Chapter 2

What Is Information Assurance, How Does It Relate to Information Security, and Why Are Both Needed?

This chapter explains what information assurance (IA) is, how it relates to information security, and why both are needed. To begin, IA is defined in terms of what it involves and what it accomplishes. Next, the application and technology domains in which information security/IA should be implemented are explored. Finally, the benefit of information security/IA to individuals and organizations is illustrated from the perspective of the different stakeholders. The interaction between information security/IA and infrastructure systems is illustrated throughout the chapter.

2.1 Definition

The first standardized definition of IA was published in U.S. DoD Directive 5-3600.1 in 1996:

> Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, and nonrepudiation; including providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

This definition provided a good starting point in that it recognized the need for protection, detection, reaction, and restoration capabilities. However, it is too narrow in scope.

This book proposes a broader definition of IA:

> An engineering discipline that provides a comprehensive and systematic approach to ensuring that individual automated systems and dynamic combinations of automated systems interact and provide their specified functionality, no more and no less, safely, reliably, and securely in the intended operational environment(s).

A broader definition of IA is needed for the following reasons. First, the definition proposed by this book uses the term "automated systems" rather than "information systems." Automated systems encompass a broader range of systems and technology, consistent with the infrastructure systems identified in Chapter 1 and later in this chapter. Automated systems include systems employing embedded software or firmware and performing critical control functions. In this context, information can take many forms beyond the alphanumeric information associated with information systems; for example, a control sequence that stops a subway train, opens a bridge, or shuts down a power distribution hub. All types of information and systems need the protection provided by IA.

Second, the definition of IA proposed in this book incorporates individual systems and dynamic combinations of systems. Many automated systems are dynamically connected and configured to operate in tandem, series, or parallel, to accomplish specific tasks. This combination of systems may include traditional information systems as well as other types of automated systems. The specific systems connected, the duration of the connection, the operational modes, scenarios, and dependencies change frequently. The dynamic reconfiguration can occur as part of a new capability or service or in response to the execution of a contingency plan. Dynamic combinations of disparate geographically dispersed systems is the norm rather than the exception in today's technology landscape.

The 1991 Gulf War has often been called the first information war. In many ways, the Gulf War was the harbinger of IA. The ability to rapidly integrate commercial and military information technology from multiple companies and countries and the ability to dynamically reconfigure it was critical to the success of the Allies. As Toma[430] reports:

> *The communication network that supported Operation Desert Storm was the largest joint theater system ever established. It was built in record time and maintained a phenomenal 98 percent availability rate. At the height of the operation, the system supported 700,000 telephone calls and 152,000 messages per day. More than 30,000 radio frequencies were managed to provide the necessary connectivity and to ensure minimum interference.*

The Gulf War also presented another unique technological situation. It was the first time journalists (audio, video, and print) provided near-real-time reporting. This led to competition between the military and the journalists for the (fixed) capacity of commercial satellite networks and the intrinsic security vulnerabilities of this arrangement.[235]

Third, more robust properties are needed than availability, integrity, authentication, and nonrepudiation if a system is to meet its IA goals. These properties by themselves are important but incomplete. A more complete set of system properties is provided by combining safety, reliability, and security. For example, authentication and nonrepudiation are two of many properties associated with system security. Likewise, availability is one of many properties associated with system reliability. A safe, reliable, and secure system by definition has proactively built-in error/fault/failure (whether accidental or intentional) prevention, detection, containment, and recovery mechanisms.

IA is a three-dimensional challenge; hence, the problem must be attacked from all three dimensions — safety, reliability, *and* security. Safety and reliability vulnerabilities can be exploited just as effectively, if not more so, as security vulnerabilities, the results of which can be catastrophic. As Neumann[362] notes:

> *…many characteristic security-vulnerability exploitations result directly because of poor system and software engineering. … Unfortunately, many past and existing software development efforts have failed to take advantage of good engineering practice; particularly those systems with stringent requirements for security, reliability, and safety.*

Historically, safety, reliability, and security engineering techniques have been applied independently by different communities of interest. The techniques from these three engineering specialties need to be integrated and updated to match the reality of today's technological environment and the need for IA. As Elliott states[256]:

> *…although safety-related systems is a specialized topic, the fruits from safety-related process research could, and should, be applied to support the development of system engineering and the management of other system properties, such as security and reliability.*

It is the synergy of concurrent safety, reliability, and security engineering activities, at the hardware, software, and system levels, that lead to effective information security/IA throughout the life of a system. Gollmann[277] concurs that:

> *…similar engineering methods are used in both areas. For example, standards for evaluating security software and for evaluating safety-critical software have many parallels and some experts expect that eventually there will be only a single standard.*

2.2 Application Domains

Information security/IA is essential for mission-critical systems, business-critical systems, and infrastructure systems. In fact, there are very few automated systems today that do not require some level of information security/IA. The decade following the Gulf War led to an awareness of the all-encompassing nature of information security/IA. As Gooden[279] observes:

> *Today we see a reach for maximum bandwidth to support a global telecommunications grid, moving terabits of voice, data, images, and video between continents. But in many cases, the grid has a foundation of sand. It continues to be vulnerable to service disruption, malicious destruction or theft of content by individuals, criminal cabals, and state-sponsored agents. The threat is as real as the growing body of documentation on bank losses, service disruptions, and the theft of intellectual property.*

An infrastructure system is defined as[176,178]:

> A network of independent, mostly privately owned, automated systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services.

As mentioned in Chapter 1, the eight categories of infrastructure systems identified in PDD-63 are:

1. Telecommunications systems
2. Banking and financial systems
3. Power generation and distribution systems
4. Oil and gas distribution and storage systems
5. Water processing and supply systems
6. Water, air, and ground transportation systems
7. Emergency notification and response systems
8. Systems supporting critical government services

These eight categories represent a wide range of technology. Each of the eight infrastructure systems is critical. Furthermore, there is a high degree of interaction and interdependence among the eight, as shown in Exhibit 1. For example, banking and financial systems are dependent on telecommunications and power generation and distribution, and interact with emergency systems and government services. It is interesting to note that all infrastructure systems: (1) are dependent on telecommunications systems, and (2) interact with emergency systems and government services.

Exhibit 2 illustrates the interaction and interdependency between infrastructure systems, mission-critical systems, and business-critical systems. Together, these sets of systems constitute essentially the whole economy. Again, there is a high degree of interaction and interdependence. All of the mission-critical systems and business-critical systems are dependent on telecommunications,

Exhibit 1 Interaction and Interdependency Among Infrastructure Systems

Infrastructure System	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1. Telecommunications	—	I	D	I	I	I	I	I
2. Banking and finance	D	—	D				I	I
3. Power generation and distribution	D	I	—	I	D	I	I	I
4. Oil and gas distribution and storage	D	I	D	—		D	I	I
5. Water processing and supply	D		D		—		I	I
6. Transportation systems	D	I	D	D	I	—	I	I
7. Emergency systems	D	I	D	D	D	D	—	I
8. Government services	D	D	D	D	D	D	I	—

Note: D - dependent on infrastructure system; I - interacts with infrastructure system.

Exhibit 2 Interaction and Interdependency Between Infrastructure Systems, Mission-Critical Systems, and Business-Critical Systems

Mission-Critical/Business-Critical Systems	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
9. Wholesale/retail business systems	D	D	D	D	D	D	I	
10. Manufacturing systems	D	D	D	D	D	D	I	
11. Biomedical systems	D	D	D		D	D	I	I
12. Postal/package systems	D	D	D	D		D	I	I
13. Food production and distribution systems	D	D	D	D	D	D	I	I
14. Entertainment, travel systems	D	D	D		D	D	I	
15. News media, broadcast, and publishing systems	D	D	D			D	I	I
16. Housing industry systems	D	D	D	D	D	D	I	
17. Education, academic systems	D	D	D		D	D	I	I

Note: D - dependent on infrastructure system; I - interacts with infrastructure system.

banking and financial, power generation and distribution, and transportation systems. They all interact with emergency systems. Campen[231] notes some the ramifications of this interdependency:

> *Major reorganizations are taking place within the (U.S.) Departments of Defense and Justice to provide policy and leadership to defend critical infrastructures. The White House describes these infrastructures as essential to the minimum operations of the economy and the government.*

2.3 Technology Domains

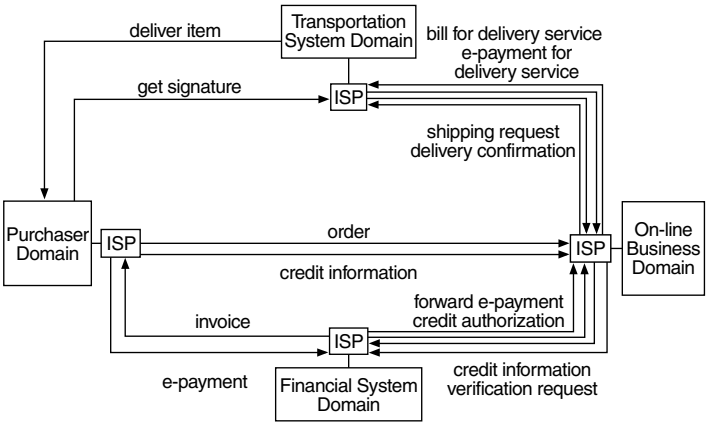
Information security/IA applies to all technology domains; in fact, it is difficult to talk about a technology domain to which information security/IA does not apply. In terms of hardware, information security/IA is applicable to computer hardware, communications equipment, communications lines — terrestrial and wireless, power grids, and other connected equipment within the operational

environment. In terms of software, information security/IA is applicable to all layers of the International Organization for Standardization (ISO) open systems interconnection (OSI) and TCP/IP communications reference models, from the physical layer through the application layer. Common examples of information security/IA technology domains include military computer communications command control and intelligence (C^4I) systems, manufacturing process control systems, decision support systems, e-Commerce, e-mail, biomedical systems, and intelligent transportation systems (ITS). To illustrate, Barber[208] has identified the following information security/IA concerns related to medical informatics:

1. Clinical implications of data reported
2. Loss of medical records, subrecords, or data items
3. Unauthorized or accidental modifications of data
4. Privacy of medical records
5. Misidentification — wrong record, person, treatment profile
6. False positive or false negative test results
7. Wrong treatment delivered
8. Malicious errors (nonprescribed/bogus therapies)
9. Accuracy and currency of information reported

In today's technological environment, it is rare for an individual or organizational user to own all of the equipment involved in a transaction. Instead, they own some basic equipment but rely on service providers from the infrastructure systems to do the rest. Consider when an item is purchased online. The purchaser owns the computer/modem, pays for local telephone service, and pays for an Internet service provider. The online business pays for the same equipment and services on their end. Both the purchaser and the online business are relying on the: (1) telecommunications systems to make the purchase possible; (2) banking and financial systems to approve/authenticate the purchase and payment; and (3) transportation systems to deliver the item(s) purchased to the purchaser and provide proof of delivery to the seller. The reliable and secure exchange of critical information, across many systems, in a timely manner is required to complete this transaction.

This scenario, which is depicted in Exhibit 3, illustrates some of the challenges for information security/IA. First, all of the systems within each of the four domains involved in the transaction (purchaser, online business, financial, and transportation) must function correctly. This may involve one or more geographically dispersed systems/components. Second, the transactions among these four domains must work correctly. Eleven high-level transactions are identified in the figure. However, this is only a subset of the total transactions involved. Other transactions include wholesale/retail exchanges, ordering packing materials, etc. Underpinning all of these transactions is reliable and secure telecommunications. To grasp the scope of the IA challenge, one needs to multiply the transactions involved in this one example by the total number of online purchases made simultaneously each day and each week. McGraw[349] sizes up the e-Commerce information security/IA challenge:



*Note: All of the systems rely on the power generation and distribution systems. The transportation system relies on the oil and gas distribution and storage system.

Exhibit 3 Illustration of the Technology Domains Involved in Information Assurance Using an Online Purchase as an Example

> *Data from Forrester Research indicates that e-Commerce, which totaled about $8 billion in 1998, will reach more than $327 billion in the U.S. by 2002 and will be four times that amount globally.*

2.4 Importance

IA affects nearly all aspects of the everyday life of individuals and organizations. As reported by Wood[442]:

> *The Presidential Decision Direction - 63 (PDD-63) … notes that infrastructures — energy, banking, finance, transportation, water systems, etc. — have historically been 'physically and logically separate with little interdependence.' Now they are increasingly linked together by, and absolutely dependent on, an information infrastructure that is vulnerable to technical failure, human error, natural causes, and physical and cyber attacks.*

IA has a pervasive role in today's technological society. This role can be divided into seven categories:

1. Human safety
2. Environmental safety
3. Property safety
4. Economic stability and security
5. Social stability
6. Privacy, both individual and corporate
7. National security

Exhibit 4 examines the role of IA in relation to the benefits provided, the beneficiaries, and the infrastructure systems that are required to be functioning correctly to achieve this benefit.

IA protects humans from death and injury by preventing accidental or intentional equipment failures and minimizing the consequences of potential failures. (The term "equipment" is used broadly to encompass anything that is automated or under computer control.) This protection benefits the individual, their family, and employer. The manufacturers, seller, and operator of the equipment also benefit because they avoid liability lawsuits.

Consider the following example. Three hundred and fifteen people were scheduled to board a flight to Chicago at 9 a.m. Due to a mechanical problem, the plane scheduled for that flight had to be unloaded immediately before takeoff. The airline had to:

1. Query its fleet database to locate a new plane that is available in the immediate vicinity.
2. Check the new plane's maintenance records/status to verify that it is air worthy and has adequate fuel and supplies.
3. Verify that the new plane will accommodate this number of passengers.
4. Verify that the original flight crew is trained/certified for this type of plane.
5. Coordinate with the local air traffic control system to bring the new plane to the gate and have the defective one removed.
6. Arrange to have baggage moved from the first plane to the second.
7. Coordinate with air traffic control systems locally and in Chicago to develop a new flight plan/schedule.
8. Update departure/arrival monitors at both airports.
9. Book passengers on later connecting flights, if necessary.
10. Accomplish all of this very quickly and pleasantly so that the passengers do not get rowdy and create another hazard.

Each of these steps depends on the accurate and timely processing of correct information across multiple systems, from the initial detection of the problem through booking new connecting flights. In this scenario, IA played a role in protecting human safety, environmental safety, and property safety. It also prevented economic disruption for the airline, passengers, and their employers.

This example is not far from reality. On January 6, 2000, WTOP News and National Public Radio reported that the air traffic control (ATC) system serving Washington National Airport and Dulles Airport was inoperative for three hours in the morning due to an "unknown" problem. Because no flights could land or take off at these two airports, all East Coast air traffic was essentially shut down. An additional four hours were required to clear the backlog. Apparently, a similar problem was experienced at Boston Logan Airport earlier that week. The Chicago example only involved one flight. The shutdown on January 6, 2000, involved several hundred flights.

Representatives to the U.S. Congress frequent Washington National and Dulles airports. As a result, any shutdown at these airports has visibility. That

Exhibit 4 The Importance of IA in the Real World

Information Assurance Role	*Benefit*	*Who Benefits*	*Infrastructure Systems Required*
Human safety	Protection from accidental and malicious intentional death and injury	Individuals Their families Their employers Manufacturer of equipment Seller of equipment Operator of equipment	Telecommunications Power generation Oil & gas Water supply Transportation Emergency
Environmental safety	Protection from accidental and malicious intentional permanent or temporary damage and destruction	Individuals Society as a whole Manufacturer, distributor, and operator of equipment	Telecommunications Power generation Oil & gas Water supply Transportation Emergency Government
Property safety	Protection from accidental and malicious intentional permanent or temporary damage and destruction	Property owner Property user Manufacturer Distributor	Telecommunications Power generation Oil & gas Water supply Transportation Emergency
Economic stability and security	Protection from economic loss, disruption, lack of goods and services	Individuals Society as a whole Financial institutions Wholesale, retail businesses Manufacturing Local, national, global trade	Telecommunications Banking & finance Power generation Oil & gas Water supply Transportation Emergency Government

Exhibit 4 The Importance of IA in the Real World (continued)

Information Assurance Role	*Benefit*	*Who Benefits*	*Infrastructure Systems Required*
Social stability	Protection from social chaos, violence, loss of way of life, personal security	Individuals Society as a whole	Telecommunications Banking & finance Power generation Oil & gas Water supply Transportation Emergency Government
Privacy a. Individual b. Corporate	a. Protection from identify theft, financial loss, intrusion into private life, character assassination, theft of intellectual property rights b. Protection from financial loss, loss of customers, theft of intellectual property rights	a. Individuals, their family, their employer b. Corporation employees, stockholders, business partners	Telecommunications Banking & finance Power generation Oil & gas Water supply Transportation Emergency Government
National security	Access to and disclosure of sensitive economic and other strategic assets is safeguarded	Individuals Society as a whole Neighboring countries Global trading partners Multinational corporations	Telecommunications Banking & finance Power generation Oil & gas Water supply Transportation Emergency Government

evening, one Representative asked, "How could this happen? — the air traffic control system is brand new." How? Because newness does not mean a system is safe, reliable, or secure; in fact, the opposite often is true.

IA plays a role in protecting the environment from accidental or intentional damage and destruction. An example is the nuclear power plant control and protection systems that notify operators of any anomalies and prevent the release of radiation into the atmosphere. IA also plays a role in protecting property, for example, monitoring equipment that prevents water or fire damage and notifies emergency response teams.

IA plays a critical role in maintaining economic stability and security. Business, industry, the financial markets, and individuals are dependent on the near-instantaneous, accurate, and secure processing and exchange of correct information across multiple systems worldwide. This capability sustains the global economy.

Human safety, environmental safety, property safety, and economic stability and security are all precursors for social stability. Hence, IA contributes to social stability. Given the vast quantity of information stored electronically about individuals and organizations and the advent of data mining techniques, IA plays a critical role in protecting privacy. Likewise, national security organizations, whether operating alone or within the context of multinational alliances, are totally dependent on the safety, reliability, and security provided through the discipline of IA.

2.5 Stakeholders

As one can see from the discussion above, all of us are stakeholders when it comes to IA, whether one is acting as an individual or as a member of an organization. This highlights the fact that the benefits of IA (or the vulnerabilities and threats encountered when IA is not implemented or implemented ineffectively) accrue from many different perspectives, including:

- Individuals and organizations
- Financial institution a, buyer, seller, financial institution b
- Equipment owners, operators, and manufacturers

In contrast, there are the (illegal or, at a minimum, unethical) benefits that an individual or organization accrues when they exploit vulnerabilities in a system.

Consider the purchase of this book. Exhibits 5 and 6 illustrate all the possible ways in which this book could be purchased — the potential transaction paths. In other words, the book could be purchased in person at a bookstore, over the Internet, over the phone, by mail, or by fax. These are the only five purchase options. Payment options are limited to cash, credit card, debit card, check, gift certificate, previous store credit, or corporate purchase order. (In this example, the cash must be obtained from an ATM.) The combination of a possible purchase method with a feasible payment mode results in a transaction path. Exhibit 7 correlates these transaction paths to

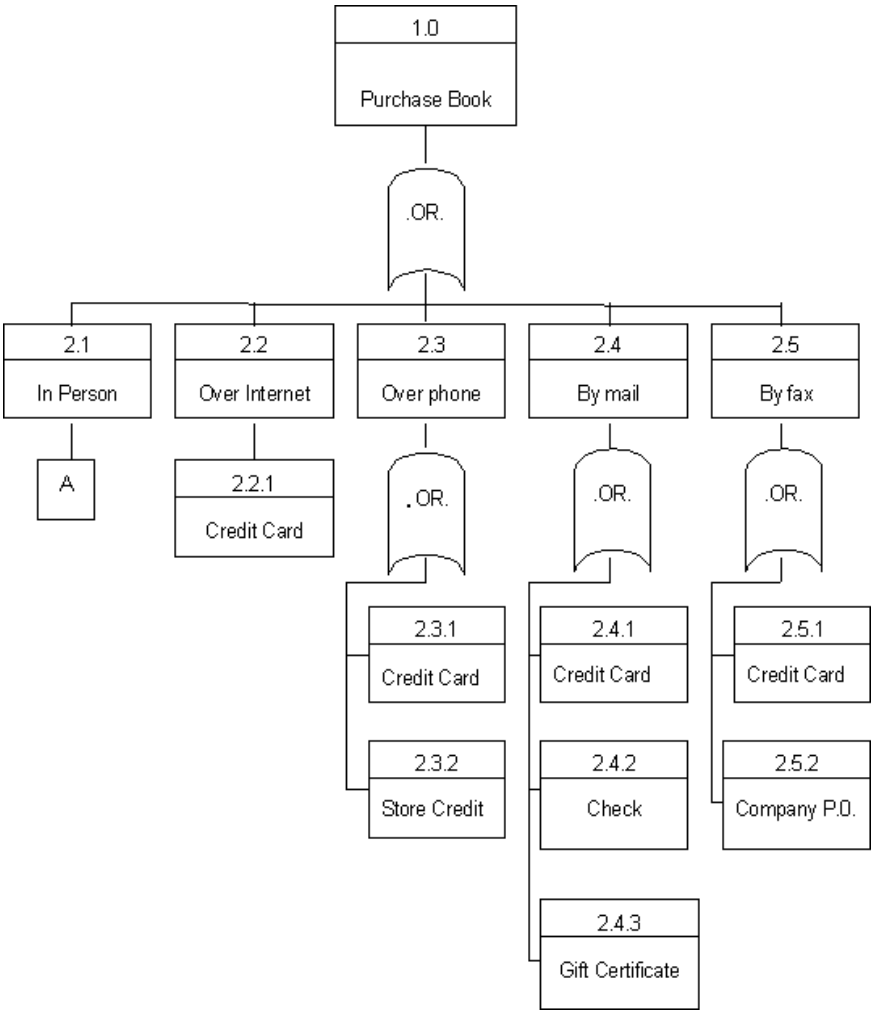


Exhibit 5 Sample Identification of Transaction Paths

vulnerabilities and threats, and identifies potential consequences to the different stakeholders. Different transaction paths may have the same or similar vulnerabilities, threats, and consequences. Hence, the set of transaction paths for which threat control measures are implemented represents a reduction of the original set. Likewise, the likelihood and severity associated with specific transaction paths must be analyzed prior to developing threat control measures. The process of analyzing transaction paths to identify critical threat zones is explained in Chapter 5.

This is a hypothetical example and for illustrative purposes, worst-case scenarios are developed. Many of these events may seem far-fetched. However, several similar events have actually occurred in recent years; examples include:

1. Examine the vulnerability/threat scenario for transaction path 1.0 ← 2.1.6.1a. In 1996 following an "upgrade" to ATM software, a major East

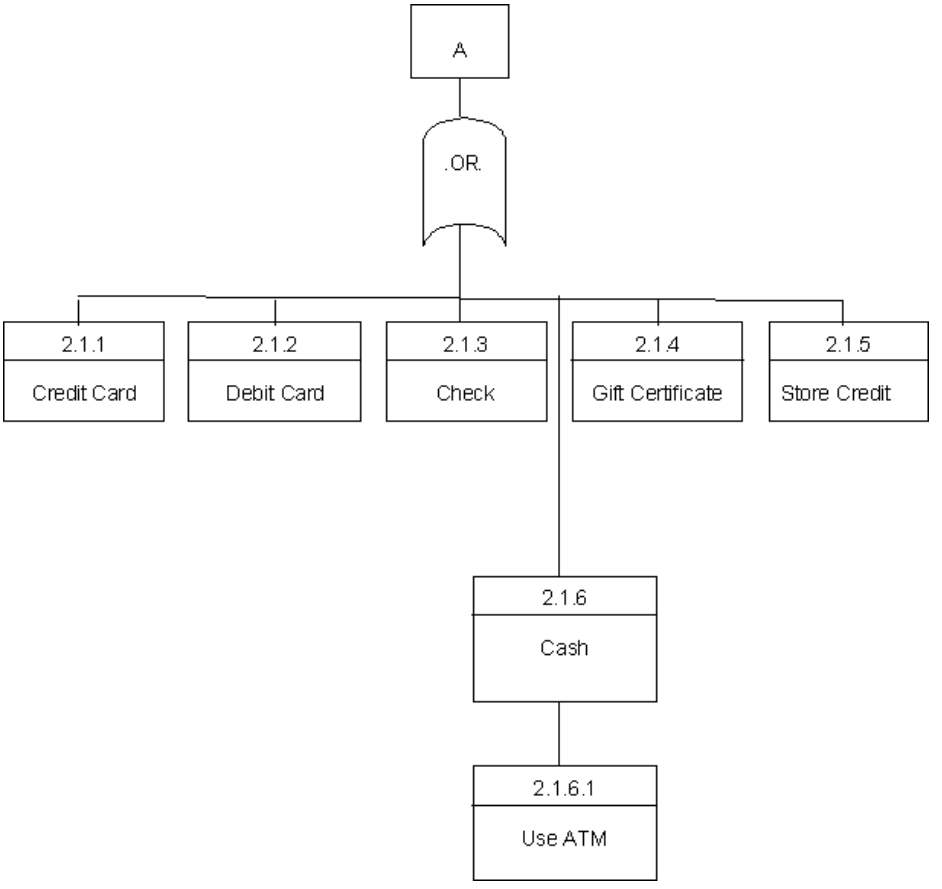


Exhibit 6 Sample Identification of Transaction Paths (continued)

Coast bank actually deducted twice the cash amount withdrawn from customer accounts. Needless to say, the customers were not happy.

2. The vulnerability/threat scenario for transaction paths 1.0 ← 2.1.4 and 1.0 ← All is similar to the Jewell situation following the 1996 Atlanta Olympics in which profiling resulted in erroneous information being reported to the news media, which then quickly spread worldwide. Jewell subsequently won several lawsuits related to character defamation.
3. The vulnerability/threat scenario for transaction path 1.0 ← 2.2.1.2a is similar to that reported by WTOP News and National Public Radio on January 10, 2000. In this incident, the credit card information, names, and addresses of 200,000 customers of an online business were stolen by a hacker. When the extortion payment was not made, information about 25,000 of the customers was posted on a Web site.
4. The vulnerability/threat profiling scenario (1.0 ← All) relates to the Monica Lewinsky affair. During the investigation/trial, a local Washington, D.C., bookstore was asked to provide a list of the books purchased and videos rented by Ms. Lewinsky. The bookstore admitted that it had the information but, despite the legal pressure, declined to provide it.

Exhibit 7 Sample Correlation of Vulnerabilities, Threats, Transaction Paths, and Consequences

Transaction Path	*Vulnerability*	*Threat*	*Consequences*		
			To Individual	*To Store*	*To Financial Institution*
1.0 ← 2.1.6.1	a. ATM software error	a. ATM returns correct amount of cash, but deducts twice the amount from your account.	a. You are unaware of the situation; bank account becomes overdrawn, checks bounce, and you incur fines; it takes 3 months to straighten out; credit report is damaged.		a. Loss of public confidence, customers; bad publicity.
	b. Remote ATM network has limited security.	b. ATM account and PIN numbers are intercepted.	b. Fraudulent ATM use.		b. Loss of public confidence, customers; bad publicity.
1.0 ← 2.1.1	a. Credit card number is stored in store's computer with your name and address.	a. Misuse of credit card information by store employee.	a. Fraudulent credit card use.	a. Loss of public confidence, customers; bad publicity; potential lawsuit.	
	b. Credit card information transferred over unsecured line for verification.	b. Credit card information intercepted and misused.	b. Fraudulent credit card use.	b. Loss of public confidence, customers; bad publicity. Potential lawsuit.	

	c. Software error in reconciling purchase.	c. You are billed for 9 other purchases that were made after yours.	c. Difficulty in proving you did not make these purchases; credit is tied up while situation is resolved; potential damage to credit history.	c. Unhappy customer notifies others; bad publicity.	c. Unhappy customer notifies others; bad publicity.
1.0 ← 2.1.2	a. Debit card information is stored in store's computer with your name and address.	a. Misuse of debit card information later by store employee.	a. Fraudulent debit card use.	a. Loss of public confidence, customers; bad publicity; potential lawsuit.	
	b. Debit card information is transferred over unsecured line for verification.	b. Debit card information intercepted.	b. Fraudulent use of credit card.	b. Loss of public confidence, customers; bad publicity; potential lawsuit.	b. Loss of public confidence, customers; bad publicity; potential lawsuit.
	c. Software error in reconciling purchase.	c. You are billed for 9 purchases that were made after yours.	c. Difficulty in proving you did not make purchases; account is tied up during resolution; possible damage to credit history.	c. Loss of public confidence, customers; bad publicity; potential lawsuit.	c. Loss of public confidence, customers; bad publicity.
1.0 ← 2.1.3; 1.0 ← 2.4.2	a. Unsecured line used to send/ receive information to check verification service	a. Account number and balance intercepted; account is drained.	a. You are unaware of the situation; bank account becomes overdrawn; checks bounce; you incur fines; it takes 3 months to straighten out; credit history is damaged.	a. Loss of public confidence, customers; bad publicity; potential lawsuit.	a. Loss of public confidence, customers; bad publicity; potential lawsuit.

Exhibit 7 Sample Correlation of Vulnerabilities, Threats, Transaction Paths, and Consequences (continued)

Transaction Path	*Vulnerability*	*Threat*	*Consequences*		
			To Individual	*To Store*	*To Financial Institution*
1.0 ← 2.1.4; 1.0 ← 2.4.3	a. Gift sales clerk preparing gift certificate makes a typo in the "from" section, typing XZY instead of XYZ.	a. Retail sales clerk notices that certificate is from XZY, a terrorist organization that has been in the news recently, and tells store manager, who calls the police.	a. You spend a few days in the clink because the person who can straighten this out is away on business; in the meantime, you lose your security clearance and hence your job; your name is all over the news media.	a. Store, media, and law enforcement officials face potential character defamation and other related lawsuits; bad publicity.	
	b. Gift sales clerk preparing gift certificate makes a typo in the "to" section, misspelling your last name.	b. Retail sales clerk thinks you are attempting to use the gift certificate fraudulently.	b. You endure a major hassle and/or end up forfeiting the value of the gift certificate.	b. Unhappy customers tell others; bad publicity.	
	c. Sales clerk preparing gift certificate makes a typo in the year.	c. Gift certificate was only good for one year; because it is "expired," you cannot use it.	c. You lose the value of the gift certificate.	c. Unhappy customers tell others; bad publicity.	
1.0 ← 2.1.5; 1.0 ← 2.3.2	a. Database containing store credit has been corrupted.	a. Your $50 store credit has been reduced to $5.00.	a. You have to prove the $50 credit or forfeit the $45.	a. Loss of public confidence, customers; bad publicity.	

	b. Database containing store credit is "busy" and not accessible right now.	b. Customers become annoyed and leave.	b. You have to come back later or use another payment option.	b. Loss of business.	
1.0 ← 2.2.1; 1.0 ← 2.3.1; 1.0 ← 2.4.1	a. Credit card number is stored in store's computer with your name and address.	a. Misuse of credit card information by store employee.	a. Fraudulent credit card use.	a. Loss of public confidence, customers; bad publicity; potential lawsuit.	
	b. Credit card information transferred over unsecured line for verification.	b. Credit card information intercepted and misused.	b. Fraudulent credit card use.	b. Loss of public confidence, customers; bad publicity; potential lawsuit.	
	c. Software error in reconciling purchase.	c. You are billed for 9 other purchases that were made after yours.	c. Difficulty in proving you did not make these purchases; credit is tied up while situation is resolved; potential damage to credit history.	c. Loss of public confidence, customers; bad publicity; potential lawsuit.	c. Loss of public confidence, customers; bad publicity.
	d. Order entry processing error.	d1. You receive and are billed for 100 copies of the book. d2. Your order is shipped to Hawaii while you receive the order that should have gone to Hawaii.	d. Major inconvenience; credit is tied up pending resolution.	d. Loss of public confidence, customers; bad publicity.	

Exhibit 7 Sample Correlation of Vulnerabilities, Threats, Transaction Paths, and Consequences (continued)

Transaction Path	*Vulnerability*	*Threat*	*Consequences*		
			To Individual	*To Store*	*To Financial Institution*
1.0 ← 2.5.1	a. Unsecured line is used during fax transmission either to place or verify the order.	a. Credit card information is intercepted and misused.	a. Fraudulent use of credit card.	a. Loss of public confidence, customers; bad publicity; potential lawsuit.	
	b. Credit card number is stored in store's computer with your name and address.	b. Misuse of credit card information by store employee.	b. Fraudulent credit card use.	b. Loss of public confidence, customers; bad publicity; potential lawsuit.	
	c. Credit card information is transferred over unsecured line for verification.	c. Credit card information intercepted and misused.	c. Fraudulent credit card use.	c. Loss of public confidence, customers; bad publicity; potential lawsuit.	
	d. Software error in reconciling purchase.	d. You are billed for 9 other purchases that were made after yours.	d. Difficulty in proving you did not make these purchases; credit is tied up while situation is resolved; potential damage to credit history.	d. Loss of public confidence, customers; bad publicity.	d. Loss of public confidence, customers; bad publicity.

	e. Order entry processing error.	e1. You receive and are billed for 100 copies of the book. e2. Your order is shipped to Hawaii while you receive the order that should have gone to Hawaii.	e. Major inconvenience; credit is tied up pending resolution.	e. Loss of public confidence, customers; bad publicity.
1.0 ← 2.5.2	a. Order entry processing error.	a1. You receive and are billed for 100 copies of the book. a2. Your order is shipped to Hawaii while you receive the order that should have gone to Hawaii.	a. Major inconvenience; credit is tied up pending resolution.	a. Loss of public confidence; bad publicity.
1.0 ← All	a. Retail store maintains a database of all books purchased by you.	b. Profiles of your book-buying habits are exchanged with other sources.	c. Law enforcement officials notice that you have been buying many books related to computer security, encryption, etc. and determine you are a potential cyber terrorist; you have to explain that you are doing research for your Ph.D. in Computer Science.	c. Customer sues store for breach of privacy, among other things.

2.6 Summary

This chapter demonstrated why the discipline of IA must be applied to all categories of automated systems and dynamic combinations of these systems. The need for safe, reliable, and secure functionality is near universal in terms of today's application and technology domains. The benefit of IA, to a variety of stakeholders, individuals, organizations, and the environment, is manifest.

President Clinton acknowledged the importance of and benefits from IA in an address he made January 8, 2000. As reported by Babington[207] in the *Washington Post*, Clinton announced plans for a $2 billion budget to meet the nation's security challenges related to high technology. Part of the funding will go toward the establishment of a new research Institute for Information Infrastructure Protection. Babington[207] quoted Clinton as saying:

> *Our critical systems, from power structures to air traffic control, are connected and run by computers. … There has never been a time like this in which we have the power to create knowledge and the power to create havoc, and both these powers rest in the same hands. … I hope that … we will work together to ensure that information technology will create unprecedented prosperity … in an atmosphere and environment that makes all Americans more secure.*

Next, Chapter 3 examines the historical approaches to information security/IA.

2.7 Discussion Problems

1. Why is IA important to the biomedical industry?
2. What infrastructure systems do law enforcement officials: (a) depend on and (b) interact with?
3. Which of the eight infrastructure systems is more important than the rest? Why?
4. Why is IA concerned with more than information systems?
5. What does software safety contribute to IA?
6. What does software reliability contribute to IA?
7. Who is responsible for IA?
8. Develop a diagram illustrating the technology domains in the news media that are dependent on IA.
9. What benefit do individuals derive from IA programs implemented by banking and financial systems?
10. What additional vulnerabilities and threats could be associated with Exhibits 5 and 7?
11. What is the relationship between IA and infrastructure systems?
12. Exhibit 3 illustrates the transactions that must take place to complete an online purchase. Identify the vulnerabilities associated with these transactions.