
Information Custodian	ADP support staff	Ability to recover from attack	Staff hours used in responding and recovering from attack	Staff hours to participate in national security program, including training, versus staff hours to support direct customer base

*Peter H. Daly, *Soldiers, Constables, Bankers and Merchants Managing National Security Risks in the Cyber Era* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-3, June 2000), 29, [On-line]. URL:

Some items are clearly missing from **Table 5-2**, namely the following: Who will pay for the IS&S infrastructure for PDDs 62 and 63? Who is responsible for the overall success of the program established under the PDDs? Finally, who determines what is "secure enough"? Because these questions are not currently (2001) answerable, the table does not address them.[5]

Initially, an organization may find it beneficial to sort and examine stakes and conflicts according to the various information products in order to prioritize stakes according to the importance of different products (see **Chapter Two**) and as an aid to highlighting "problem" products. This procedure may lead to recommendations to change certain information products or for certain stakeholders to use different products better suited to their needs.

5.3 Threats, Vulnerabilities, and Mitigation

> *Experience indicates that the current vulnerabilities may not persist. Little attention has been paid to building defenses until now. The technology is changing rapidly, and information systems continue to evolve as they keep up with these changes.*[6]

The information age has brought "disruptive technology" not only to business[7] but also to information security. The Internet and its myriad associated interconnections change the number and the types of threats and the potential damage they may cause. In e-commerce, an entire venture can fail if the customer base loses confidence in the site's security. The damage resulting from a site being "hacked" may not be the loss of information to the hacker but, rather, a loss of business reputation because the site was hacked. As an organization evaluates security threats, it may need to develop damage assessments based on business value to augment its assessment of potential technical damage. (See **Table 5-3** for an example of IS&S stakes for the GCCS environment.)

Sharing and security approaches, like operational implementation, need to be flexible and adaptable to keep pace with the changing world, advancing technology, and evolving threats. Here the term *threat* is used to refer to a potential compromise of information or of its quality. Traditionally, a threat has both a source and a potential consequence. Sources may be internal, such as an untrained computer operator who accidentally deletes an organization's database, or external, such as an industrial spy or saboteur. The IS&S approach needs to describe the potential consequences of a threat in concrete terms, that is, the actual information compromised or impact on quality if the threat were to materialize. Commercial domains where interest is high and risks

[5] Peter H. Daly does an excellent job of weighing such questions as "Who will pay for the security?" "Who will choose the response to an attack?" and "Who will assure readiness?" See Daly, *Soldiers, Constables, Bankers, and Merchants: Managing National Security Risks in the Cyber Era* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-3, June 2000), 32–33, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/daly\daly-p00-3.pdf

[6] Marshall, 4.

[7] Clayton M. Christensen, *The Innovator's Dilemma* (Boston, Mass.: Harvard Business School Press, 1997), xv.

are evident have responded strongly to the threat of external intrusions. Certainly, the demand for services that help companies defend themselves is increasing very rapidly.[8]

Threat assessments, sometimes referred to as security risk assessments, ordinarily identify, qualify, and quantify dangers to the U.S. information environment. Although there is an art to threat assessments, most organizations can find either internal or external entities to accomplish the basic technical effort. RAND's 1999 Project Air Force book provides excellent background about generic threats to information sharing and interconnectivity.[9] What is often overlooked in making assessments is the subsequent "internalization" of the assessment to account for the specific objectives, culture, and stakes of a given organization. Something that threatens the very existence of one organization may not even apply to another.

In terms of business value, *vulnerabilities* reflect the potential costs of not addressing a threat or a series of threats. Vulnerabilities differ from security risks in that a *risk* has several contexts, including an action's likelihood of success.[10] Vulnerability can be direct, such as the loss of sensitive data, or indirect, such as the loss of customer confidence or degradation of business reputation. A vulnerability assessment, which needs to be based upon the threat assessment, depicts the likelihood of a threat and the threat's probable impact. The urgency of a vulnerability reflects its probability, timing, and business value; thus, a near-term threat with a high probability of occurrence and large business value would be of high urgency.

A synopsis of the threat environment in a chart such as **Table 5-4** provides decisionmakers with a quick reference guide. It allows IS&S developers to rank threats and recommendations based upon urgency, business impact potential, vulnerability rating, or mitigation approach, or upon the objective (business or IS&S) affected. Additional columns outlining the effects of various mitigation mechanisms on objectives, performance, costs, and culture may assist in the development of a mitigation approach. Finally, an organization may find it useful to create charts that depict information product vulnerabilities, mitigation mechanisms, and the effectiveness of those mechanisms.

Both the PDDs and the GCCS face the generic threats outlined in this section. For the PDD setting, the PCCIP and PDD 63 reports highlight the vulnerabilities resulting from insider actions—for example, where system administrators or users divulge a password or information—and denial of service as the most serious vulnerabilities. Chapter Nine of RAND's 1999 Project Air Force book does a good job of outlining and analyzing the threats to the critical infrastructure

[8] Marshall, 4.

[9] Zalmay M. Khalilzad, "Defense in a Wired World: Protection, Deterrence, and Prevention," in *Strategic Appraisal*, 406.

[10] The security community ordinarily uses the terms *risk* and *risk assessment* in the same way that *vulnerability* and *vulnerability assessment* are used here.

Table 5-3

Sharing and Security Stakes Across GCCS Information Products

Information Product	Stakeholder Class	Stakeholder	Stakes in Sharing	Stakes in Security	Conflicts
War Plan	**Information Consumer**	Field units, transportation providers, deploying forces, task force commander and staff	1. Ability to get the right forces to the right places at the right time to win the war 2. Ability to communicate plan and execute decisions in a timely and reliable manner to carry out plan effectively and efficiently	1. Surprise; do not want the enemy to know "when, where, and who" of our plan. Must provide proper level of security for two different security levels of plans during execution 2. Time and expertise to execute the sharing and security approach 3. Adherence to NDP-1 and other statutory requirements for sharing classified and privacy data with allies and coalition partners	The warfighting community concurs that the separate, disjoint realization is significantly impacting information accessibility, availability, and reliability. Accessibility and availability cost the organization staff hours and decision accuracy as people have to physically move from workstation to work-station to collect, analyze, assimilate, cross check, and disseminate information. The reliability aspect stems from information being copied to various networks for accessibility reasons, where the information subsequently gets out of synchronization with the source information thereby jeopardizing the quality and value of the information and subsequent decisions.*
	Information Provider	Planning staffs, transportation managers, deploying units	Timely and realistic feedback on supportability and capability critical to planning	Must provide for security of three different level of plans during plan development	
	Information Protector	NSA, software vendors, DISA, GCCS SWG**	Financial well being of secure software vendors and security technology markets	Enforcement of national security regulations and guidance for handling and processing classified information	
	Information Custodian	ADP support staff	1. People, tools, time and money to implement and operate sharing realization 2. Enforcement of NDP-1 3. Determination by NDPC of what information can be released or disclosed to allies and coalition partners	People, tools, time and money to implement and operate security realization	

*Interview by the author with Col. H. Gordon Thigpen, Director, CSOD, JCS/J33, Washington, D.C.: The Pentagon, Dec. 15, 1999.

**The GCCS SWG is the GCCS Security Working Group, chaired by the Joint Staff with representatives from all nine warfighting commands.

Table 5-4

Generic Web Site Threats

Threat and Source	Urgency (Likelihood)	Impact Potential (Business Terms)	Business Impact Rating	Approach(es) to Mitigation
Corruption of product information hacker or competitor	Possible today but not likely in the near term	Business impact—minor Loss of e-commerce product sales from time of corruption until corruption corrected. Loss of customer confidence in Web site	Low	Ensure security features properly configured on Web server
Corruption of customer information by hacker or competitor	Six months	Business impact—major Loss of orders sent or billed to wrong accounts—likely to involve limited number of transactions from time of corruption until corruption remedied	Medium	Ensure security features properly configured on Web server
Theft of product information by insider	Possible today but not likely in the near term	Business impact—nuisance Indicates possible insider vulnerability that should be dealt with Can be achieved by copying site or company magazine	Low	None
Theft of product information by competitor or hacker	Possible today but not likely in the near term	Business impact—nuisance Could indicate vulnerability for more aggressive actions Can be achieved by copying site or company magazine	Low	Ensure security features properly configured on Web server
Theft of customer information by insider	Possible today but not likely in the near term	Business impact—catastrophic Loss of customer sales, customer confidence, business reputation Indicates extreme vulnerability within organization	Highest	Deter by ensuring employees understand consequences of stealing company data Institute security awareness program including safeguarding passwords Conduct background checks for ADP support personnel
Theft of customer information by hacker	Possible today but not likely in the near term	Business impact—catastrophic Loss of customer sales, customer confidence, business reputation	High	Procure and install security software for customer information database and transactions
Theft of customer information by competitor	Possible today but not likely in the near term	Business impact—catastrophic Loss of customer sales, customer confidence, business reputation	Highest	Procure and install security software for customer information database and transactions Deter by ensuring employees understand consequences of selling company data Institute security awareness program including safeguarding passwords Conduct background checks for ADP support personnel
Denial of service (DOS)	Near term for e-commerce and other Internet-dependent business	Business impact—major Loss of e-commerce business until DOS attack subsides Loss of Internet connectivity with strategic partners until DOS subsides	Medium	Procure and install DOS prevention software and hardware Participate in anti-DOS partnership with neighboring Internet sites and routers
Physical attack	No foreseeable actors	Long-term loss of operations	Low	No additional actions required

described in PDD 63.[11] Peter Daly emphasizes the importance of business culture and business value to mitigation approaches for NII threats:

> As the cold war wound down and as the pursuit of economic reward became, for most nations, the driving force of global policy, emerging new linkages and new forms of competitiveness dramatically altered the national security landscape into one where private assets may become primary targets [and] conventional business models may prove inadequate to comprehend fully the tension between risk and uncertainty. Heavy reliance on statistical probability and other quantitative decision theories to guide choices that affect such issues as network security are liable eventually to cause regret when an exposure assessed as financially insignificant in terms of probability can be exploited by an adversary, bringing embarrassment and public alarm that might translate into lost confidence in the enterprise. As business increasingly separates from central government, it may not need to adopt the high sensitivity to risk of the politician but, instead, to redefine its traditional concepts of risk to include the new elements that come with dependence on an information infrastructure whose ownership and control are greatly different.[12]

The Project Air Force book provides insights specific to the GCCS setting, including a good outline and analysis of the threats and risks to command and control.[13] Although the book is specific to the Air Force, its terminology applies to other military settings. In Chapter Ten, “Implications of Information Vulnerabilities for Military Operations,” the threats are sorted into computer hackers, traditional weapons, machinery, jamming, new weapons, and “[a]cts of God, nature, and evil spirits.”[14]

5.3.1 Approaches to Mitigation

Organizations need to take mitigating action to foil a threat or to lessen its potential impact. In many respects, mitigation approaches are where the balancing act between sharing and security begins. Selecting mitigation strategies is a balancing act because:

- sharing normally makes money, and security usually costs money;
- the more sharable the information, the less secure the environment;

[11] Roger C. Molander, Peter A. Wilson, and Robert H. Anderson, “U.S. Strategic Vulnerabilities: Threats Against Society,” in *Strategic Appraisal*, [On-line]. URL: http://www.rand.org/publications/MR/MR1016/ (Accessed Feb. 27, 2001.)

[12] Daly, 14–15.

[13] Glenn C. Buchan, “Implications of Information Vulnerabilities for Military Operations,” in *Strategic Appraisal*, 283–323.

[14] Ibid., 288.

- the more secure the environment, the less sharable the information;
- no approach will make an information environment 100 percent invulnerable; and
- people are both the biggest security asset and the biggest security threat.

The balancing act can be complicated, because there is rarely a single mitigation approach to a vulnerability, and rarely is a particular mitigation mechanism unaffected by others. These mechanisms vary in effectiveness, cost, and intrusiveness on information sharing. In addition, there is usually a significant interdependence of the best mitigation mechanism and the business culture. The organization needs to assess the effect of each approach on the overall business culture as well as on other mitigation approaches.

If no basic mitigation strategy is in place, organizations may find it to their benefit to design one prior to taking on specific threats. In selecting mitigation strategies, as for other purposes, an organization needs to turn to the business culture. Two strategies predominate: the government's "detect-protect-respond" defense-in-depth model for INFOSEC and the "resist-recognize-recover" model described by the Computer Emergency Response Team at Carnegie Mellon University.[15] The organization needs to establish an overall mitigation strategy to ensure that all specific mitigation approaches meld with and adhere to it.

RAND's 1999 Project Air Force book outlines and details three basic approaches to mitigating vulnerabilities in IS&S: protection, deterrence, and prevention.[16]

- **Protection** means steps taken to defend directly against a threat before or once it begins to materialize.
- **Deterrence** involves actions taken to compel the source of a threat not to act. Traditionally, this is done by convincing the threat source that the costs or consequences of carrying out the threat are too high.
- **Prevention** involves actions taken to neutralize a threat at its source before it can materialize or to prevent the source from achieving the capability to carry out a threat (e.g., denying technology to the threat source).

Several tools, such as the Attack Tree[17] methodology, assist businesses to develop and weigh options for mitigating threats at the technical level. These tools are important to identifying threats and options but tend to evaluate options according to technical criteria, such as cost and technical feasibility. Although they provide a beneficial and even necessary step to narrowing the

[15] Joint Security Commission, "Report by the Joint Security Commission II," DRAFT (Washington, D.C.: Office of the Deputy Secretary of Defense and Office of the Director of Central Intelligence, August 1999), 20.

[16] Zalmay M. Khalilzad, "Defense in a Wired World: Protection, Deterrence, and Prevention," in *Strategic Appraisal*, 412–432.

[17] Bruce Schneier, "Attack Trees," *Dr. Dobb's Journal* (December 1999), [On-line]. URL: http://www.ddj.com/articles/1999/9912/9912a/9912a.htm (Accessed Feb. 17, 2000.)

broad range of options available, the tools often overlook the importance of recurring and nonrecurring costs, returns on investment, critical resource requirements, business risk assessment, and clear linkage to business objectives. Organizations often focus on finding the specific mitigation to a specific threat rather than on what is best for business overall. Often, security per se is not what impedes the organization's effectiveness or efficiency; instead, it is the implementation of a particular mitigation strategy, chosen without proper consideration for culture, business objectives, all the stakeholders, and future trends.

Other important aspects often missed during the technical analysis are developing detailed CFS at both the technical and business levels, linking them to the CFS of the IS&S objectives, and building a game plan for monitoring and assessment (see **Chapter Six** for a discussion of tools and methods for incorporating these aspects into the security and sharing approach).

5.4 Technology and the Dynamic Information and Business Environments

An architecture, implementation, and realization that can keep pace with changing information technology, changing business practices, and, most important, changing threats are key to proposing a realistic IS&S approach. By examining trends, both actual and potential, an organization will be able to create an IS&S approach that is flexible and adaptable in meeting the organization's future needs. As illustrated in **Tables 5-5** through **5-7**, this examination can be based upon four key areas: purpose or intended use of the information, value of the information, information quality requirements, and environmental considerations.

- **Purpose**. Information is collected, processed, and disseminated for intended uses. These constitute the information's purpose. Although other uses may be found, which may subsequently become purposes, the intended uses largely determine the particular bundling of process, substance, and format to employ. If the purpose of an information product includes sharing the information among individuals or divisions of the organization, or between organizations, its bundling will need to take information security into account.
- **Value**. The value of information reflects the actual or potential benefits to the organization from its use. The value factors into the bundling, because organizations will rarely pay more for an information product than the value of the information it contains. The more substantial the information's value, and the more any compromise would decrease that value, the more interest the organization has in ensuring that the bundling addresses security concerns.

Table 5-5

Trends Common to the PDDs and GCCS

Trend Area	Trend	Business Impact	Impact on Sharing	Impact on Security
Intended use of information	More dynamic information environment with increased emphasis on interactivity and collaboration	More rapid collection, analysis, and dissemination, possibly by moving analysis into either sensor or final exploitation phase	Business critical	
	Information warfare	Increased information requirements regarding infrastructure posture (system status) Increased information requirements about information infrastructure and supporting personnel		Business critical
Value/quality of information	Increased value/quality of information Information more perishable More time constrained to be usable	Increased vulnerability and urgency as business value of information rises Increased speed and throughput requirements	Business critical	Business crucial
Environment	Dramatic increase in volume of information	Increased dependence on communications, interoperability, and connectivity	Business critical	
Threats	1. Decline of vulnerability to "nuisance" hacker as secure computing technology is fielded 2. Increased threats in the asymmetric warfare category	"Increased threats, both in type and source: Second, the information 'dimension' increasingly becomes central to the outcome of battles and campaigns. Therefore, protecting the effective and continuous operation of one's own information system and being able to degrade, destroy, or disrupt the functioning of the opponent's information system will become a major focus…."*		Business critical
Technology	Maturing and adoption of secure computing technology, including MLS network technology			Business critical
Marketplace				
Infrastructure	1. Bandwidth constraint will continue 2. Faster, smaller computational hardware 3. Improved user interfaces allowing less cumbersome devices; move to more "roaming" technology 4. Costs for refreshing hardware and software will remain fairly constant	Information consumers and providers will become more mobile, restrained mostly by the availability of bandwidth "Considerations of strategies for managing the risks of the cyber era ought not become trapped in the belief that either the past or even the present offers a reliable basis for predicting the future.… Fundamental rules of life are being rewritten, from genetics to astrophysics, and with that new uncertainties appear.... When change is the norm rather than a deviation and economic connection rather than political division is rising as the world's primary organizing principle, the largely quantitative means of calculating risk used for national security strategy in the more bordered and static era of the cold war—territory, troop size, missile counts, delivery systems, and throw weights—do not easily fit the risk environment now taking shape."**		Business critical

Table 5-5 (continued)

Trend Area	Trend	Business Impact	Impact on Sharing	Impact on Security
Consumer capabilities and characteristics	1. More computer literate 2. Financially constrained 3. Larger volumes of information available 4. More interactive environment	1. Increasing connectivity and computer literacy of consumers 2. Increased interconnectivity with strategic and 'ad hoc' partners	Business critical	
Providers capabilities and characteristics	1. Financially constrained 2. Higher volumes of information production 3. Move to Web services type information providing interface	Emphasis on getting the right information to the right place at the right time. Countering the myth that everyone needs access to all information, in fact, that such a paradigm may be detrimental to military operations. In the words of Hans Mark, "Not only doesn't the sergeant need to know what the general knows; there are cases when the sergeant should not know what the general knows." Information overload also needs to be addressed.***	Business critical	

*Andrew W. Marshall, "Foreword," in *Strategic Appraisal: The Changing Role of Information in Warfare*, edited by Zalmay M. Khalilzad and John P. White (Santa Monica, Calif.: The RAND Corp., 1999), 4-5, [On-Line]. URL: http://www.rand.org/publications/MR/MR1016/ (Accessed Feb. 27, 2001.)

**Peter H. Daly, *Soldiers, Constables, Bankers and Merchants Managing National Security Risks in the Cyber Era* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-3, June 2000), 11–12, [On-line]. URL: http://pirp.harvard.edu/pubs_pdf/daly\daly-p00-3.pdf

***Hans Mark, "The Doctrine of Command, Control, Communications, and Intelligence: A Gentle Critique," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2000* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-01-1, [On-line]. URL: http://pirp.harvard.edu/pubs_pdf/mark\mark-i01-1.pdf

Table 5-6

Trends That Specifically Affect the PDDs

Trend Area	Trend	Business Impact	Impact on Sharing	Impact on Security
Environment				
Threats	"In the post-cold war world, the creation of most high technology is driven not by traditional national security requirements but by commerce. ... The displacement of ideology by commerce as the primary global organizing principle and the heavy reliance of government on private enterprise to create and deploy critical technologies present new conditions for U.S. national security planners."*	"Economic, rather than military, crises now pose the most significant direct threats to U.S. security. The tighter and tighter coupling of the world financial markets through global information infrastructures, increasing U.S. reliance on open global markets for prosperity, and the critical role of the U.S. in anchoring the global economy as a whole have made economic contagion both a reality and a risk, while military crises, in the absence of opposing bloc alliances, tend to be confinable. … Although governments retain an important role, the development and protection of commercial technology is primarily a business problem, amenable to business solutions more than to public policies. This change suggests a new tolerance for security as well as privacy and a new style of command and control systems that are not exclusively under the jurisdiction of either the military or national security apparatus." (Daly, 3).		Business critical
Technology	"Essentially, this uncertainty [regarding risk assessment] requires an extension of risk calculation from self-interest to the interests of the global financial system as a whole" (Daly, 24).		Business critical	
Marketplace				
Infrastructure	Changing role of government in information security	"The role of government in general, and of the traditional national security establishment in particular, in managing emergent risks is less clear or widely supported now than government supremacy was in national security matters during the cold war. When primary targets were military command and control centers, missile silos, ships at sea, and the like, there was no real question of who was in charge or what alternatives for response were available in the event of attack. As the twenty-first century opens, the targets are just as likely to be privately owned assets and commercial information networks as defense systems. Just as financial markets, for example, now exert enormous influence on governance by insisting on transparency and sound fiscal policies, so such new areas of vulnerability constrain traditional law enforcement, intelligence, and military approaches to national security" (Daly, 11).		Business critical

*Peter H. Daly, *Soldiers, Constables, Bankers and Merchants Managing National Security Risks in the Cyber Era* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-3, June 2000), 3, [On-line]. URL: http://pirp.harvard.edu/pubs_pdf/daly\daly-p00-3.pdf

Table 5-7

Trends That Specifically Affect the GCCS

Trend Area	Trend	Business Impact	Impact on Sharing	Impact on Security
Intended use of information	Sensor to shooter Move to “sensor to shooter.” For example, some believe long-range precision strike weapons coupled to systems of sensors and to command and control systems will fairly soon come to dominate warfare.*	More rapid collection, analysis, and dissemination, possibly by moving analysis into either sensor or final exploitation phase	Business critical	
	Move to “crisis planning” process for all planning	More dynamic information environment with increased emphasis on interactivity and collaboration	Business critical	
Environment	Dramatic increase in volume of information	Increased dependence on communications, interoperability, and connectivity	Business critical	
Threats	1. Decline of vulnerability to “nuisance” hacker as secure computing technology is fielded. 2. Increased threats in the asymmetric warfare category	Increased threats, both in type and source: “Second, the information ‘dimension’ increasingly becomes central to the outcome of battles and campaigns. Therefore, protecting the effective and continuous operation of one’s own information system and being able to degrade, destroy, or disrupt the functioning of the opponent’s information system will become a major focus of the operational art” (Marshall, 4–5). “One of the hottest military publications in China is a book written by two professional soldiers in the People’s Liberation Army, Colonels Qiao Liang and Wang Xiangsui. They proposed a new military strategy, advocating moving away from conventional martial doctrine toward “unrestricted war,” which involves multitasking of aggression/defense to include acts of direct terrorism, cyber attacks on critical infrastructures, financial attacks on currencies, political interference, and other methods carried out by military and nonmilitary organizations.”**		Business critical
Technology	Changing characteristics of warfare: “[In 2020] The critical operational tasks will be destroying or disabling elements of an opponent’s forces and supporting systems at a distance. Defeat will occur due to disintegration of command and control capacities, rather than due to attrition or annihilation” (Marshall, 4–5).	Chapter Eleven of RAND’s 1999 Project Air Force Book outlines the effects of “flattening,” “formatting,” and concentrating on core competencies, all of which are direction within the DOD. These moves add dependence on the information infrastructure, add risk to information flow disruption, and increase the importance of IS&S as the need for information sharing increases. Later, the chapter discusses the need to address training and personnel.***	Business critical	
Marketplace **Provider capabilities and characteristics**	1. Financially constrained 2. Higher volumes of information production 3. Move to Web services type information providing interface		Business critical	

*Andrew W. Marshall, “Foreword,” in *Strategic Appraisal: The Changing Role of Information in Warfare*,” edited by Zalmay M. Khalilzad and John P. White (Santa Monica, Calif.: The RAND Corporation, 1999), 4-5, [On-line]. URL: http://www.rand.org/publications/MR/MR1016/ (Accessed Feb. 27, 2001.)

**Daly, 19-20, quoting John Pomfret, “China Ponders New Rules of ‘Unrestricted War,’” *The Washington Post*, Aug. 8, 1999, A1.

***Francis Fukuyama and Abram N. Shulsky, “Military Organization in the Information Age: Lessons from the World of Business,” in *Strategic Appraisal*, 327–360.

- **Quality requirements**. Organizations assess information quality based on eight factors: accuracy, relevance, timeliness, usability, believability, completeness, brevity, and security.[18] If the bundling does not maintain or enhance the quality of the information, it decreases the information's value or may not be suitable to the purpose.
- **Environmental considerations**. Aside from purpose, value, and quality, several environmental factors drive bundling choices: availability of technology, resources, and information; threats; statutory and regulatory requirements; consumer confidence, characteristics, and capabilities; and provider characteristics and capabilities.

To achieve the flexibility and adaptability necessary to a workable approach, an organization needs to outline the key trends in the areas of information purpose, value, quality and environment. Will the purpose for which the information is used change? Will changes in business practices or the business environment change the balance of information value? Must aspects of IS&S change to support the planned evolution of the organization? Must information quality change for the information to retain or increase its value? What other key changes in technology, threats, customer base, or competition may affect the approach to sharing or security?

5.5 Pulling It All Together

A unified view of the objectives, issues, concerns, players, and the business value making up the IS&S approach can be invaluable to obtaining the support of upper management and determining the appropriate direction. Although organizational dynamics and priorities may dictate layout and content, staffs can develop a final chart that succinctly represents the proposed IS&S answers, using the previously developed charts as supporting documentation to provide sufficient justification and background for decisionmakers. **Table 5-8** presents a sample summary chart.

Table 5-8

Sample Prioritized IS&S Recommendations

Objectives	**Recommendation**	**Priority**	**Business Value and Costs**	**Key Stakes and Stakeholders**	**Issues/ Dependencies**	**Risks and Tradeoffs**

[18] The DOD's *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations* (Joint Publication 6-0 [Washington, D.C.: Office of the Chairman, Joint Chiefs of Staff, May 30, 1995], I-5) outlines seven factors. An eighth is to be added here: believability. There must be a level of confidence in the data, whether it stems from a credible source or just because it seems logical.

Once staff members have established the format of the chart, how will they determine its content? A prioritized presentation of options would be valuable, but how are options to be organized, ranked, and weighed against the other factors and concerns discussed in earlier chapters? **Chapter Six**, on business processes, describes how to manage the IS&S approach within the overall business model; but how is the IS&S approach itself to be chosen? There is no single answer to this question. Every organization has unique processes for prioritizing resources and weighing options. Although these processes are highly dependent on organizational dynamics, culture, and politics, some general considerations apply.

Grouping and then arranging information according to objectives facilitates and focuses discussion on sets of recommendations (for example, sharing mechanisms and mitigation approaches) that satisfy a given objective. The organization can analyze these sets according to business value, culture, stakeholders, trends, and feasibility to yield the best recommendations for each objective. By developing several sets of recommendations, the staff can help to identify options and clarify recommendations.

For example, suppose an organization drafted four sets of recommendations for an objective: (1) the “bare minimum” or “80 percent solution,” which emphasizes costs and time, developed to 80 percent of the target budget or functionality; (2) the “sharing Utopia,” which gives priority to sharing over security, waiving cost and time constraints; (3) the “security Utopia,” which gives priority to security over functionality, waiving cost and time constraints; and (4) the “compromise,” which reflects the optimal mix of functionality and security within reasonable cost and timing constraints. The different emphases of the first three sets of recommendations point the way to creating the fourth set by highlighting the “bottom line” for various stakeholders and showing what is possible. If the various stakeholders develop and debate the different recommendations, the discussions may expand their understanding of and support for the overall approach chosen.

As the organization develops these recommendations, dependencies—technical or cultural—between recommendations may appear in the context of funding and budgeting discussions. Identifying conflicts (if A is done, then B cannot be done) or overlaps (if A is done, then B need not be done) between recommendations will also be useful. Once the organization has established the sets of recommendations, it can prioritize them.

Organizations need to consider categorization instead of straight numerical ranking to prioritize recommendations. In addition to saving time because proponents of different recommendations are not arguing over one or two numerical rankings, categorization can lessen the chance of sending an incorrect signal when two recommendations are of equal importance. Take, for example, the categories of “must do,” “highly recommended,” and “optional.” They frequently help to separate recommendations into the top categories, while highlighting for management and stakeholders the likelihood that a recommendation will be acted upon. “Must do,” the highest priority, would consist of recommendations guaranteed funding, because they have a reasonable chance of success and either address a near-term business-critical security threat or enable sharing mandated by senior management or business forces. “Highly recommended” would consist of recommendations deemed to play a significant role in accomplishing an objective because of their business value; they may address a medium- to long-term[19] business-critical threat or mitigate a crucial near-term threat. “Optional” would consist of recommendations that the organization would need to address only if time and money permit, because some recommendations do not represent a significant enough business value or address a significant enough threat to be funded.

If the funding cutoff for IS&S projects falls within a category, or if resource management requires a finer ranking of recommendations, the potentially funded recommendations may have to be ranked. The initial categorization can enable an organization to eliminate entire groups of recommendations from the ranking process if the category falls completely inside or outside the lines of funding.

Once the prioritization is complete, the organization can apply financial and other constraints to produce the recommended IS&S approach. **Table 5-9** offers an example of prioritized recommendations for the GCCS setting. Gaining the support of key stakeholders for a recommended approach before the approach is proposed to upper management for approval can prove beneficial.

The tools and ideas presented in this chapter may not reduce the time and effort involved in developing a viable approach to IS&S, but they will help to organize, address, and format the effort for presentation to senior management. Once the organization has developed its recommendations, the highest priority is to incorporate the approach into the overall organization management scheme. How to do so is described in **Chapter Six**.

[19] Setting “medium term” as two project funding cycles and “long term” as three or more funding cycles allows recommendations not addressed in the current cycle to move up in priority.

Table 5-9

Prioritized GCCS IS&S Recommendations

Objectives	Recommendation/ Priority	Benefits and Costs	Key Stakes and Stakeholders	Issues/Dependencies	Risks and Tradeoffs
Single workstation access for all security levels of GCCS	Automatic security data labeling of electronic data “Must do”	Enables MNS* and MLS solution. Costs would vary greatly depending on data labeling scheme. Allowing DBMS automatically to set the security level based upon the network from which data are received, with limited downgrade by authorized personnel, would be cost effective. Costs: (est.) $500K	DISA and warfighters assigned responsibility for downgrading information.	Prerequisite for MNS and MLS recommendations.	Feasible today.
	MNS (see Appendix) “Must do”	Business-value–added assessment: Significant increases in operational efficiency Decreased information dissemination time as manual steps are removed Less confusion about ownership as need to copy data to multiple networks is reduced Less vulnerability because less confusion over the real classification of information More secure—imperfect trusted products less vulnerable than perfect untrusted software Both private and public sectors need trusted computing products. But these products cannot become technically or financially viable for producers and consumers if not brought in operation and matured. Better to do this now than after ideas of information warfare are more widely accepted and threats during the maturation process become too high. Business costs Implementation costs for Joint Operation and Evaluation System databases only (assuming five data servers and no client software changes required); merging GCCS and GCCS-T database; creating NIPRNet accessibility: (est.) $1 million Operational and technical support training: (est.) $500K	See stakeholders chart [The staff preparing this document would attach a customized chart.]	1. Highlights of implementation: 2. Procedural solutions may be needed to address shortfalls of maturity of trusted software solutions (e.g., limiting who can do downgrades, marking printouts). Each LAN assumed accredited and trusted to security level approved for (i.e., the U.S. accepts all those connected to allied LAN as suitable for processing SECRET information). Multiple technically feasible and economically viable realizations of MNS from ADP perspective. A few are: One MLS server containing all information (of a particular type) with duplicated systems for performance and backup; One MLS server for each level of data using distributed database technology to appear to users as one database; or One set of geographically determined MLS data servers “populated by proximity” using modern data synchronization to maintain data integrity and reliability; and Various methods for attaching or implying data classification label Security awareness and technology training key to development of viable realization	Availability of secure operating systems,** secure database tools*** and other trusted software packages**** make it a viable solution

Table 5-9

Objectives	Recommendation/ Priority	Benefits and Costs	Key Stakes and Stakeholders	Issues/Dependencies	Risks and Tradeoffs
	MLS Network Future "must do"	Recommended as long-term, evolutionary effort dependent on implementation of MNS recommendation		MLS server(s), such as implemented in MNS recommendation, must be implemented	Technology not yet available. Can be built on MNS solution.

*For a discussion of MNS and MLS technology, see section A.3.

**Sun Microsystems at URL: http://www.sun.com has a secure operating system which the company judges to be accreditable to the B1 level of trust.

***Sybase at URL: http://www.www.sybase.com and Oracle at URL: http://www.oracle.com have secure DBMS products that, when implemented on a B1OS, provide B1 level of trust for database functions.

****Trusted Computer Solutions, Inc., at URL: http://www.tcs-sec.com

ADP = automated data processing DISA = Defense Information Systems Agency GCCS = Global Command and Control System GCCS-T = Global Command and Control System-Trusted K = thousand LAN = local area network MLS = multilevel security MNS = multinetwork system NIPRNet = Nonsecure Internet Protocol Router Network

Chapter Six

Business Processes: The Balancing Act

Sharing and security represent recurring and nonrecurring costs for technology, administration, personnel, and infrastructure. Organizations need to assess, prioritize, and weigh IS&S requirements against other business requirements. They need an approach to management of IS&S that is both inclusive—whose scope truly reflects the potential contribution of information—and specific. To be meaningful to business managers, the management concept for IS&S should go beyond attractive theories to specific, business-related measures. To do this, IS&S should be formulated in terms of business value and brought directly into the business management process (see **Figure 6-1**).

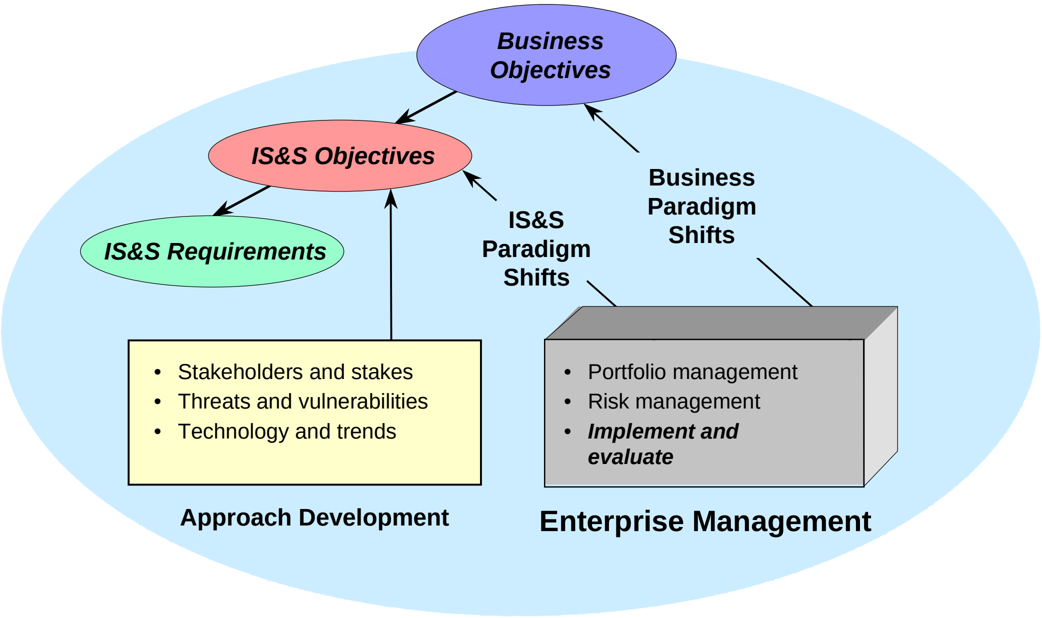


Figure 6-1

Bringing the IS&S Approach into the Organization

Adapting the concepts of IT presented by Peter Daly and Charles Popper allows the inference that a core barrier remains.[1] Despite efforts to develop guiding principles for

[1] See Peter H. Daly, *Soldiers, Constables, Bankers, and Merchants: Managing National Security Risks in the Cyber Era* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-3, June 2000), 32–34, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/daly\daly-p00-3.pdf; and Charles Popper, *A Holistic Framework for IT Governance* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-00-1, January 2000), Chapters Two and Four, [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/popper\popper-

management of the IS&S function, most organizations have not yet attained the alignment and integration between business and IT they aspire to. Senior managers often lack a clear understanding of how good decisions about IS&S can contribute to the success of their organization; even more often, they cannot reconcile the growing costs of IT with their perception of the value received.

Security advisors and IT advocates also need to understand that the organization does not have infinite resources. They need to present options with different levels of cost and effectiveness. If the recommendations avoid all-or-nothing approaches and ensure that decisionmakers are fully informed about the vulnerabilities and urgency associated with each proposal, senior management will be able to balance IS&S requirements within the larger business context.

Instituting well-defined evaluation programs, managing security and sharing efforts as portfolios (i.e., in an integrated way), and incorporating IS&S into the overall organization risk management scheme may be keys to successful balancing of IS&S.

6.1 Portfolio Management

IS&S efforts are laced with interdependencies. Often, the success of one mitigation approach depends directly on the success of another. Changes to the schedule, technology, or functionality of one approach can drive changes to others. Portfolio or integrated management of IS&S may alleviate problems resulting from implementation dynamics. If the organization's ability to share certain information or accept certain information partners depends on a security mechanism, portfolio management may be beneficial.

The proposed framework may help organizations to determine the best portfolio of overall business investments by easing systematic comparison of the costs and benefits of candidate projects. The framework can identify the best approaches to sharing and security for an information product and indicate the likely costs involved. In fact, the "best" IS&S approach may be prohibitively expensive and may lead an organization to decide against implementing an otherwise promising information product in favor of another type of product or service.[2]

IS&S implementations often affect the business culture and create the need to consider awareness, training, technology, policies, and procedures (see section **2.1**). The operational community cannot properly share and secure information without the security community, and neither community can properly do its work without the support (systems developers and maintainers) community. Security implementations may not only constrain operations but may

p00-1.pdf The discussion in the next three sections of portfolio management, risk management, and evaluation is based on detailed information provided by Daly and Popper.

[2] Charles Popper, personal communication to the author, Dec. 7, 2000.

also incur costs related to support staff (ADP, training, and development), security staff, acquisition, and system resources (bandwidth, computing power, data duplication, procedures, and processes). A security strategy should address communications, computer, and operational security.

6.2 Risk Management

> *The advent of the information age will require, as never before, that* [the DOD] *take a wider perspective and avoid stovepipes that blind us to changes taking place outside our own sphere of direct responsibility*.[3]

What should an organization be willing to give up to support IS&S: information sharing efficiency, information sharing effectiveness, customer trust, security risks, or partnership relations? After pulling together the results of the trend analysis, assessing the current approach, and identifying areas of improvement, an organization needs to propose changes to its IS&S approach. Programmatic changes, which are usually the most economical, reflect ways to improve the approach, perhaps by automating some tasks. Evolutionary changes reflect a natural progression of the approach to account for changes in technology or environment. Revolutionary changes, often the most risky, reflect fundamental ways to change how an organization carries out IS&S. Charles Popper provides additional insight and mechanisms into evaluating and portraying such changes.[4]

IS&S has the potential to change or prohibit the changing of basic business functions and can have a potentially far-reaching effect on an organization. For this reason, only the appropriate level and amount of involvement of senior business management can determine the success of the IS&S approach.[5] The goal is to instigate informal dialogue and formal decisionmaking. Ongoing informal dialogue is needed for managers fully to understand the planned use of technology and its impact upon the organization and to elicit their guidance, feedback, and strategic insight. Formal decisionmaking helps to ensure that all groups in the organization are fully committed to critical decisions. Finally, senior managers are often best qualified to assess progress toward achieving the desired business value.

Although there are many proven techniques to involve management in IS&S, according to Popper they all boil down to a few common principles. First, the senior managers—preferably an existing management committee or, if necessary, a dedicated IS&S committee—needs to accept

[3] Andrew W. Marshall, “Foreword,” in *Strategic Appraisal: The Changing Role of Information in Warfare*, edited by Zalmay M. Khalilzad and John P. White (Santa Monica, Calif.: The RAND Corp., 1999), 2, [On-line]. URL: http://www.rand.org/publications/MR/MR1016/ (Accessed Feb. 27, 2001.)

[4] Popper, *A Holistic Framework*, Chapter Four.

[5] The point that “senior executive support is critical” to discussions of information security is highlighted in GAO, *Information Security Management: Learning from Leading Organizations*, Executive Guide (Washington, D.C.: U.S. General Accounting Office, GAO/AIMD-98-68, May 1998), 35.

formal responsibility for strategic decisions regarding IS&S. Second, they must agree on processes to identify the decisions to be made; to collect, analyze and disseminate the data needed to make informed decisions; and to make and communicate decisions. In principle, the processes need not differ from those used to manage all aspects of the business. Third, the senior managers need to remain involved on a regular basis, not merely after a disaster to a project. They need to take the initiative in setting priorities and establishing and revisiting strategies. Today's business world is far too dynamic to implement strategy by remote control. The life cycle of a typical IT project often exceeds that of the underlying business strategy. Hence, the vigilance and participation of upper or senior management are essential.[6]

To use the GCCS as an example, the global command and control (GCC)/global combat support (GCS) management structure provides a forum for development and implementation of an IS&S approach. The GCC/GCS Advisory Board is composed of senior-level stakeholder representatives and chaired by the warfighting communities—the major stakeholders for command and control. The charters of the GCC Advisory Board, GCC Review Board, and GCC Requirements Board need to be modified to move information security requirements out of the category of technical requirements, which is prioritized and funded separately, and into the category of functional requirements.

6.3 Assessments

Because IS&S has many facets, assessment of IS&S approaches also needs to be many faceted to be useful. First, the organization needs to conduct the technical feasibility assessment: "Is the approach doing what it was designed to do?" Next comes the business value assessment: "Do the benefits justify the costs?" Third, assessment of the impact on business culture: "Have changes in the IS&S approach changed how we do business, or do changes in how we do business require changes to the IS&S approach?"

Assessments of technical factors and returns on investment are fairly common, well-documented activities for individual efforts at development and implementation. Assessments of business value across the whole IS&S approach are less common and less straightforward. Even rarer are successful assessments of the impact of the IS&S approach on the business culture. But the last two activities can capture the true impact of the approach on the organization and also become the evaluation that senior management may best understand.

To use the example of antivirus software, information security staff could collect information on the number and types of viruses encountered on the organization's information infrastructure; details on the software's performance; and cost data, including the costs to procure, implement, maintain, and operate the software. The staff could then analyze that information in relation to actual or projected loss of productivity, clients, or other business factors caused by

[6] Popper, *A Holistic Framework…*, 11.

computer viruses. The business value CFS (see **Chapter Four**) demand that an organization assess integrated, or portfolio, approaches (see section **6.1**) correlated with each objective, which allows analysis of progress toward overall business objectives and business value. Such assessments may lead to discoveries. For instance, implementation of antivirus software may allow the organization to relax the ban on employees' bringing diskettes in from home, or antivirus software might prove ineffective because of a failure in the associated security awareness effort.

The framework could have another, especially important role in the context of business value. By drawing attention to the vulnerabilities associated with a planned information product, it might help organizations to decide whether to create the product at all. In some cases, the potential for misuse of information might outweigh the probable benefits, or the dollar costs of protecting the information might exceed the expected profits or savings from making the information available. For example, a database available on a corporate intranet that lists an organization's R&D targets or its clients in a given income bracket could save time for staff members engaged in strategic planning or customer outreach. It could also represent a single and highly valuable entry point to business-critical information. Hedging the database with multiple security methods would protect the information from most competitors, but this approach could be costly, could reduce the database's usefulness to employees with a legitimate need to know the information, and could be useless against a malicious insider.

The framework could also point out aspects of a new product that might require employee training. As the Iran-Contra affair (1983–88) and the more recent antitrust suit against Microsoft (1997–2001) show, the convenience of retaining electronic messages might well be outweighed by the potential damage if the correspondence were brought to light in a legal proceeding. An organization might therefore need to provide guidelines not only on the retention of e-mail but also on the types of information not to include in electronic correspondence.[7]

Given the speed of change in business practices, identifying and capitalizing on new business techniques can be an important part of a new risk-based business model. Taking the assessment to the next step—examining effects on business culture—has a twofold result: it prompts organizations to look for expected revolutionary effects and helps them to find unexpected ones.

6.4 Summary

The proposed framework for balancing information sharing against information security can help organizations to develop an IS&S approach rooted in how and why organizations do business. Creating the framework impels organizations to link their IS&S objectives to their

[7] Charles Popper, personal communication to the author, Dec. 7, 2000.

business objectives, to recognize the essential role of business value, to develop an IS&S approach (by examining and weighing influences and options) based upon that value, and then to manage and evaluate IS&S efforts from an organizational perspective (see **Figure 1-1**). The framework, which spans the modeling process and associated tools and concepts, uses business value as both the driving force for IS&S decisions and the standard by which an organization can measure success.

Balancing sharing and security is an art, because decisionmakers often need to resolve previously unrecognized dichotomies. For example, as noted in section **5.3.1**, they need to weigh the profits to be expected from sharing information against the costs of security. They must determine the most appropriate balance between making information available and protecting sensitive information, bearing in mind that perfect security cannot be achieved. They must also recognize that people—in many cases their own staff—represent both their greatest asset and their greatest threat to security.

The framework proposed in this report is only a foundation for individual action. Its effectiveness will be determined, not by the diligence and rigor with which an organization applies the concepts and tools, but by the skill and finesse an organization uses in adapting the framework to its own culture and needs.

Appendix

The PDD and GCCS Environments

A.1 PDDs 62 and 63

> *As we approach the 21st Century, our foes have extended the fields of battle from physical space to cyberspace; from the world's vast bodies of water to the complex workings of our own human bodies. Rather than invading our beaches and launching bombers, these adversaries may attempt cyber attacks against our critical military systems and our economic base.*
>
> President William J. Clinton, May 22, 1998[1]

> *Computers are changing our lives faster than any other invention in our history. Our society is becoming increasingly dependent on information technologies, which are changing at an amazing rate..…We must ask whether we are becoming so dependent on communications links and electronic microprocessors that a determined adversary or terrorist could possibly shut down federal operations or damage the economy simply be attacking our computers.*
>
> Senator Fred Thompson (Rep.-Tenn.),
> May 19, 1988[2]

PDDs 62 and 63 require unprecedented cooperation by federal, state, and local government entities and the private sector. To a large extent, PDD 62 mandates interconnections among organizations in all these spheres to support sharing of information about terrorism and responses to it. PDD 63 requires government and industry to establish a supporting network to protect the NII by enabling an exchange of information regarding potential and actual attacks and appropriate responses.

Information needs will continue to broaden and efforts to manage information will overlap and duplicate each other. The increased demand comes at a time when critical information resources are at a premium, pushed to the point where the burdens of collecting, analyzing, and disseminating information should be shared. Given this background, how can participants protect the critical NII?

[1] Quoted in Zalmay M. Khalilzad and John P. White, editors, *Strategic Appraisal: The Changing Role of Information in Warfare* (Santa Monica, Calif.**:** The RAND Corp., 1999), 7, [On-line]. URL: http://www.rand.org/publications/MR/MR1016/ (Accessed Feb. 27, 2001.)

[2] Ibid.

A.1.1 Background

Executive Order 13010, dated July 15, 1996, established the President's Commission on Critical Infrastructure Protection (PCCIP) to examine eight sectors for security vulnerabilities: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. In response to the PCCIP, President Clinton signed PDD 62, Combating Terrorism, and PDD 63, Critical Infrastructure Protection, on May 22, 1998. The initial plan for implementation of PDD 63 was published in January 2000. Both directives were designed to defend the nation's critical infrastructure from various threats, including "cyber attacks" by computer hackers and terrorists.

The two PDDs call for new levels of cooperation and partnerships by federal, state, and local governments, as well as local responders and the private sector in accomplishing their respective tasks. For either PDD to succeed, the participating entities will probably need to establish some type of intranet, similar to the intelligence community's Intelink, to accommodate the information sharing required. This report has focused on the IS&S aspects of establishing interactions among agencies, departments, and organizations to support antiterrorism and infrastructure protection efforts.

A.2 The Joint Command and Control Infrastructure

Within the context of command and control, the DOD has devoted extensive discussion to such topics as information warfare, interoperability, battlespace dominance, rapid response, integration of air and space assets, and combined information operations. What is missing is a clear, comprehensive, and workable approach to IS&S. Will the approach to security of the DOD's joint command and control infrastructure meet the needs of tomorrow? No document, other than a few writings on data encryption and other specific solutions, addresses how the security environment of today will evolve to meet the DOD's information sharing demands for 2010.

The DOD shares information by classifying data as SECRET, TOP SECRET, and UNCLASSIFED and then mandating processes and procedures for labeling, handling, protecting, sharing, and accessing information. The GCCS ADP system realizes this concept in the form of separate networks at the classification levels. The situation facing GCCS would arise in any organization in which some data can be shared with only a subset of the company (e.g., data on personnel, customers, salaries, etc.), but some individuals (chief executive officers, network administrators, etc.) need access to more than one pool of data. The issues are complicated by the growing diversity, in mission and geography, of organizations in today's networked environment.

A.2.1 Background

> *[T]he information "dimension" increasingly becomes central to the outcome of battles and campaigns. Therefore, protecting the effective and continuous operation of one's own information system and being able to degrade, destroy, or disrupt the functioning of the opponent's information system will become a major focus of the operational art.*[3]

For clarity here, the term GCC is used to refer to the people, processes, procedures, tools, methods, and information involved in global command and control, whereas GCCS is used to refer to the ADP-based information infrastructure and information system supporting GCC. Both *Joint Vision 2010*[4] and the GCC concept of operations designate GCCS as the single command and control system for joint operations. GCCS comprises over 700 sites with more than 10,000 workstations and holds information on current operations, situational awareness, weather, intelligence, logistics, operations planning, unit correspondence, DOD messages, and systems administration. At the joint level alone, GCCS uses four separate networks for command and control on a daily basis—GCCS-SECRET; GCCS-TOP SECRET; a North American Aerospace Defense version of GCCS that allows access by Canada, and the Internet (UNCLASSIFIED), used heavily for logistics, communications with reserve and National Guard forces, and contact with agencies outside of the DOD, including contractors and support organizations. Staff with TOP SECRET clearance need to access three different networks, using three different workstations, logins, and passwords, to see all the planning, logistics, or operational data pertaining to their jobs. Some military units have access only to a single network, and no single network connects all the units.

The DOD lacks a formal, overall IS&S approach. Given that, and in the interest of brevity, an examination of the perceived difference between the labeling of the hard copy and electronic information bundlings can illustrate the necessary concepts. At the architectural level, statutes and DOD regulations provide the high-level framework needed for labeling information classifications. The NSA's accreditation guidance documents, DISA's electronic data-labeling documents, and other DOD documentation retain the DOD's traditional preference for at least paragraph-level labeling of information classification. Despite this, the electronic versions contain no explicit labeling, and the level of data security is implied by the security classification of the ADP system in which the information resides. To promote accessibility and availability, most classified networks contain information at many security classifications, up to and including the highest level permitted by the system. This situation came about because no adequate or economically feasible approaches to electronic data labeling were available. The private sector

[3] Andrew W. Marshall, "Foreword," in *Strategic Appraisal*, 4–5.

[4] Chairman, Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.: Office of the Chairman, Joint Chiefs of Staff, n.d.), [On-line]. URL: http://www.dtic.mil/jv2010/jv2010.pdf (Accessed Dec. 7, 1999.)

has frequently taken a similar approach, particularly in e-commerce and e-business, but also in basic business environments.

A.3 Getting Technical

A.3.1 Confidentiality Levels

Categorizing information indicates the desire to limit access to or exposure of the information. The government uses the term *security classification* and the labels UNCLASSIFIED, SECRET, and TOP SECRET, along with a book full of caveats, downgrading instructions, and rules, to indicate confidentiality levels of information. Business uses such terms as PROPRIETARY, CONFIDENTIAL, and DEPARTMENTAL USE ONLY to indicate the need for special handling of information.

A.3.2 Data Marking and Labeling

The term *data marking* is used to mean placing a human-readable label of confidentiality on information, whether by putting a stamp on the page or by putting the data in a special folder. *Data labeling* is generally used to refer to the electronic counterpart of data marking.

A.3.3 Multiple Network Security

A multiple network security (MNS) approach involves networks at various classification levels strategically interconnected by secure computing devices. Although each network is at a single classification level, users can access and change information on their own intranet and see selected information on intranets at lower classification levels. Any data added or modified enter the network at the classification level of the higher intranet. A separate step is required to downgrade data, if appropriate and desired.[5] Three types of technology are available for such an implementation: secure gateways, firewalls, or guards[6] and multilevel security (MLS) data servers.

Firewalls and guards control the flow of information between networks. With firewalls, the user (or an automated agent on behalf of the user) travels onto another network and retrieves the information. With secure data servers, information at various classification levels resides on the server (see **Figures A-1** and **A-2**). The secure server allows authorized users to see information from the lowest classification level up to and including the classification level of the intranet

[5] Downgrading data means lowering the classification level; reclassifying data means changing the compartment or country releasability markings of data

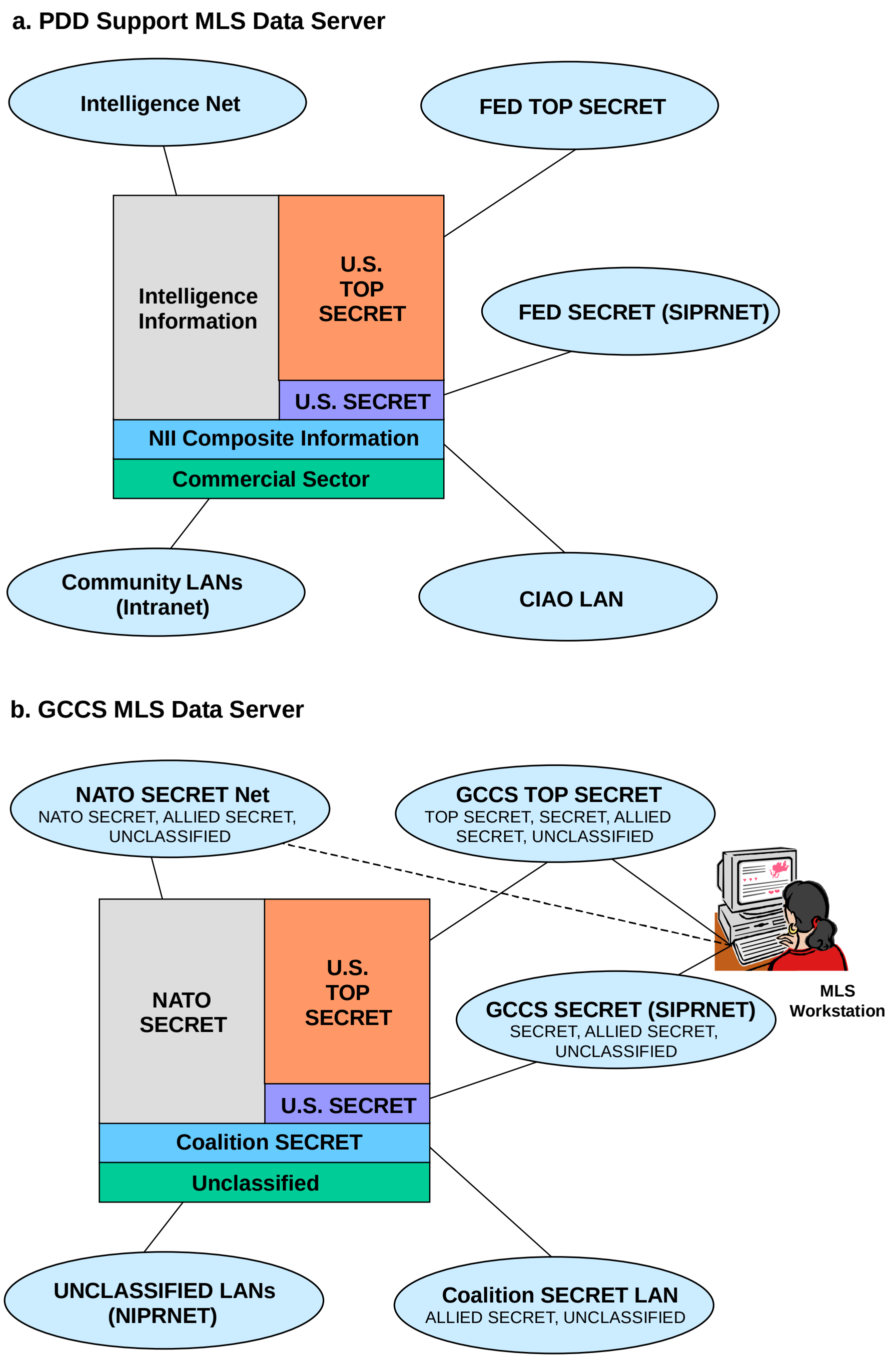
[6] Guards, as currently accredited, prohibit network traffic and implement information flow by transferring files or certain types of e-mail/message traffic. By contrast, firewalls filter network traffic, but still allow it to pass. Linda M. Schlipper, Trusted Computer Solutions, Inc., personal communication to author, Dec. 15, 2000.

through which the user entered the server (“read down” approach). The user cannot see data at other equal or higher classification levels (no side or “up” look). Data entered by a user are labeled at the security level of the network, and a separate step is required for the user to downgrade the data. Information destined for or going from the data server is not required to travel on a network outside the user’s intranet; all data requests and communications occur between the user’s workstation and the data server. A distributed database may exist at a particular security level, in which case the two data servers communicate to access or store distributed data.

A.3.4 Multilevel Security

An MLS network simultaneously supports many levels of information and many users with varying levels of confidentiality, all with reasonable trust that unintended exposure of information will not occur. The step to MLS requires the ability to secure intranet communications so that workstations of varying classification levels can function on the same network.[7]

[7] See Norman E. Proctor and Peter G. Neumann, “Architectural Implications of Covert Channels,” in *Proceedings of the Fifteenth National Computer Security Conference* (Menlo Park, Calif.: SRI, Inc., October 1992), 28–43, [On-line]. URL: http://csl.sri.com/neumann/ncs92.html (Accessed November 8, 2001.)


a. PDD Support MLS Data Server

b. GCCS MLS Data Server

NATO SECRET Net
NATO SECRET, ALLIED SECRET, UNCLASSIFIED
GCCS TOP SECRET
TOP SECRET, SECRET, ALLIED SECRET, UNCLASSIFIED
NATO SECRET
U.S. TOP SECRET
GCCS SECRET (SIPRNET)
SECRET, ALLIED SECRET, UNCLASSIFIED
MLS Workstation
U.S. SECRET
Coalition SECRET
Unclassified
UNCLASSIFIED LANs (NIPRNET)
Coalition SECRET LAN
ALLIED SECRET, UNCLASSIFIED

Figure A-1

MNS Server: Conceptual Examples

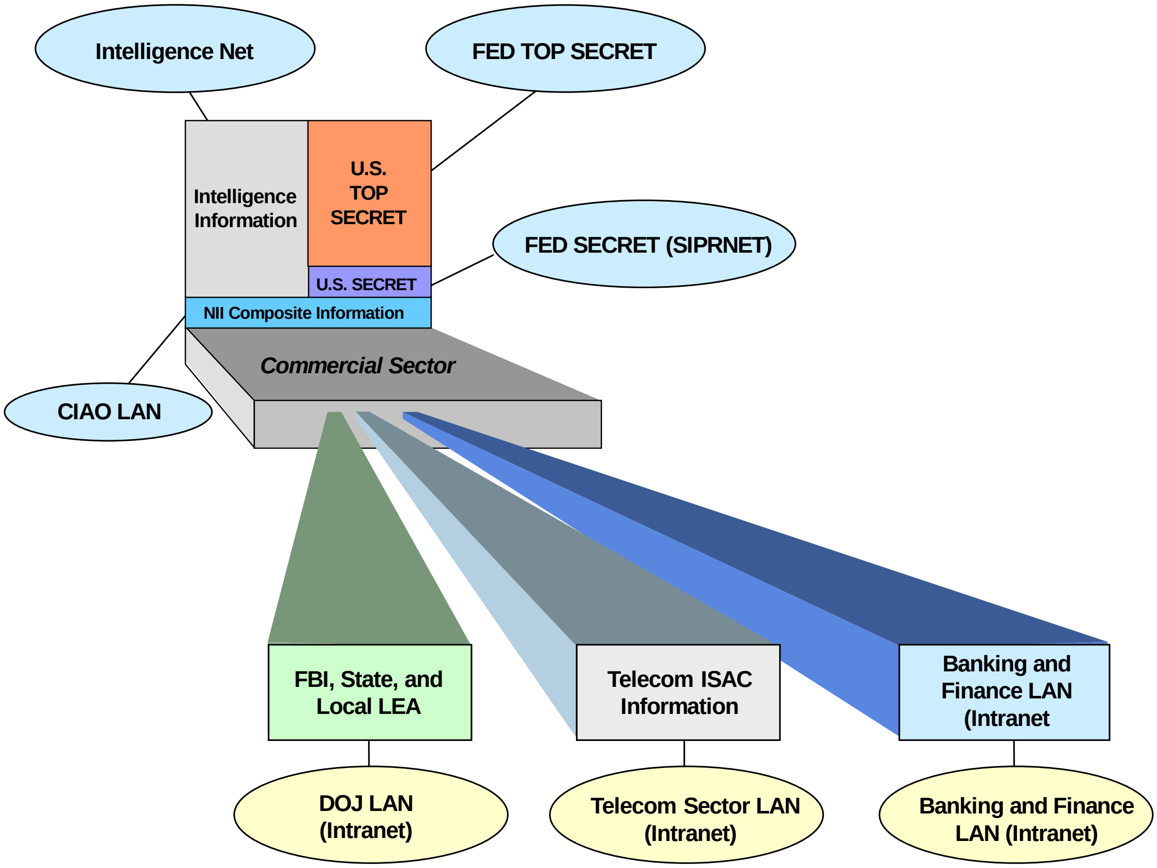


Figure A-2

Example of PDD Intranets: Detailed

Acronyms

ADP	automated data processing
CFS	criteria for success
CSOD	Current Situation Operations Division
CSS	Central Security Service
DBMS	database management system
DISA	Defense Information Systems Agency
DOD	Department of Defense
DOS	denial of service
GAO	General Accounting Office
GCC	global command and control
GCCS	Global Command and Control System
GCS	global combat system
GCSS	Global Combat Support System
INFOSEC	information security
IS&S	information sharing and security
IT	information technology
JCS	Joint Chiefs of Staff
LAN	local area network
MLS	multilevel security
MNS	multiple network security
MOP	measure of performance
NDP	National Disclosure Policy
NII	National Information Infrastructure
NSA	National Security Agency
OPSEC	operational security
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
URL	Uniform Resource Locator