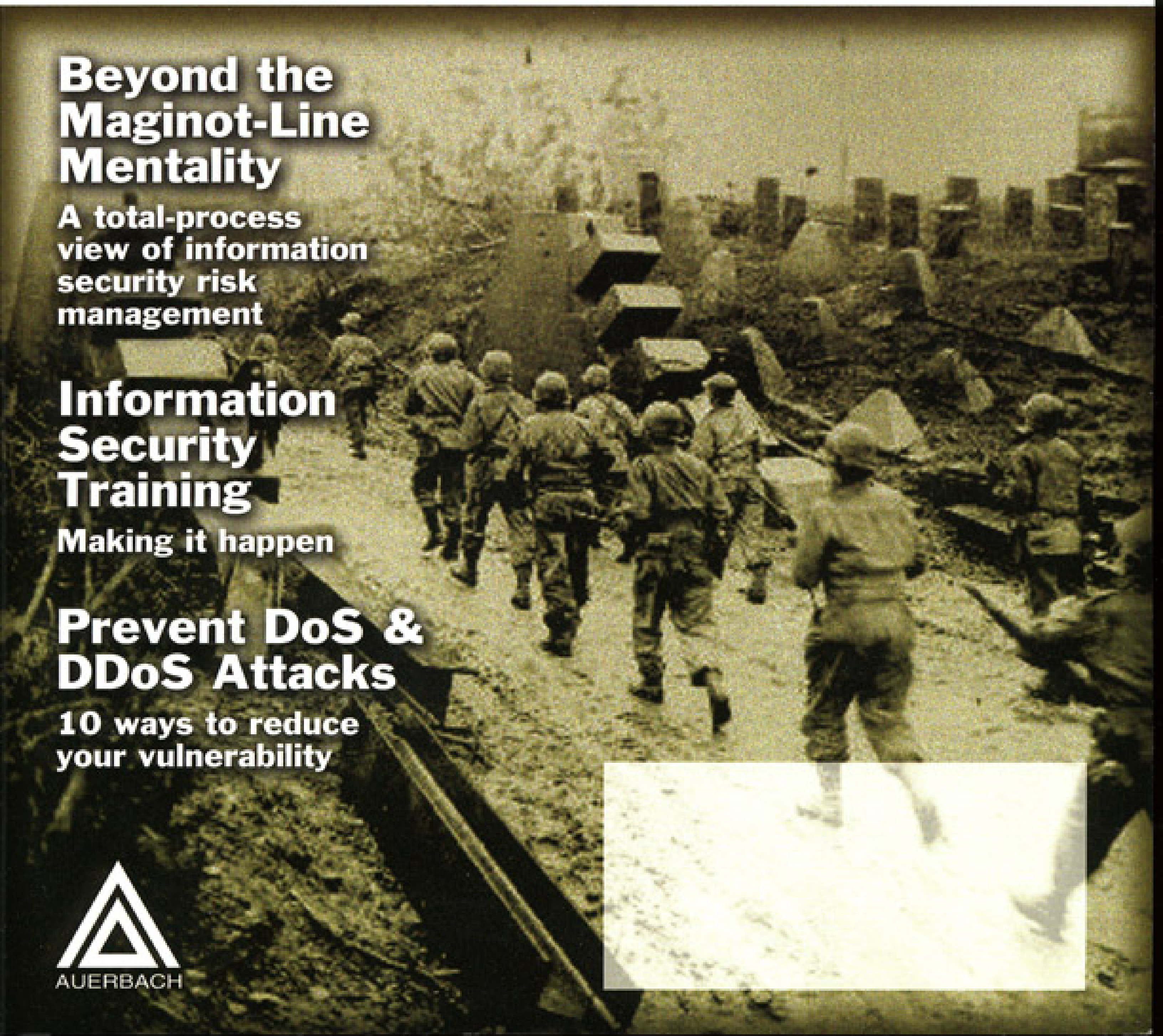
Identify Theft: Who Are You Anyway?

VOLUME 10 • NUMBER 3 JULY / AUGUST 2001

INFORMATION SYSTEMS SECURITY



Beyond the Maginot-Line Mentality

A total-process view of information security risk management

Information Security Training

Making it happen

Prevent DoS & DDoS Attacks

10 ways to reduce your vulnerability

AUERBACH

Beyond the Maginot-Line Mentality: A Total-Process View of Information Security Risk Management

Based on COSO principles and supplemented by other control models and the author's experience.

Allan R. Paliotta, CISA, CFE, CFSA

In his 1951 book *The Hedgehog and the Fox,* British political philosopher Isaiah Berlin refers to an adage from the ancient Greek poet Archilochus that theorizes that "the fox" concentrates his thoughts on many things (i.e., "foxes" think at the detail level), while "the hedgehog" concentrates his thoughts on a few big things (i.e., "hedgehogs" think at the conceptual or policy level). It is my opinion that a substantial portion of information security risk management practitioners tend to think like "foxes." As a result, they have been concentrating their efforts on the details within the information technology (IT) architecture level, while giving relatively short shrift to the recognition of other aspects of information security controls (including the protection of sensitive and confidential corporate and individual information) at the organizational, procedural, cultural, and, to a lesser extent, physical levels. Consequently, the resulting

Allan R. Paliotta, CISA, CFE, CFSA, is a private consultant. He has over 35 years of experience in information technology (IT), auditing, and risk management professions, having held executive/management positions in the consulting and financial services industries, including Director of Security Risk Consulting at Vigilinx, a leader in developing strategy and providing professional services to companies that need to protect their intellectual capital; Senior Manager in KPMG's Information Risk Management practice; and Officer-in-Charge of MetLife's IT Auditing, Insurance Auditing, and Special Investigation Units, respectively. He also had been a project manager in MetLife's system development organization. Paliotta earned his degree in mathematics from Hunter College in New York and has attended MIT's Center for Information Systems Research. He may be reached at arpaliotta@aol.com.

control structure of "fox"-directed security efforts may be as effective as that early modern version of the firewall, the Maginot Line, was in protecting France during World War II. The Maginot Line was a brilliant technological infrastructure that provided virtually no protection to France because the German armies merely went around and over it.

This article is a "hedgehog's" attempt to provide a more balanced and total-process view of the information security risk management process. It is based on the principles espoused by the Committee of Sponsoring Organizations of the Treadway Commission (more commonly known as "COSO") and is supplemented by other generally recognized control models and by my own experience. As stated in the January 2001 issue of *CIO* magazine:

> [Jim Klein of the Gartner Group] says privacy compliance will be more a matter of policies and procedures than of technology. 'If you have a corporate culture that's absolutely scrupulous in controlling information dissemination, you're going to be all set.'

In support of Klein's position (in the February 2001 edition of *Smart Business* magazine), Kevin Mitnick, the well-known hacker, was quoted as having testified to Congress that his "social engineering" skills were so successful that he "rarely had to resort to technical attack."

GENERAL BACKGROUND

Historical

Before getting into the specifics of this article, I think it would be advantageous to the reader to briefly review the historical background of COSO and the basic concepts used in this article as based on COSO and some of the other control models as I have interpreted them. (There is that "hedgehog" mentality showing up.)

In 1987, the National Commission on Fraudulent Financial Reporting, known as the Treadway Commission, issued a report that contained a number of recommendations, including a call for sponsoring organizations to work together to integrate the various internal control concepts and definitions.

In 1992, COSO, whose membership included the AICPA, American Accounting Association, Financial Executives Institute, Institute of Internal Auditors, and Institute of Management Accountants, published a document entitled *Internal Control — Integrated Framework*. Much of this article is based on that document. Additional control models referenced in this article (the concepts of many are similar to COSO) include the following:

□ COBIT (Control Objectives for Information and Related Technology/Information Systems Audit and Control Association) (http://www.isaca.org/)
□ SAC (System of Audit and Controls/Institute of Internal Auditors) (http://www3.theiia.org/)
□ SASs 55/78 (Statements on Auditing Standards/AICPA) (http://www.aicpa.org/index.htm)
□ BS 7799 (British Standards Institute Code of Practice for Information Security Management) (http://www.bsiglobal.com/DISC/index.xhtml)

I chose to use COSO as the primary base model for the following reasons:

□ COSO is a generally recognized approach to internal control evaluation
□ COSO provides a framework/conceptual model/general methodology for evaluating internal controls (i.e., it provides a top down approach, preferred by hedgehogs).
□ COSO is not limited to the IT or information security processes. COSO's primary audience is management and the primary focus is on the overall entity, which makes it:

EXHIBIT 1 COSO Compared to Other Control Models

	COBIT (ISACA)	SAC (IIA)	COSO	SASs 55/78 (AICPA)
Primary Audience	Management, users, information system auditors	Internal auditors	Management	External auditors
Internal Control ("IC") Viewed as a	Set of processes including policies, procedures, practices, and organizational structures	Set of processes, subsystems, and people	Process	Process
IC Objectives	Effective and efficient operations Confidentiality, integrity, and availability of information Reliable financial reporting Compliance with laws and regulations	Effective and efficient operations Reliable financial reporting Compliance with laws and regulations	Effective and efficient operations Reliable financial reporting Compliance with laws and regulations	Reliable financial reporting Effective and efficient operations Compliance with laws and regulations
Components or Domains	Domains: planning and organization; acquisition and implementation; delivery and support; monitoring	Components: control environment; manual and automated systems control procedures	Components: control environment; risk managment; control activties; information and communication; monitoring	Components: control environment; risk assessment; control activties; information and communication; monitoring
Focus	Information technology	Information technology	Overall entity	Financial statement
IC Effectiveness Evaluated	For a period of time	For a period of time	At a point in time	For a period of time
Responsibility for IC System	Management	Management	Management	Management
Size	187 pages in 4 documents	1193 pages in 12 modules	353 pages in 4 volumes	63 pages in 2 documents

Source: ISACA at http://www.isaca.org/bkr_cbt3.htm.
Note: Although not included, BS 7799 is also IT and information security specific.

It is my opinion that the Chief Information Security Officer should be responsible and accountable for the effectiveness of the information security process.

— More easily scalable (i.e., can be applied to any business process)

— More readily adaptable (to new scenarios, technologies, business models)

Exhibit 1 compares COSO to some of the other control models.

The Basic Tenets of Internal Control

As used in this article, the basic tenets of internal control include the following:

□ Internal control is defined as being concerned with:

— Accuracy of financial reporting
— Efficiency and effectiveness of operations
— Compliance with laws, regulations, and corporate policies and strategies

□ The limitations of internal control include the concept that it does not *ensure* or *guarantee* business success, accurate reporting, or compliance, but rather, it provides *reasonable assurance* of the effectiveness of control activities.

□ An internal control structure includes multidimensional components (which will be discussed in greater detail in following sections) as follows:

— Components
— Control environment (i.e., the "tone at the top," or "soft" controls)
— Risk assessment
— Control activities (i.e., "hard" controls)
— Information and communication
— Monitoring

□ Dimensions (as defined by the author) (see Exhibit 2):

— Organizational
— Procedural
— Cultural
— Physical
— Technological

The roles and responsibilities of the various units within organizations are defined as follows:

□ The owner of the system of internal controls is not Auditing.

□ Senior management (including the CEO) is ultimately responsible for the effectiveness of internal control system.

□ The Board of Directors/Audit Committee/Risk Management Committee provides governance, guidance, and oversight. An active and effective board should understand and focus on critical issues and may be in the best position to identify management weaknesses and excesses.

□ Risk management is a multidisciplined function that addresses risk across the organization. Depending on the nature of the organization, such risks could involve financial issues, strategic directions and the competitive landscape, business models, acts of God and man, investment strategy, engineering issues, environmental and ecological considerations, health and safety issues, and legal and regulatory requirements — ***as well as*** — *continuity* of IT operations, *security* of IT infrastructure, and *privacy* of sensitive or confidential corporate and individually identifiable information

□ Internal auditing is a control that evaluates the effectiveness of internal control systems.

□ Other internal personnel must be made aware of, and held accountable for, complying with the concept that internal control is a responsibility of everyone in the organization.

EXHIBIT 2 The Control Matrix

Components/ Dimensions	Control Environment	Risk Management	Control Activities	Information/ Communication	Monitoring
Organizational					
Procedural					
Cultural					
Physical					
Technological					

□ External auditors, consultants, other external personnel may provide information about external events and internal processes. However, external parties are not considered responsible for, nor are they part of, the internal control structure.
□ For reasons described in Section C below, it is my opinion that the Chief Information Security Officer should be responsible and accountable for the effectiveness of the Information Security process.

Note: For the purposes of this article, the concept of the Chief Information Security Officer is being differentiated from the concept of Chief Privacy Officer, whose role, in my opinion, is akin to Customer Ombudsman.

The Basic Tenets of Internal Control as Applied to Information Security

In order to apply the general principles of internal control, *information security* is defined as follows:

□ Information security is a business process, it is neither a goal nor a product.
□ It is an *ongoing and continual* business process.
□ Information security is a major component of the overall system of internal control. Its primary functions are to reasonably assure: (1) the prevention or detection of unauthorized or undesirable corruption, destruction, theft, use or disclosure of sensitive/critical/confidential information (corporate or individual), and information resources, whether intentional or unintentional, and (2) the organization's ability to recover from such breeches. Another way of saying the same thing is — the primary function of information security is to maintain the availability, accessibility, integrity, and confidentiality of corporate and individual information.
□ Although the prominence of information security on corporate and personal radar screens is due in large part to the prominence of IT in the everyday lives of organizations and the general public, viewing information security as a subprocess of IT can limit the scope, attention, and effectiveness that is brought to bear on the process. Because (1) sensitive, mission-critical, confidential information can be stored elsewhere than on corporate computers and (2) security breeches can impact the overall organization on such levels as financial, legal/regulatory, and business model/ business product viability, information security should be viewed as a corporate-level business process and should be placed organizationally so that its objectivity is not compromised, its independence is assured, and its reporting relationships are not encumbered by political considerations.

Business Process Auditing Concepts

On the basis that information security should be considered as a *business process*, the concept of *business*

It is because of the prominence of IT in business and in the daily lives of the general public that we are living in "the Information Age".

process auditing needs to be briefly reviewed.

□ Business processes should be categorized according to risk significance, taking into account the importance of the process and the likelihood of significant risk.
□ Based on risk significance, over the course of a predetermined period (e.g., two to five years), the control components of each business process should be reviewed and evaluated across organizational and geographical boundaries in order to provide an opinion on the adequacy of the internal control structure relative to the entire business process.

Exhibit 3 provides the rationale of why it is important to view a business process as a whole.

While this article is not directed at the discussion of "theologic wars," the analogy is a valid one. It is critical to fully understand the nature of that which is being evaluated — be it an elephant or business process. It is not in the practitioner's best interest to be seen as expounding on the characteristics and weaknesses of a rope, while, in fact, the purpose is to evaluate and comment on an elephant. Exhibit 4 provides my view of the components of the information security and IT operations process.

Protecting Digitized Information and Digitized Product Content in Storage and During Transmission

The importance of digitized information and product content to the success, or even viability, of a business can include the following:

□ Strategic information (e.g., customer information, price lists, trade secrets, proprietary program code, cost information, business partner/third-party information)
□ Decisionmaking information (e.g., provide the basis of management and financial decisions, product decisions, transaction decisions, A/P–A/R decisions)
□ Information that is referenced by privacy and confidentiality laws and regulations (e.g., individually identifiable financial information, individually identifiable health information, other "nonpublic personal information," certain lifestyle choices)
□ Certain third-party expectations (e.g., employees, customers, business partners, the board) regarding the use and confidentiality of certain information
□ Business success and survival can be dependent on the maintenance of the integrity, privacy and security of the product content (e.g., e-mail, digital music, digital books, etc.)

Information Security's Relationship to COSO's Definition of Internal Control

The following are examples of the relationships of the information security process to COSO's definition of internal control:

□ The information security process provides reasonable assurance of the protection of the reliability of financial data from corruption.
□ The information security process provides reasonable assurance of the protection of the efficiency and effectiveness of operations from unplanned interruptions.
□ The information security process provides reasonable assurance of the protection of the integrity and confidentiality of private and sensitive information in compliance with, or to meet the reporting requirements of, appropriate laws and regulations.

EXHIBIT 3 *The Blind Men and the Elephant*

It was six men of Indostan
To learning much inclined,
Who went to see the Elephant
(Though all of them were blind),
That each by observation
Might satisfy his mind.

The *First* approached the Elephant,
And, happening to fall
Against his broad and sturdy side,
At once began to bawl:
"God bless me, but the Elephant
Is very like a WALL!"

The *Second*, feeling of the tusk,
Cried, "Ho! what have we here,
So very round and smooth and sharp?
To me 'tis mighty clear
This wonder of an Elephant
Is very like a SPEAR!"

The *Third* approached the animal,
And, happening to take
The squirming trunk within his hands,
Thus boldly up and spake:
"I see," quoth he, "the Elephant
Is very like a SNAKE!"

The *Fourth* reached out an eager hand,
And felt about the knee
"What most the wondrous beast is like
Is mighty plain," quoth he:
"Tis clear enough the Elephant
Is very like a TREE!"

The *Fifth*, who chanced to touch the ear,
Said: "Even the blindest man
Can tell what this resembles most;
Deny the fact who can
This marvel of an Elephant
Is very like a FAN!"

The *Sixth* no sooner had begun
About the beast to grope,
Than, seizing on the swinging tail
That fell within his scope,
"I see," quoth he, "the Elephant
Is very like a ROPE!"

And so these men of Indostan
Disputed loud and long,
Each in his own opinion
Exceeding stiff and strong,
Though each was partly in the right,
And all were in the wrong!

—John Godfrey Saxe (1816–1887)

Acknowledgment is to Hanan Rubin, Ph.D., CIA, CISA, Vice-President (retired), MetLife (emphasis added).

EXHIBIT 4 The Components of the Information Security and IT Operations Processes

Because the differentiation between the information security process and the IT operations process has not been always been made clear, the following is offered as one method of reviewing the controls over the subprocesses of both.

Information Security

□ *Security management* — including responsibility and accountability for effectiveness of the security control structure, conducting investigations, of possible security violations, maintaining statistics, and reporting to management and the board.

□ *Security Awareness and Training* — including development of the corporate security policy and development and maintenance of the ongoing awareness and training programs.

□ *Security Infrastructure* — including internal and external communications and access procedures, and ongoing monitoring for, and reporting of, potential violations.

□ *Security Risk Assessment* — including risk identification, risk classification, and mitigation strategy.

IT Operations

Computer Facility Management

□ *Operating Systems Management* — including access controls over system software libraries and the ability of systems programmers to function "above" the security software level.

□ *Internal Telecommunications Management* — including backbone networks, LANs, and WANs. Bandwidth adequacy for current and future needs and single points of failure should be included.

□ *External Telecommunications Management* — including E-commerce, Internet-based connectivity, telephone lines-based portals, e-mail, firewalls. Include Access/Message and Sender Authentication/Data Integrity/Non-Repudiation Protocols and Transmission Protocols and Encryption (e.g., PKI, Digital Signatures, Certificate Authorities)

□ *Planning* — including asset classification, capacity monitoring and planning, and planning for new technologies (e.g., is business management sufficiently involved to assure that new technologies will support business requirements?).

□ *Production, Problem and Change Management* — including program change control and management approval requirements, application and operating system reliability and availability, system documentation maintenance and control, help desk/site support, programmer access to the production environment in emergency situations.

□ *Third-Party Relationships* — including adequacy of third-party controls and nondisclosure agreements.

□ *Environment Management* — including physical access to sensitive areas, protection of equipment, uninterruptable power supplies, fire retardant/fighting equipment.

□ *Contingency Planning/Disaster Backup and Recovery* — including the applicability to current and planned technological environments and business operations, and the adequacy of controls at off-site storage facilities.

□ *Outsourcing Management* — including ascertaining the adequacy of the internal control structure of any organization to whom portions of IT Operations have been outsourced or co-sourced, via audits/reviews conducted either by the outsourcing organization or by a trusted third party.

Computer Applications Management

□ *Application Development/Maintenance* — including project initiation/authorization, specification development, system development methodologies, project management: costing/target date tracking, adequacy of testing, user involvement, and signoffs.

□ *Application Systems Controls* — both pre- and post-implementation. Depending upon the level of technology used to support the application system, these audits could be led by either IT or business-type auditors and should include the involvement and perspectives of both organizations. The clerical and administrative processes that interact with the application should be included in the review.

There are, of course, alternate ways of viewing the IT operations process. For example, the subprocesses can be divided on the basis of: platform level (mainframe/midrange/client server/stand-alone PCs); internal vs. external access; or business product line. However, any such methodology must, in accordance with Process Auditing Concepts, include an evaluation of the same activities in order to provide an overall evaluation of the IT operations process.

THE TECHNOLOGY CONTINUUM

It is because of the prominence of IT in business and in the daily lives of the general public that we are living in “the Information Age.” Because of this prominence in the everyday lives of organizations and the general public, the accessibility, availability, and usability of the information that has been captured and warehoused has elevated the awareness for the need for effective information security processes. It is important to recognize where we are currently on the IT continuum when developing an information security risk management program. This section is intended to address this issue.

In retrospect, the world moved from the Agrarian Age to the Industrial Age at a relatively leisurely pace. In contrast, movement into the Information Age is occurring at breakneck, and often daredevil, speed and the rate of change is accelerating. Rapid technological advances are occurring concurrently in multiple directions, and sometimes the technologies converge.

Over the course of the last half of the 20th century, IT evolved from a process whose primary purpose was to *support* the processing of high-volume *transactions* of limited complexity in accordance with the *business paradigm of the day* into processes that *enable significantly modified business paradigms*. It is the author’s opinion that the Information Age will not reach full maturity until those who have been exposed to new technologies virtually in their cribs grow to the point where they influence the development of t*otally new business paradigms* without any preconceived notions based on 20th century business models.

In today’s world, E-commerce/Internet–intranets–extranets/wireless communications/enterprisewide applications/customer relationship management/document management/data analysis-data mining-data warehousing/multimedia technologies/knowledge-based systems/programming methodologies and tools/chip and cable technologies/mainframe-midrange-client-server/worker specialization/regulatory and legal compliance/yada yada yada are just some of the technologically related issues that organizations are addressing. Of particular note to the audit, security, and risk management communities is that, in general, the primary focus of new technologies is initially on functionality. Control and security issues generally tend to be addressed later.

The primary focus of new technologies is initially on functionality. Control and security issues generally tend to be addressed later.

Today, businesses must select from the constantly changing palette of technologies, sometimes just to survive, sometimes to seek competitive advantage, sometimes to achieve operational excellence, and other times to branch out into totally different arenas of operation. In today’s world, information processing has become the business process upon which virtually all other business processes depend. In this Information Age, information assets can be as critical to an organization’s success as its financial, physical, and human resource assets and, as such, also need to be safeguarded.

It is in this environment of continual and accelerating change in business activities and the supporting, and often enabling, technologies that the management and control of the IT and information security processes must be performed. No longer can the focus be only on *internal* controls.[1]

THE DRIVERS OF THE INCREASING IMPORTANCE OF, AND THREATS TO, INFORMATION SECURITY

In addition to understanding where we are on the technology continuum, it is equally important to understand the factors that drive information security and privacy up the risk ladder of importance. This section identifies some of these driving forces.

Changing Business Models

Outsourcing and downsizing have increased competitive positioning, but they have also increased the threat from reduced or negated organizational loyalty. The growth of the E-commerce business model has brought with it significant opportunities for business growth, but it has also brought new threats and exposures to warehoused and transmitted information and content.

Changing Technological Infrastructures

As indicated in the prior section, E-commerce/enterprisewide applications/customer relationship management/data analysis, data mining, data warehousing/multimedia technologies/knowledge-based systems/programming methodologies/mainframe versus client-server/chip technology are just some of the technological issues that organizations are addressing. The primary focus of new technologies is initially on functionality. Security and privacy of information often tend to be addressed later.

The advances in data warehousing and telecommunications are also changing the nature of the capture and use of public information. As indicated in a sidebar to the article "Privacy Matters," which appeared in the January 16, 2001 edition of *Red Herring* magazine, since 1969 the company Acxiom, headquartered in Arkansas, has been "amassing a monster database of consumer information… including dossiers on 160 million Americans — 90 percent of U.S. households." Its database includes "20 million unlisted telephone numbers — gleaned mostly from those warranty cards you filled out when you bought that new coffee maker." In addition to selling this information to law enforcement agencies and just about anyone willing to pay its fees, it also helps E-commerce clients *fraud score* Web surfers. While the sources of the information collected by organizations such as Acxiom may be little influenced by technological advances, the availability, accessibility, and usability of such individually identifiable personal information is significantly impacted by such advances.

Board and Management Liabilities and Responsibilities

The board and management are generally viewed as being responsible for the conservation of an organization's assets.

□ A new report prepared by PwC and sponsored by the IIA, entitled *Corporate Governance and the Board — What Works Best,* states that:

> While CEOs recognize that developing the 'right' strategy is extremely difficult and consistently rank strategy as one of their top issues, a poll of directors shows that board contribution to strategic planning is lacking.

□ As security breeches continue virtually unabated, some of the best-known organizations are victimized, and their business models are significantly impacted by such breeches or other security-related business decisions (e.g., the music industry vis-à-vis Napster and MP3, Amazon.com, AOL, Western Union, Egghead, Toys-Я-Us), the ability to characterize a security breech or transgression that jeopardizes the information assets of an organization as an "unforeseen or unintended event" may become increasingly difficult, thereby potentially increasing the legal liability of board members and senior management to such events.

The Public's Concern About the Level of Protection Over Personal and Confidential Information

In an *Associated Press* news report dated June 16, 2000 entitled "Poll:

Cybercrime Concerns Americans," it was stated that a recent study commissioned by EDS revealed that almost 70 percent of the American public is concerned about the security and privacy of personal information. Adding to the public's concerns are the following:

□ In a news article dated August 10, 2000, Forbes.com reported that Netscape admitted that its SmartDownload program was capable of collecting information about customers using the program. (Netscape also indicated at the time that a new version would end this practice.)
□ Amazon's position, as reported in the September 2000 issue of *CIO* magazine, was that they would consider selling the personal customer information that had been collected as a business asset.
□ The statement to reporters by Scott McNealy, Sun Microsystem's CEO, said "You have zero privacy … Get over it."

Privacy Standards

The Platform for Privacy Preferences (P3P), which was developed by a combination of several companies, privacy advocates, and the standards- setting World Wide Web Consortium (W3C), has called for the development and use of software that will allow customers and site browsers to indicate how much personal data they are willing to share, will allow Web sites to indicate their P3P-based privacy policies, and will automatically alert users when they encounter Web sites that seek to collect more data than users want to share.

Netizen Perceptions Regarding Downloading Anything Floating Through Cyberspace

As suggested during recent litigation activities involving the music industry and Napster, a fair portion of the public has not ascribed to the concept that downloading cybermusic is tantamount to physically pilfering a CD. As noted in an August 28, 2000 news report from *eWEEK,* the lawyers from the Electronic Freedom Foundation, representing the hacker-related publication *2600* (2600.org), "have convinced a growing segment of the public that source code is indeed speech and that viruses, vulnerability exploits and copyright hacks are protected by the Bill of Rights." Whether such an argument would hold up in a court of law is questionable; however, if a sizable number of Netizens believe it to be true, then the resultant security ramifications would become significant.

Governmental Regulations

Government regulations include:

□ The Health Insurance Portability and Accountability Act (HIPAA) and the Gramm–Leach–Bliley (GLB) Financial Services Modernization Act address privacy of nonpublic personal information, including financial and individually identifiable health information.
□ The recent passage of the Digital Signature Law gives electronically signed documents the same legal validity as paper documents.
□ The European Union Data Protection Directive raises legal issues relative to the privacy of personal data.
□ The "safe harbor" framework developed by the U.S. Department of Commerce and the European Commission bridges the differences between EU and U.S. approaches to protecting the privacy of personal information.
□ According to Center for Democracy & Technology, as reported in the article "Privacy Matters," which appeared in the January 16, 2001 edition of *Red Herring* magazine,

EXHIBIT 5 Bytes Without the Blood in the Mideast:
The Internet Blossoms as a Battleground in the Conflict

Scenes of street violence are played out day after day in Palestinian towns across Gaza and the West Bank. But another modern-day arena for battle between the Palestinians and the Israelis is growing ever more heated, so much so that the Internet war waged by computer-savvy political activists is being dubbed an "e-Jihad."

CYBER-SOLDIERS for months have been hacking computer servers, distributing viruses, defacing Web sites and conducting e-mail "bombing" campaigns, which overload systems and produce "denial of service" crashes. From the outset of the conflict, the cyberwar has been relentless, and now it is escalating."

—Hanson R. Hosein of *NBC NEWS*
Tel Aviv, Israel, January 4

eight privacy bills were considered by the 106th Congress of the United States.

Growing Threat of Terrorist Attacks

In late October 2000, the FBI's National Infrastructure Protection Center, the agency that combats cybercrimes, sent out an advisory warning that the tit-for-tat attacks that have shut down and defaced Israeli government, Hezbollah, and Hamas Web sites in the last month could "spill over" into the United States. The FBI advisory said "due to the credible threat of terrorist acts in the Middle East region and the conduct of these Web attacks, [users] should exercise increased vigilance to the possibility that U.S. government and private-sector Web sites may become potential targets."

As shown in Exhibit 5, if the internet becomes the battleground in the next major war — and indications are that it will be ONE of the — if not THE — major battleground(s) — then we must consider all organizations to be at risk, much in the same way that nonmilitary targets are at risk in a military conflict. Military superiority does not necessarily translate into technological invulnerability. Along the same lines, wars often include attempts at destabilizing the economy of the enemy — heretofore by printing and distributing counterfeit money. Think of the potential economic destabilization that would result through the disruption of the e-commerce model and by the disclosure/destruction/counterfeiting of personal information, such as that warehoused in databases controlled by organizations like Acxiom.

Nikolai Lenin once said something to the effect that, "We will hang the capitalists and they will sell us the rope." While his political system did not accomplish his prediction, the concept he espoused may not yet be dead. Perhaps, instead of "rope," "fiber optics" or "coaxial cable" would have been a more appropriate reference.

THE COMPONENTS OF INTERNAL CONTROL AS APPLIED TO THE INFORMATION SECURITY PROCESS

As indicated earlier, the five components of internal control consist of (1) the control environment, (2) risk management, (3) control activities, (4) information and communication, and (5) monitoring. This section will provide a detailed look at these components and how they are applied to the information security process.

Control Environment (Tone at the Top/Soft Controls)

Definition

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility; the way management organizes and develops its people; and the attention and direction provided by the board of directors.

Control Dimensions

Answers to the following questions should be obtained in order to evaluate the effectiveness of the control structure.

I. Organizational

A. Is responsibility and accountability for the security process clearly defined and assigned?

Note: The following observation was taken from the July 24, 2000 edition of *Redherring.com*: Research from network associates showed that 63 percent of companies do not have anyone in charge of security.

B. Does the organizational structure provide reasonable assurance that the security process will operate effectively and efficiently?

C. Is there adequate staff and budget?

D. Is the staff well-trained?

> The number one management error that leads to security vulnerabilities is: assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.
>
> —SANS Security Institute

E. Are internal reporting relationships and procedures established and functioning as intended?

F. Has consideration been given to establishing ongoing contacts with law enforcement, regulatory, and other IT control organizations?

G. If appropriate, has a cross-functional forum of management representatives from relevant parts of the organization been established to coordinate the information security control structure?

II. Procedural/Cultural

A. Management awareness and interest

1. Is security a board-level topic?
2. Are board-level reports of the number and type of violations reported, investigated, and confirmed prepared on a regular basis?
3. Are independent reviews of the security process scheduled and conducted regularly? Are results communicated to top management?

B. Security policies and standards

Note: A security policy is typically a generalized document defining the tone, philosophy, and objectives of the organization relative to security.

Standards tend to provide more detailed strategies in support of the policy. (1) they serve two purposes: They inform people what is expected of them so they can "do the right thing" and (2) they provide the basis for taking action against those that "do the wrong thing."

1. Do corporate security policies and standards exist?
2. Are they adequate? Do they include:
   a. The purpose of the information security program?
   b. Definitions of the roles and responsibilities of management, information owners, security personnel, IT personnel, and the general employee population?
   c. Guidelines for classifying information based on the level of importance?

d. Acceptable uses of computer equipment and facilities?

e. Requirements for, approvals of, and limitations surrounding access to computerized information and facilities?

f. Procedures for accessing information and facilities both from within and external to corporate premises?

g. The use of unique identifiers to assure individual accountability?

h. The maintenance and protection of access security protocols (e.g., passwords) and devices (e.g., tokens, smart cards)?

i. Procedures for transmitting information to external sources and receiving electronically transmitted data from external sources?

j. The removal of corporate information, software, and hardware from corporate premises?

k. The use of corporate information, software, and hardware away from corporate premises (e.g., on the road or at home)?

l. Procedures for computer virus prevention, detection, reporting, and removal?

m. Acceptable behavior regarding Internet access and telecommunication with external entities in terms of how they represent the organization, what information may be disclosed publicly, what sites are deemed unacceptable for access, and use of resources for personal purposes?

n. A statement of the organization's right to monitor and review all electronic transmissions to and from, and all information stored within, organizational computers? A statement indicating whom, within the organization, has the right to review such information and the procedure for evoking that right?

o. Protection of personal and confidential information?

p. Protection of sensitive and confidential corporate information assets?

q. Protection of computer hardware and software in an employee's possession?

r. Procedures for obtaining, installing, using, maintaining, and disposing of hardware, software, communication, and other related components, particularly as they relate to federal copyright laws?

s. Procedures for, and limitations of, divulging information — electronically, orally, or in writing — to outside parties?

t. Procedures for reporting potential security violations, including a well-publicized contact point (e.g., an 800 number) for reporting (anonymously, if desired) such potential violations? Are statistics of such reports maintained and are procedures for follow-up investigations in place and followed?

u. Procedures for deactivating user accesses that are no longer required?

v. Requirements for periodic consultation with security personnel during the business development and systems development processes?

w. Requirements for the storage of confidential/sensitive hardcopy files in locked file cabinets and cautionary statements on the transmission or discussion of sensitive/

EXHIBIT 6 Asset Value Determination

Asset to Company	Value
Achievement of business objectives	
Monetary value	
Support for strategic decisions	
Operational performance	
Organizational reputation	
Compliance with legal and regulatory requirements	

confidential information via fax machines, cellular telephones, or other wireless transmission devices?

x. Disciplinary actions resulting from failure to comply?

y. Obtaining written certifications of awareness and compliance from employees and other collateral personnel?

3. Are they consistent with business objectives?
4. Do new business models consider security policies?
5. Have they been promulgated throughout the organization?
6. Have security policies enforcement procedures been established and are they applied equitably?
7. Is there a clearly written privacy statement on the organization's Web site that indicates what information is collected and retained, the purpose for retention, the identities of any third parties with whom the information is shared, and an opt-out procedure?

C. Awareness and training

1. Is there a security awareness and/or training program for all members of the organization?
2. Is the message of the program reinforced periodically?
3. Are new security-breech schemes communicated to all appropriate employees on a timely basis?
4. Are security responsibilities included in the job definitions of all employees and in performance appraisals?
5. Are employees required to sign confidentiality agreements where appropriate?

D. Incentive program

1. Are employee incentive programs consistent with security policies?

Risk Management

Definition

Risks from external and internal sources must be assessed. A precondition to risk is the establishment of internally consistent objectives. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks must be managed. Mechanisms are needed to deal with the special risks associated with change.

Control Dimensions

The answers to the following questions should be obtained in order to evaluate the effectiveness of the control structure:

I. Procedural

A. Have the major components and systems that represent significant asset value to the company been identified and classified? Significant assets include:

EXHIBIT 7 Security Risk Assessment

Threat	Likely Source (Internal/External/Both)	Significance 1 (low) to 5 (high)
Theft of information	External — hostile	
Unauthorized disclosure of information	Internal — Nonhostile	
Improper usage of information	Internal — Nonhostile	
Corruption/modification of information	Both — hostile	
Interruption of operations	External — hostile	
litigation	External	

1. External connectivity points/Web servers
2. Internal network
3. Operating systems
4. Application systems
5. Information databases
6. People

   Note: *Asset value* can represent different factors to different organizations, including: achievement of business objectives, monetary value, support for strategic decisions, operational performance, the value of the organization's reputation, and compliance with regulatory and requirements. (Exhibit 6).

B. Have the asset owners been identified and job responsibilities related to the protection of assets established?

C. Have the security threats and exposures to the major components and systems been identified and assessed (Exhibit 7)?

1. Theft, disclosure, improper usage, or corruption of information and product content, resulting in the dilution of product value, loss of revenue, difficulties in conducting business, litigation exposures
2. Interruption of operations/ denial of service, resulting in lost revenue, reduced customer confidence, unplanned employee overtime
3. Loss of knowledgeable and critical people

D. Have the sources of threats and exposures been identified and assessed?

1. External threats

   a. General E-public as a result of a business model that is incongruous with public expectations and technological capabilities

   b. Hackers

> According to the FBI/Computer Security Institute, 9 out of 10 U.S. organizations reported computer security breaches within the previous year. Of those, 35 percent reported two to five incidents.
>
> —*Darwinmag.com*, 12/00

   c. Typhoid Mary, Melissa/ I Love You, etc., virus spreaders

> $6.7 billion — the cost to businesses for the first five days of last spring's "I Love You" virus as estimated by Computer Economics, a research company.
>
> —*Darwinmag.com*, 12/00

   d. Blackmailers/thieves/fraudsters

> Global companies often take out insurance on executives who are sent abroad in case they are kidnapped and held for ransom. These days, however, kidnappers are more likely to go after your data than your corporate honchos.
>
> Last January, a hacker broke through the security system of CD Universe, an online music retailer based in Wallingford, Conn., and absconded with 300,000 of the company's credit card files. In a plucky move, the hacker then turned around and offered to return them for $100,000.
>
> —*Darwinmag.com*, 12/00

e. Terrorists/industrial and military spies/drug cartels/ domestic and international organized crime

By definition, every company on the Web is now a global operation. Most policies have a territorial definition and do not cover exposures that a company might face outside its country's borders. If a company is sued abroad, it will most likely have to face the suit on its own.

—*Darwinmag.com*, 12/00

f. Accidents (natural disasters, electrical outages, civil disruption)
g. Competitors
h. Business partner vulnerabilities

2. Internal threats

For larger companies — the Global 2000 — the likelihood of an internal systems threat is greater than 60 percent, according to an Internet crime survey of 600 companies conducted in March 2000 by the FBI and the San Francisco-based Computer Security Institute. Employees can steal customer credit card numbers or e-mail the company's proprietary information and product designs to a competitor in the blink of an eye. The FBI survey found that, on average, 41 percent of security-related losses are the direct result of employees stealing information from their companies. The average cost per internal incident? A cool $1.8 million.)

—*Darwinmag.com*, 12/00

a. Disgruntled employees; inquisitive, indiscreet, or overextended employees; uninformed employees: inadequate/inappropriate internal security policies, and employee awareness
d. Inappropriate human resources hiring and retention policies

3. Litigation threats
   a. Every business with a Web page is a publisher with a publisher's sensitivity to copyright issues, including misuse of trademarks and domain names, plagiarism, copyright infringement, defamation, and libel.
   b. The revelation of confidential/sensitive information as a result of legal actions stemming from allegations of:
      i. Noncompliance with regulatory requirements, noncompliance with stated privacy policies, disclosure of personal/confidential/ sensitive customer information
      iv. Noncompliance with third-party agreements

E. Is the risk mitigation strategy reasonable?
   1. Are analyses of the control structure performed?
   2. Are the scope and frequency of such analyses reasonable?

F. Are there change management processes in place to (1) identify new security risks on an ongoing basis and (2) manage such risks?
   1. Are internal and external sources of information regularly accessed to identify new security risks?
   2. Are there procedures in place to help ensure that security risks are considered as part of the new business development and new system development processes?
   3. Are security personnel included as initial team members in the new business development and new system development processes?

Control Activities

Definition

Control activities are the policies and procedures that help ensure that management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels.

Control Dimensions

The answers to the following questions should be obtained in order to evaluate the effectiveness of the control structure.

I. Organizational

A. Have procedures to effect the security policies been developed for the organization(s) that have responsibility and accountability for the security process?

B. Have the procedures been communicated appropriately and adequately and to upper management?

C. Are the procedures being followed?

D. Has responsibility for reviewing the effectiveness of security-related procedures been established?

E. Is there an organization in place with the knowledge and ability to examine and eradicate computer viruses and recommend operational improvements?

II. Technological

A. Are mechanisms in place that limit access to information and software resident within the internal network to only management-approved resources (e.g., umbrella-type security products are installed with default passwords deactivated and default logic set to "no access unless specifically authorized," application-level coding is in place to limit access to applications on an application-specific basis)?

B. Are controls in place to help provide access security in accordance with established organizational standards and guidelines from external and internal sources at the following levels: network, operating system, applications, databases? For example:

1. From internal locations: Use of unique personal identifiers such as unique user IDs that are continually monitored against personnel-type files for appropriateness and mechanisms for enforcing compliance with password construction rules and the regular changing of passwords?

2. By employees and specified partners from external locations: use of firewalls, use of VPNs, use of smart cards or tokens to supplement the user IDs?

3. By customers and other members of the general public: use of firewalls?

C. Do the access security controls differentiate between employees and contractors, co-sourcers, and outsourcers?

D. Are transmission controls in place to help assure the authenticity, integrity, and nonrepudiation of transmissions in accordance with established organizational standards and guidelines?

1. Is transmitted information encrypted, where appropriate?

2. Are message authentication protocols utilized to assure the data received is the data sent and to prevent repudiation of transmission?

3. Are secure socket layers, authentication certificates, digital signatures, and the like used as appropriate?

E. Are there controls in place to help ensure that individual accountability is maintained in accordance with established organizational standards and guidelines?

F. Have security event detection devices been installed, do they function as intended, and are they monitored in accordance with established organizational standards and guidelines?

G. Is virus detection software installed, operational, and regularly updated on each personal computer and server, as appropriate, and is virus detection software operational on those midrange and mainframe computers that support mission-critical operations?

III. Physical

A. Is access to internal and external facilities and equipment controlled in accordance with established organizational standards and guidelines (e.g., swipe cards or biometric scanners utilizing a sensitivity-level type protocol)?

B. Has interruption event detection and response equipment been installed in accordance with established organizational standards and guidelines?

C. Are locks and cables used to secure the hardware in an employee's possession and are sensitive information and software stored in a locked location?

D. Has equipment been installed to prevent, detect, and react to natural and manmade disasters, particularly taking into account any geographically influenced risk factors, including fire, flood, wind, earthquake, and electrical and transmission line outages?

IV. Procedural

A. Have procedures been developed and communicated to all employees regarding the reporting of potential security incidents?

B. Have policies for the use of computer facilities at all platform levels and external connectivity procedures been promulgated to all employees?

C. Have "No Trespassing" notices been placed at each entry point to the internal network?

D. Are procedures in place to assure management approval is obtained before access is provided to computerized information and facilities?

E. Does management approval for access to computerized information and facilities identify specific resources based on a "need to know" or "need to access" basis? Is there a process in place to report changes in employee status?

F. Are comparison procedures in place to ensure that an employee does not have more than one identifier (at least on a platform basis) and that an identifier is not shared by more than one person?

G. If necessary, can all the identifiers of each employee be assembled, reported, and disabled across platforms on a timely basis?

H. Are there written procedures describing the steps that are to be taken prior to monitoring and reviewing electronic transmissions sent to or from, and information stored within, organizational computers (e.g., a written reason for the action, the obtaining of approval from legal counsel, performing the review in collaboration with some other trusted internal entity)?

I. Do third-party contracts include descriptions of the acceptable rules of behavior while accessing and utilizing information and software within the organization's network and are they regularly reviewed by legal counsel?

J. Has consideration been given to the purchase of Web insurance policies to share the risk of breeches of security?

$6.7 billion — the cost to businesses for the first five days of last spring's "I Love You" virus as estimated by Computer Economics, a research company

$125,000 per hour — the cost to companies for Web outages as estimated by Cahners In-Stat Group

$142,000 — the average cost of a network security breach in 1999 as estimated by the FBI (which found that 55 percent of U.S. companies experienced at least one breach that year)

Companies like American International Group (AIG), Insuretrust.com, Marsh and The St. Paul Companies are selling policies that specifically insure organizations against Internet risks like hacker attacks, viruses and cyberextortion.

—*Darwinmag.com*, 12/00

K. Are employee background checks conducted as part of the hiring process and do termination procedures include the immediate disabling of all employee accesses and the return of any physical security devices?

L. Has an adequate DBR/BCP plan been developed and implemented and are the testing procedures appropriate to minimize the impact of an interruption of services attack and to mitigate security exposures that might be prevalent during the recovery phase?

Information and Communication

Definition

Pertinent information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. This information emanates not only from internal sources, but also includes information about external events, activities, and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across, and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role and have a means of communicating significant information upstream.

Control Dimensions

The answers to the following questions should be obtained in order to evaluate the effectiveness of the control structure.

V. Procedural

A. Information

1. Has the information necessary to manage the security process been identified?
2. Is it appropriate? Does it include the identification of exception occurrences?
3. Does management include obtaining information from external, as well as internal, sources, in order to keep abreast of the security risks *du jour*?
4. Is the procedure for capturing, processing, and reporting information well defined? Does it include immediate notification procedures?
5. Is the security-related information captured, processed, and reported on a timely basis?
6. Does management utilize the information efficiently and effectively?

B. Communication

1. Is the organization's commitment to security communicated clearly and effectively throughout the organization?
2. Are employee responsibilities clearly defined, particularly relative to suspected improprieties?
3. Are formal and informal communication channels in place to facilitate the communication of significant information?
4. Are management's communications about security matters with external parties clear, forthcoming, consistent with internal policies, and appropriate and serious in follow up?
5. Are security issues regularly discussed and coordinated

among risk management, IT, legal, business operations, internal audit, and security personnel?

Monitoring

Definition

Internal control systems need to be monitored — a process that assesses the quality of the systems' performance over time. This is accomplished through ongoing activities, separate evaluations, or a combination of the two. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

Control Dimensions

The answers to the following questions should be obtained in order to evaluate the effectiveness of the control structure.

I. Procedural

A. Compliance monitoring

1. Has responsibility been established to identify on an ongoing basis those laws and regulations promulgated by all relevant jurisdictions (national and international) that are applicable to the security process?
2. Has responsibility been established for the continual monitoring for compliance of the security process with applicable laws and regulations?
3. Is the process functioning as intended?

B. Ongoing monitoring by management

1. As part of its regular activities, does management obtain evidence that security controls have not been compromised?
2. Are critical components continuously monitored on a 24 × 7 basis in real time?
3. Are general operating problems reviewed to identify any relationship to potential security breeches?
4. Do security-related problems communicated from external parties trigger a review of organizational controls?
5. Do the organizational structure and supervisory responsibilities support the continual review and awareness of security-related issues?
6. Are security-related audit recommendations routinely implemented and reported on?
7. Do employees periodically attest to their understanding of security policies, procedures, and expectations?

C. Separate evaluations

1. Are audits of the security process included in the program of internal audits?
2. Are all aspects of the security process included in the program of audits?
3. Is the methodology for evaluating, reporting, and following up on security-related issues appropriate?
4. Is the schedule for conducting security audits appropriate and is the scheduled adhered to?
5. Are the appropriate skill levels available for the conducting of such audits?
6. Are significant items reported at the board-level?
7. Does management perform self-assessments?

Exhibit 8 graphically illustrates some major control mechanisms of the information security process in matrix format.

INFORMATION SECURITY CONTROL ANALYSIS VERSUS INFORMATION SECURITY CONTROL VALIDATION

This section is intended to differentiate between the steps involved when conducting an *analysis* of the adequacy of the intended information security

EXHIBIT 8 Examples of Major Mechanisms of the Control Matrix

Components/ Dimensions	Control Environment	Risk Management	Control Activities	Information/ Communication	Monitoring
Organizational	• Responsibility assigned • Organizational placement • Adequate staff, budget, ability • Reporting relationships • Cross-functional forum		• Security organization authorities to effect implementation established • Responsibility for reviewing effectiveness established • Computer virus SWAT team in place		
Procedural/ Cultural	• Board-level topic and reports • Policies and standards • Awareness training • Independent reviews scheduled • Salary incentive programs	• Asset classification • Exposure identification • Sources of exposures IDs • Reasonable mitigation strategy • Ongoing risk ID process	• Promulgated event observation notification procedures • Promulgated acceptable use of IT facilities • Management preapproval of accesses • Need to know basis • Unique employee identification • Corporate access to information stored on "personal" devices • Employee background checks • Third-party contracts • Web insurance • DBR/BCP	• Information to manage process identified and available • Information captured and reported timely • Information used by management • Organizations' commitment to security promulgated • Employee responsibilities promulgated • Cross-functional discussions	• Compliance with laws and regulations monitored • Compliance with corporate policy and strategies monitored • Periodic employee attestations • Independent evaluations • Results reported to appropriate levels and followed up
Physical			• Physical access – Swipe cards – Biometrics – Locks • Disaster prevention/ detection equipment in place • Locks/cables for "personal" computers • Off-site storage and encryption		
Technological			• Access/authentication controls – Firewalls – VPNs – User profiles/IDs – Password construction – Smart cards – Tokens – Biometrics • Transmission controls – Encryption – Message authentication – Digital signatures – Certificate authorities • System controls – Disable default passwords – Internet scanners – IDs – System logs – Currency of vendor patches • E-mail filtering • Virus detection		

EXHIBIT 9 Documentation Review and Interview Questions

In order to identify the primary areas of security concerns/threats/exposures for each major area of an organization and to develop a management report addressed to such issues, the following steps should be performed:

□ 1. Certain key corporate documents should be reviewed (see below for examples).
□ 2. A series of meetings should be held with key members of corporate management (see below for sample list of interviewees).
□ 3. A high-evel analysis should be performed comparing the identified controls and processes to “best practices.”
□ 4. A report should be prepared providing high-level recommendations for information security process/control improvements to help mitigate any outstanding threats and to help align the security posture with the business strategy.

It should be noted that the initial control evaluation process is conducted at a high level and does not include any substantive testing of controls or processes at this level. However, the information obtained can form the platform from which further, lower-level analyses and testing can be conducted.

It should be recognized that, in trying to draw out management’s perceptions of its risks and opportunities for control improvements, the idea of “controls” is sometimes viewed as something that inhibits progress. To overcome this concept, it is recommended that controls be presented as being supportive of business strategy, i.e., “controls are things intended to make sure that what we want to happen, happens — and what we don’t want to happen, doesn’t happen.”

Sample documentation list:
□ Business mission and strategy
□ Organization chart
□ High-level chart outlining IT environment, including interfaces with customers and third parties
□ Corporate security/fraud prevention policies and procedures
□ Notifications to employees and customers regarding security/fraud prevention policies
□ List of security software in use
□ Third party agreements/contracts
□ Web security insurance policies
□ Critical items classification report
□ Security-related audit reports

Sample interviewee list:
□ Chairman/President/CEO
□ Chief Operating Officer (COO)
□ Chief Financial Officer (CFO)
□ General Counsel (GC)
□ Chief Information Officer (CIO)
□ Chief Security Officer (CSO)
□ Chief Product Officers (CPOs)

Sample Questions

These are samples. The actual questions should be tailored specifically to reflect each organization’s products, processes, and architecture, and follow-up questions would be expected based on the responses to these questions. Note that the answer to many of these questions may be obvious to an internal audit staff; however, it is recommended that they be asked anyway. The identification of differences in management perspectives may result.

Background Questions

These questions are primarily directed toward senior company management. e.g., President, CEO, COO, CFO, and GC:
□ What are the primary products and services of the organization?
□ Who has primary responsibility for the success of each such product and service?
□ What are the primary distribution channels used to get our products to market?

—continued on page 44

—continued from page 43

□ What roles do the Chief Financial Officer, General Counsel, Chief Information Officer, and Chief Security Officer have in the development and/or support of overall business strategy?

For EACH major digital business-related product/service:
□ What is the strategy to increase the value of the product/service?
□ What are the major forces driving our industry in the near term? Long term (internal/external; Presumably E-commerce should be one of the forces)?
□ How are these forces (in general) and E-commerce (in particular) affecting our industry, our competitors, and our organization (product content/order-delivery processes/supply chain-business partner linkage/distribution channels/new sources of competition)?
□ Have you made any modifications to our strategy or business model as a result of E-commerce? Are you planning any changes (this year, 3 years, 5 years)?
□ What do you think our industry will look like in 5 years (expansion-consolidation/new players [who, why]/ big winners-losers [who, why])?
□ How do you envision the role of technology relative to the business strategy (Enabler/supporter, internal: employees, products, storage of digitized data /external: customers, product order-delivery, supply chain)?
□ Do you store any digitized data (either information or product content) in environs that are not within our corporate control (including off-site storage and staging areas)?
□ Have there been any changes in the business environment that have altered the legal/regulatory landscape (e.g., security/privacy requirements, reviews of contracts/third-party agreements, requests by external entities)?
□ Have you been hit by any computer viruses, denial of service attacks, or the like (describe)?
□ Have there been any instances where our product or corporate information has been compromised or corrupted? How would you know if it had been compromised?
□ Have you developed and published a corporate policy regarding the security of confidential/sensitive corporate and customer information? Has it been promulgated to all employees and has it been posted on your Web site?
□ Have there been any litigation threats (or actual litigation) that relate to electronic processes (including noncompliance with regulatory requirements or promulgated privacy policies, disclosure of personal/confidential/sensitive customer information, and noncompliance with third-party agreements)?
□ Have any internal reviews been conducted under the “attorney/client privilege” heading?
□ Have you looked into acquiring a “Web insurance security policy”?
□ Within the context of the wired world of the Internet and E-commerce,

— WHAT do you see as the major threats to our organization?
— HOW and from where do you see such threats being launched?
— WHERE do perceive your vulnerable points to be?
— WHO do you see as the major potential originators of attacks?
— WHICH assets do you see as the most vulnerable or the most enticing, i.e., what keeps you up at night with worry?

Specific Questions
These questions are directed to identifying threats/exposures/concerns related to each major digital business area. Wording may need to be tailored based on the general information obtained above. They are primarily directed to other senior company management; e.g., CPOs, CIO, CSO, GA.
□ How do you assure that you have identified our organization’s key assets (including digitized data, customer order/delivery processes/technology infrastructure) that need to be protected?
□ Have you prioritized them by risk?
□ Are your security efforts based on the risk assessment?
□ Have you considered whether the organization has established responsibility and accountability for directing the ongoing effectiveness of security products, administration, and awareness programs?
Consider the following assets:
□ Digitized assets:
— Information (needs protection from: theft, disclosure, monitoring, misuse, corruption)
— Product (needs protection from: theft, corruption, unauthorized use/distribution/exposure)

□ Customer service/product distribution process (needs protection from: service interruption, modification of order/delivery information, falsification of payment information, repudiation of request for service, weaknesses in partner processing)
□ Supportive and enabling infrastructure (needs protection from inappropriate logical and physical access, degradation of service/destruction, tampering)

Examples of Levels of Digitized Data That Need to Be Protected

Corporate

□ Intellectual property
□ Financial records
□ Customer records
□ Product content
□ Business plans and strategies (including pricing strategies and third party contracts)
□ Internal analyses/ research/correspondence that could result in brand dilution/embarrassment or litigation

Customer

□ Financial Information (e.g., credit card numbers)
□ Health/medical information
□ Sensitive personal preferences
□ Other personal/confidential information (e.g., Social Security numbers, telephone numbers, addresses, ages, children-related data)

Third Parties: Business Partners/Vendors

□ Their corporate/ customer information in your possession
□ Your corporate/customer information in their possession
□ Regulatory/legal/ self-regulatory reporting
□ Analyses of compliance between privacy policies/controls with privacy statements
□ Corporate financial data
□ EEO data

In addition to the traditional hackers, from what sources do you see the primary threats to our organization coming (internally and externally)? Consider:

□ External:
— General E-public
— Blackmailers/thieves/fraudsters
— Competitors
— Business partners
□ Internal:
— Disgruntled employees
— Indiscreet or “Overextended” employees

The general public’s perception about freely acquiring product content that has been digitized and is resident somewhere in cyberspace appears to differ from their perception about freely acquiring equivalent content that is resident in some form of hard copy (e.g., “downloading” versus “stealing”). If that is true, are you concerned about this “cyberworld” perception relative to your business model and how do you assure that your business model is not at odds with that perception? Consider:

□ Whether you have developed a business strategy that is congruous with customer/target/public expectations in a wired world and takes into consideration technological capabilities generally available
□ Performance of regular reviews of the effectiveness of the system of internal controls and establishment of programs to maintain awareness of the “threats du jour”

How do you assure that sensitive/confidential information — both corporate and customer — and product content are not corrupted or improperly replicated/disclosed/utilized by either internal or external forces while it is (a) resident in our corporate files and (b) in transit to/from our network as part of the conducting of your business? Consider:

□ Utilization of access controls to protect access to sensitive/confidential information resident in

— *continued on page 46*

— continued from page 45

corporate databases and digitized product content resident in corporate and staging locations, from external threats (e.g., use of firewalls) and internal threats (e.g., establishment of user profiles consistent with job requirements, continual establishment/updating/monitoring of unique user IDs and profiles, regular changing of passwords, establishment of password construction rules including minimum length and password content)

□ Utilization of transmission controls to protect access to data during transmission, to authenticate and maintain the integrity of data transmitted, and to prevent repudiation of transmission, including encryption, digital signatures, authentication certificates, public key infrastructures, and/or copy protect mechanisms

□ Effective utilization of security software, including the use of optimum default settings and resetting or disabling powerful standardized access/authorization channels provided in vendor software

□ Consideration of the use of technical protection services to limit the number of times a product can be replicated

□ Utilization of physical safeguards to protect product; information systems, databases, and networks; related buildings and equipment

□ Conducting of background checks on employees who have access to confidential information or product content

□ Off-site and encrypted storage of data, product content, and operational software in secure environs

How do you assure that the security of such information complies with the security policy posted on our Web site? What processes do you have in place in the event that such occurrences are successful? Consider:

□ Development of a corporate security/fraud policy, dissemination of the policy throughout the organization, establishment of ongoing employee awareness programs, employee certification of compliance with the policy, promulgation of the policy to the public, ongoing monitoring of adherence to the policy, application of corrective actions when necessary

□ Verification of the controls to ensure that customer “opt out” procedures related to the capture and use of customer information function as intended and as promulgated

□ Performance of regular reviews of the effectiveness of the controls

Are you concerned about spamming/denial of service attacks? If so, how do you assure that you are protected against them? What processes have you put in place in the event such attacks are successful? Consider:

□ The establishment of firewalls

□ The utilization of anti-virus software

□ Continual monitoring of activities to detect suspicious incidents, including unauthorized intrusions and potentially menacing spikes in transmission activities

□ The establishment of exception reporting and corrective action procedures, including an emergency response plan

□ Consideration of the establishment of a “Web security insurance policy” for reimbursement for losses due to hacks or outages and the resultant lost traffic and advertising revenue plus the cost of employee overtime.

How do you assure that orders for product are received from the appropriate person, that the order received is the intended order, and that the product is delivered to, and accepted by, the person who requested it? What processes do you have in place in the event the order is repudiated or delivery is claimed not to have taken place? Consider:

□ Utilization of effective access controls

□ Utilization of certificate authorities to authenticate customers and establish non-repudiation

□ Utilization of transmission controls to protect access to data during transmission, to authenticate and maintain the integrity of data transmitted, and to prevent repudiation of transmission

How do you assure that our business partners and other third parties (including the operators of off-site storage facilities) with whom you transact maintain appropriate levels of security over confidential/sensitive corporate and customer electronic information that you have supplied them with? How do you assure that transmission of such information between organizations is properly controlled? What processes do you have in place in the event that such occurrences are successful? Consider:

□ Utilization of "nondisclosure" agreements with third parties (suppliers/vendors/outsourcers/business partners)

□ For those business partners with whom confidential/sensitive information and product content is shared, contractually established rights to either (1) obtain the results of a third-party review of adequacy of business partner's control structure (e.g., SAS 70) or (2) conduct such a review

□ Verification of the adequacy of security controls at backup data storage sites

Have you had any suspicious or unusual activity relative to the accessing of your systems in the past 6 months? How do you assure that you are aware of any such activity? If such activity has taken place, what was the response? If no such activity has taken place, what are the response procedures if it were to occur? Consider:

□ Continual monitoring of activities to detect suspicious incidents, including unauthorized intrusions and potentially menacing spikes in transmission activities

□ The establishment of exception reporting and corrective action procedures.

How do you assure that physical access to the locations (including off-site storage and staging areas) that house your product, and your IT hardware and software/data bases/network components is limited to those whose jobs require such access? Consider:

□ Utilization of physical safeguards to protect product; information systems, databases and networks; related buildings and equipment

□ Off-site and encrypted storage of data, product content and operational software in secure environs

□ Verification of the adequacy of security controls at off-site storage and staging sites

Aside from the issues discussed above, what security-related issues keep you up at night?

controls and the steps involved when *validating* the adequacy of the operational controls (Exhibit 9).

Security Control Analysis

□ Along with operational management, identify the intended functionality of the business process being reviewed.

□ Along with operational management, identify the security risks/threats/exposures and categorize based on significance of occurrence.

□ Along with operational management, identify the security controls that are intended to be in place to mitigate the risks/threats/exposures.

□ Analyze whether the security controls — if they function as intended — provide reasonable assurance that the risks/threats/exposures would be mitigated.

□ Provide results of analysis, including recommendations for security control enhancements, to operating management

Security Control Validation — Substantive *Testing* of the Control Structure

As a starting point, the results of the security control analysis should be used as the basis for substantive testing. Testing includes probing of all dimensions of security controls, including organizational, procedural, cultural, and physical, as well as technological.

Following are some suggestions for the type of testing that can be conducted:

□ Organizational/procedural testing (look for the evidence)

— Is there evidence of a formal and

current security awareness and training program (beyond e-mail reminders)? Are documented, periodic meetings held to discuss security (at team, department, total-company levels and not just the IT and security organizations)?

— Is a formal and specific acceptable use document provided to each new employee and are periodic updates provided to *all* employees? Is the acceptable use document signed and returned for filing? Have all been returned?

— Are basic reference checks performed on *all* new employees? For employees with access to critical assets, does background check include felony review (particularly, computer-related crimes) and credit check?

— Is there a formal, documented termination procedure that is followed without exception? Does it include reference to terminating access to critical assets and immediate escort out of facility? For noncritical access, are computer user accounts monitored during the termination period? Is there primary focus on assuring the securing of assets and maintaining business operations?

— Are (1) user ID access approval/ termination procedures, (2) password construction and change requirements, and (3) workstation inactivity logoff requirements clearly defined and are they enforced? Is there electronic enforcement?

□ Cultural testing (social engineering)

— Humans are generally the weakest link in the security chain.

— Target newer employees.

— Establish a rapport via telephone and then ask for sensitive information (e.g., calling *from* IS: "I'm from IS and I'm working on this problem and I need your ID and password to verify the fix;" or calling *to* IS: "I'm a high-level user and I'm having a problem getting into my account. I'd like to change the password.")

— Send e-mail asking to establish an account for a new (fictional) employee.

— Inquire (judiciously) as to whether passwords are shared and observe whether hardcopy versions of passwords are displayed publicly (particularly if the passwords are random characters assigned by the system).

□ Physical testing (visit a location that houses critical assets)

— People tend to be trusting and want to be helpful.

— Walk around and observe what security mechanisms are in place, whether they appear to be functioning, and whether they appear to be limiting access to critical assets (i.e., does everyone seem to have access to everything?).

— Attempt a blatant, unsophisticated attempt at a break-in to a secure computer facility and see what happens. Are the entrances physically secure (i.e., locked)? Are guards where they are supposed to be? Do people help? Is the attempt reported?

— Knock on the front door. Will someone buzz you in?

— Do sensitive areas publicly announce that they are sensitive areas?

— Are the walls in critical/sensitive areas solid and do they reach the ceilings? Are there cameras, which are monitored and which record onto tapes that are stored for a reasonable period, in the critical areas? Are there motion detectors installed in critical areas?

— Have biometric security systems been considered?

— Are there badges that differentiate between employees and visitors? Can you wander around the premises freely? Can you sit down at an unattended workstation and access files/send e-mail/etc.? Attempt to gain access to a critical area with a visitor badge.

— Reconnoiter the loading dock and other delivery areas for indications of lax or ineffective security measures. Observe the procedures for allowing entry to the overnight cleaning crew for indications of lax or ineffective security measures.

— Visit the off-site storage facility and attempt access to critical datasets.

□ Technical penetration testing (probing the Maginot Line for weaknesses through, over, under, and around it)

— Direct, frontal attack is usually the most expected and most defended; however, sometimes, the side door is left open (but always try the front door, first, anyway).

— Try the vendor-supplied default IDs and passwords applicable to the system configuration in place.

— Determine if all vendor-supplied patches to known security weaknesses have been applied.

— Try passwords that match user IDs and employee names (and, if known, family member names, keeping in mind that pets are usually considered family members, particularly if their pictures are on an employee's desk).

— Look for passwords that are kept out in the open (on top of a desk, pasted to the side of a workstation, etc.).

— Use multiple password cracking and sniffing tools to seek out specific passwords.

— Test the ports that are the entry points into the internal environment. Web servers provide significant opportunities as entry points.

— Look for noncritical (and less protected) services that are supported within the network. Once in the network, the ability to move around may be easy.

CONCLUSION

It is hoped that the reader has come away with the recognition that an effective and efficient control structure addressed to information security is comprised of multidimensional components that need to be made to function in an integrated and coordinated manner to yield synergistic results. As Bruce Schneier, founder and chief technical officer of Counterpane Internet Security, stated in the February 2001 edition of *Smart Business* magazine:

> People basically want to buy magic security dust. 'Sell me the thing that I can sprinkle on my network that will magically imbue it with the property of security.' It doesn't exist.

Notes

[1] Adapted from the article "A Personal View of a World Class IT Auditing Function" by Allan R. Paliotta, published in *Information Systems Audit & Control Journal* on-line edition, June 1999.

For More Information

1. "The Internal Control-Integrated Framework," COSO report, issued by the Committee of Sponsoring Organizations of the Treadway Commission, 1992.
2. COBIT (Control Objectives for Information and Related Technology), released in 1996 and updated in 1998 by the Information Systems Audit and Control Association (ISACA).
3. BS 7799-1, -2, Information Security Management: Code of Practice for Information Security Management and Specification for Information Security Management Systems. British Standards Institute.
4. Dan Ackman. "Netscape Admits to Collecting Customer Information." *Forbes.com,* August 10, 2000.
5. Michael Bertin. "The New Security Threats." *Smart Business,* February 2001
6. Ben Charny. "Protect your Internet privacy ... by lying." *ZDNet News*, August 22, 2000.
7. Charles Cooper. The brewing Web revolt. *ZDNet News*, August 21, 2000.
8. Paul Desmond. "When security fails." *Network World,* September 13, 2000.
9. Daintry Duffy, "Cyberinsurance — Prepare for the Worst." *CIO.com*, December 2000.
10. Daintry Duffy, "Security Audits: Test Your Defenses." *Darwin Magazine*, December 2000.
11. Michael Fitzgerald. "Picking the locks on the Internet security market." *Redherring.com*, July 24, 2000.
12. Steve Gutterman. "Western Union Web Site Hacked." *Associated Press*, September 11, 2000.
13. Luc Hatlestad. "Privacy Matters." *Red Herring*,

January 16, 2001 (Side Bar 1: Paul Elias, Paid Informant; Side Bar 2: Internet Privacy Bills considered by the 106th Congress. *Source:* Center for Democracy & Technology).

14. David Ho. “Poll: Cybercrime Concerns Americans.” *Associated Press*, June 19, 2000
15. Hanson R. Hosein. “Bytes without the blood in Mideast — The Internet blossoms as a battleground in the conflict.” *MSNBC, NBC NEWS*, January 5, 2001.
16. Brian Krebs. “Feds warn of concerted hacker attacks.” http://www.computeruser.com/news, January 2, 2001.
17. Robert Lemos. “Egghead cracked by credit-card hack.” *ZDNet News*, December 22, 2000.
18. Allan Paliotta. “A Personal View of a World Class IT Auditing Function.” *Information Systems Audit & Control Journal on-line edition,* June 1999.
19. Allan Paliotta. “The Downside of Downsizing — A Window of Vulnerability.” The Association of Certified Fraud Examiners’ *White Paper*, March/April, 1997.
20. Linda Rosencrance. “Toysrus.com faces online privacy inquiry in New Jersey.” *Computerworld*, December 12, 2000.
21. John Taschek. “Life, liberty and the pursuit of free DVDs,” *eWEEK*, August 28, 2000.
22. “Is Amazon’s Bad Privacy Policy Good Business?” *CIO.com*, September 6, 2000.
23. “Reports raise questions over Web security.” *CNN.com*, September 14, 2000.
24. “Sony Exec Rips Napster In Student Paper,” *New York Post*, August 24, 2000.
25. *The 7 Top Management Errors that Lead to Computer Security Vulnerabilities.* SANS Security Institute.