309 Translating the Law into a Practical Technology Plan

Richard J. Corbett
Vice President, General Counsel
Applied Discovery Inc.

Charles H. Le Grand
Director of Technology Practices
The Institute of Internal Auditors, Inc.

Thomas G. Melling
Vice President & General Counsel
Serengeti, Inc.

Faculty Biographies

Richard J. Corbett
Vice President, General Counsel
Applied Discovery Inc.

Charles H. Le Grand
Director of Technology Practices
The Institute of Internal Auditors, Inc.

Thomas G. Melling

Thomas G. Melling is vice president, secretary, and general counsel of ELF Technologies, Inc., an application service provider (ASP) for the legal industry. Mr. Melling has played a central role in the formulation and implementation of ELF's business strategy, and is responsible for the direction of all of ELF Technologies' legal and contracting activities, ranging from technology licensing, security standards, commercial contracts, strategic alliances, and finance.

Prior to joining ELF Technologies, Mr. Melling practiced law at Perkins Coie, LLP internet and ecommerce group in Seattle. While at Perkins Coie, he provided counsel in a variety of substantive areas, including electronic contracting, public key infrastructures, internet law, and technology licensing.

Mr. Melling is vice chair of the Washington State Bar Committee of the Law of Commerce in Cyberspace, and an active member of the information security committee of the ABA. He speaks and writes frequently about electronic signatures, electronic contracting, public key infrastructures, and technology security.

Mr. Melling received a civil engineering degree from Brown University and is a graduate of Stanford Law School.

TRANSLATING THE LAW INTO A TECHNOLOGY PLAN

By

Thomas G. Melling
Vice President and General Counsel
Serengeti, Inc.
tom.melling@serengetilaw.com

ACCA 2001 Annual Meeting
October 16, 2001
San Diego, California

Table of Contents

INTRODUCTION

What policies or procedures has your company adopted to prepare for and respond to the following situations?

- Your company has a system for electronic contracting with your purchasers. A dispute arises over certain terms in the contract, and the party disputing the contract asserts that your company does not have a correct copy of the final contract, or your company purposefully altered the data. The only evidence available to your company is the information on your computer systems. How do you demonstrate that the data is authentic and has not been altered?

- Your company's Web site is the target of a "distributed denial-of-service attack" (DDOS), which shuts down your Web site. Alternatively, a hacker breaks into your company's computer system, and uses your computers as part of a DDOS attack on a third party's Web site. What security procedures has your company adopted to protect against such disruptions and intrusions?[1]

- A fire destroys the building that houses your company's main computer systems. Does your company have computer backup tapes stored off-site?

Many experts believe that companies which fail to establish appropriate information security practices are exposing themselves to liability lawsuits. My research indicates that such a lawsuit has not been filed yet, but one security expert recently warned "you can expect to see major liability lawsuits in the next 18 months."[2] For example, companies that fail to show due diligence in minimizing their exposure to risks such as the spread of computer viruses, financial loss from data corruption or other intrusions, and distributed denial-of-service attacks will become targets of litigation.

---

[1] Although there has been news stories about high profile DDOS attacks against Yahoo, eBay, and other large companies, the problem is more widespread than many people realize. For example, more than one-third of the respondents to the 2001 Computer Crime and Security Survey experienced some form of DDOS attack. The survey is available from the Computer Security Institute, http://www.gocsi,com/fbi_survey.htm.

[2] Jaikumar Vijayan, "IT Security Destined for the Courtroom," ComputerWorld, May 21, 2001, at 1 (quoting Randy Marchany, a member of the Virginia Tech Computing Center's systems management group and the coordinator of its Computer Incident Response Team).

This paper is intended to help in-house counsel better understand and analyze information security issues. It provides a framework and background materials to analyze your company's information security practices, and discusses an apparent trend in emerging laws governing information security practices. It is also suggests a process for using the analysis and due diligence to prepare an information security practice statement.

1. WHERE TO BEGIN: DEVELOP A FRAMEWORK TO ANALYZE ISSUES

The topic of information security is exceedingly complex, which makes it difficult for a company to properly identify its significant and material risks. To begin to analyze the issues, it is often helpful to categorize and create a framework of information security issues. Although information security experts have slight variations in the categorization of issues and terminology, this paper is organized around the framework set forth in this Section 1.

1.1 Protection and Security of Data

Security of paper-based information typically involves some type of physical security – such as a secure room or cabinet that is locked with a key. Conceptually, this type of security is relatively simple to understand and analyze (e.g. only Chris and Sarah have a copy of the key that unlocks the cabinet). On the other hand, the security of information stored electronically may involve physical, logical, and administrative security, and consequently poses more complex challenges for individuals responsible for information security. For example, a company might rely upon a software vendor's product literature claiming that the software encrypts critical data (such as credit card numbers for example). But what does that mean? What type of encryption is used? Is the encryption reliable? In addition, who has access to the encryption key and does the company keep server logs of who has accessed the data? While everyone is aware of the threat that hackers pose to the security of data, many companies have not thoroughly reviewed and analyzed the protections and tools they have employed to protect against intrusions.

1.2 Integrity and Authenticity of Data

Even if a company has sufficient safeguards to protect against hackers and other intrusions, a company is nevertheless vulnerable if it does not adequately preserve and maintain its data. Similar to paper records, companies should understand the environmental conditions in which its electronic data is stored. Backup and retention policies can protect data if it is damaged or accidentally destroyed. Auditing and other integrity verifications are important to prove the authenticity of the data.

1.3 Availability and Retrievability of Data

Data availability and retrievability issues are present whether information is stored electronically or in paper records. However, electronic data retrieval can prose technological problems that do not exist with paper records. For example, companies may fail to keep old programs that are necessary to access and read the data. Companies many not have searching tools that enable them to find data using specific search criteria. And because electronic data can be so easily copied, locating all of the different sources of electronic data can also present challenges. Richard Corbett of Applied Discovery is addressing this issue for the panel, and more information about this topic can be found in his upcoming article in the October ACCA Docket titled: "Managing Digital Data with a Smart Document Retention Policy."

1.4 Disclosure of Data / Privacy Policies

The intentional disclosure of customers' data to third parties is one of the issues that must be considered when conducting a complete review of a company's information security practices. Privacy laws are evolving, and it is a topic that has received considerable attention. Because of the extensive resources on this issue, this topic will not be addressed in any detail in this paper.

2. USE FRAMEWORK TO ANALYZE RISKS TO YOUR COMPANY

2.1 Review Framework with IT Personnel

Once you have created a framework and general categories of issues with respect to information security, the next step is to create a checklist of issues to analyze your company's information security practices. Once you have gathered this information, then it is possible to analyze any possible legal or business exposure faced by your company. One of the challenges of conducting this review is that it involves both technical and legal analysis. While a company's lawyers generally do not have the technical background to assess the technical policies of a company with respect to information security, the company's technical experts generally don't have legal training to analyze the legal risks associated with security practices. Consequently, it is particularly important to have a team of individuals who can work together to produce a meaningful technical and legal analysis that accurately assesses the company's information security risks.

For lawyers involved in this process, it is particularly important to "drill down" with the technical experts as much as possible. For example, it is not sufficient to know that information is encrypted – that is the starting point. The type of encryption, access to the encryption keys, and encryption key backup to avoid data loss are examples other issues that must be reviewed to fully understand the actual security of the data.

2.2 Other Resources to Aid Risk Analysis

There are significant resources available to companies to help them prepare their information security checklists and conduct a review of their information security practices. Below is a short list of some of the resources that are available.

2.2.1 AICPA/CICA SysTrust$^{SM/TM}$ Principles and Criteria for Systems Reliability

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have developed and published the SysTrust principles and criteria. SysTrust uses the following four principles to evaluate whether a system is reliable: availability, integrity, security, and maintainability of a system. Information about the principles and criteria can be found at http://www.aicpa.org/assurance/ systrust/princip.htm.

2.2.2 AICPA/CICA WebTrust$^{SM/TM}$ Seal Program

The AICPA and CICA have established a seal program for e-commerce sites. Under the WebTrust program, Web sites desiring to obtain a WebTrust seal are periodically examined by a WebTrust licensed CPA to ensure compliance with the current WebTrust principles, which include:

- On-Line Privacy
- Security
- Business Practices and Transaction Integrity
- Availability

Information about the WebTrust Seal program can be found at: http://www.aicpa.org/assurance/webtrust/princip.htm.

2.2.3 Control Objectives for Information and Related Technology (COBIT)

The COBIT Framework is published by the Information Systems Audit and Control Foundation. It contains detailed, and somewhat complicated, resources regarding the effectiveness, confidentiality, integrity, availability, compliance and reliability of information. The COBIT Framework is essentially a comprehensive checklist for reviewing business processes and information security. Information about the COBIT Framework can be found at www.isaca.org/cobit.htm.

2.2.4 Generally Accepted System Security Principles

The Generally Accepted System Security Principles (GASSP) are published by the International Information Security Foundation. The GASSP comprise a hierarchy

of guidance for security information, including corporate board-level guidance and executive-level information management. The GASSP draw from recognized information security guidance and authoritative documents to establish "generally accepted" status. As new developments in information technology arise and produce a material affect on information security, appropriate information security guidance is integrated into the GASSP. Information about the GASSP can be found at http://web.mit.edu/security/www/GASSP/gassp021.html.

2.2.5 British Standard 7799: A Code of Practice for Information Security Management

BS779 was developed by BSI Group, and is organized into 10 sections:

- Security policy
- Organization of assets and resources
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance to avoid breaches of any criminal or civil law

Information about BS7799 can be found at: http://www.bsi-global.com/Information+Security/page/index.xalter.

3. ANALYZE AND COMPLY WITH LAWS APPLICABLE TO INFORMATION SECURITY

3.1 Emerging Laws Applicable to Information Security Establish General Standards

It is beyond the scope of this paper to discuss all of the laws that require specific information security practices. Some laws that are applicable to information security issues apply to many industries (e.g. certain document retention laws that apply to both paper and electronic data). Some laws are specific to certain regulated industries. In general, however, there are few laws that actually govern and regulate information security.

Nevertheless, new legal rules regarding information security are emerging. Although these new authorities govern different business activities, they appear to require a consistent approach: They do not set specific standards, but instead create general, flexible rules. Two such examples are ABA Formal Ethics Opinions Nos. 95-398 & 99-413 and the Gramm-Leach-Bliley Act.

ABA Formal Ethics Opinions Nos. 95-398 & 99-413. In its Formal Opinion No. 95-398, dated October 27, 1995, the American Bar Association Standing Committee on Ethics and Professional Responsibility considered the "ethical implications of an arrangement between a law firm and a computer maintenance company whereby the maintenance company would have access to the firm's clients' files" from a terminal located at the maintenance company's offices. The issue posed was whether the third party access to client confidential information stored electronically on the law firm's computers is a breach of Professional Rule of Conduct 1.6. The Committee concluded that a law firm may use a computer maintenance company, and may allow that company to access information in client files as a necessary byproduct when "effecting repairs or correcting problems" provided that the law firm must make reasonable efforts to ensure that the vendor has in place, or will establish, ***"reasonable procedures"*** to protect the confidentiality of client information. The Committee further stated that the same analysis applies to the increasing use by lawyers of "outside agencies for numerous function such as accounting, data processing and storage, printing, photocopying, computer servicing, and paper disposal."

This "reasonable procedures" analysis was further refined in ABA Formal Opinion No. 99-413 (March 10, 1999), titled "Protecting the Confidentiality of Unencrypted E-Mail". Many people are familiar with the general holding of this opinion that transmission of unencrypted e-mail over the Internet is not a per se violation of the Model Rules of Professional Conduct. The Opinion also addressed the issue of information security with respect to data housed on a third-party's computer. In its discussion regarding third party, on-line service providers of email (e.g. "hotmail.com"), the Opinion stated that "[t]he threat to confidentiality caused by the potential inspection of users' e-mail by OSP ["on-line service provider"] system administrators who must access the e-mail for administrative and compliance purposes ***is overcome by the adoption of a formal policy that narrowly restricts the basis on which system administrators and OSP agents are permitted to examine user e-mail.*** (emphasis added, footnotes omitted.). With such protections, the Committee concluded that attorneys "have a reasonable expectation of privacy when communicating by e-mail maintained by an OSP . . . ." Although a formal policy is required, the Opinion did not discuss what are the minimum requirements of the policy.

Gramm-Leach-Bliley Act (G-L-B Act). The G-L-B Act was enacted on November 12, 1999. The purpose of the Act is to reform and modernize the banking industry by eliminating existing barriers between banking and commerce. Title V of the Act, captioned "Disclosure of Nonpublic Personal Information," addresses privacy and security issues relating to nonpublic personal information of customers of financial institutions. The Act requires certain federal banking agencies and the Federal Trade Commission to establish standards for financial institutions relating to administrative, technical, and physical information safeguards.

On February 1, 2001, the federal banking agencies promulgated a final rule establishing the safeguard standards. Exhibit A contains a copy of the regulations. Below is an excerpt from the regulations, which sets forth general standards but no specific requirements:

> II. Standards for Safeguarding Customer Information
>
> A. Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.
>
> B. Objectives. A bank's information security program shall be designed to:
>
> 1. Ensure the security and confidentiality of customer information;
>
> 2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
>
> 3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

On August 7, 2001, the Federal Trade Commission promulgated a similar general standard in its proposed rule:

> In order to develop, implement, and maintain your information security program, you shall:
>
> (a) Designate an employee or employees to coordinate your information security program.
>
> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such risk assessment should include consideration of risks in each relevant area of your operations, including:
>
> (1) employee training and management;

> (2) information systems, including information processing, storage, transmission, and disposal; and
>
> (3) prevention and response measures for attacks, intrusions, or other systems failures.
>
> (c) For all relevant areas of your operations, including those set forth in paragraph (b) of this section, design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
>
> (d) Oversee service providers, by: (1) selecting and retaining service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) requiring your service providers by contract to implement and maintain such safeguards.
>
> (e) Evaluate and adjust your information security program in light of any material changes to your business that may affect your safeguards.

Although regulators and courts have not established specific legal standards for information security, it is important to note that auditors, computer security specialists, and other organizations have considerable experience and expertise with these issues (see Section 2.2 above for a list of non-legal resources addressing information security). The standards and guidelines promulgated by these organizations offer significant resources that General Counsel, security information officers, and boards of directors can use to develop their company's information security practices for their compliance efforts with laws and regulations such as the ABA Opinions Nos. 95-398 & 99-413 and the Gramm-Leach-Bliley Act. Also, since these emerging laws do not set specific information security standards, it is important to keep in mind that judges might rely on these non-legal resources when adjudicating a dispute relating to a company's information security practices.

3.2 Affect of New Electronic Contracting Laws

Most attorneys are aware of the new electronic contracting laws such as the Uniform Electronic Transactions Act (UETA) currently enacted in over 30 states, the Electronic Signatures in Global and National Commerce Act (Federal E-Sign), Uniform Computer Information Transactions Act (UCITA), and even the revised Article 9 of the Uniform Commercial Code. While these new statutes are heralded as the means to throw open the doors of electronic commerce, and consequently have received considerable attention, there has been relatively little discussion regarding the potential implication for companies' information security practices.

Essentially, UETA and the other electronic contracting statutes remove the statute of frauds as a barrier to electronic contracting. However, these statutes do not

address burden of proof issues relating to the enforceability of an electronic contract.[3] Because electronic data can be seamlessly altered without any means of detecting the alteration, this can present challenges for companies who rely on electronic contracts.

For example, assume your company sells XYZ company 10 widgets for $180,000, and the transaction is completed using email. A month later your company's accounts receivable department receives a check for $100,000. When you confront XYZ company, they claim that the contract was for $100,000, and forward a copy of the email they allegedly received from your company which states that your company will sell the 10 widgets for $100,000. If this dispute were to go to trial or arbitration, how would you establish that your company's email records showing the purchase was to be for $180,000 are authentic and have not been tampered or altered? Thus, the ability of your company to be able to establish the authenticity of your data may be critical to your ability to rely on electronic contracts or other electronic records in the conduct of business.

Because of the importance of this issue, the Federal Financial Institutions Examination Council recently discussed this issue in a guidance on the risks and risk management controls necessary to authenticate the identity of customers accessing electronic financial services:

> Some uniform rules concerning the use of electronic signatures and records in retail and commercial transaction may emerge as a result of recent changes in federal laws. While these changes provide more legal certainty that may help promote the growth of electronic commerce, federal law leaves unresolved several important issues related to the validity of an electronic record, as well as the verification and authorization of parties who conduct electronic transactions.[4]

Companies can address the problem of verification and authentication of information in two primary ways. Use of certain electronic signature technologies,

---

[3] Some electronic contracting statutes do address burden of proof issues. For example, the Washington Electronic Authentication Act provides that if a digital signature (created using PKI technology) is verifiable to a digital certificate issued by a certification authority licensed by the state of Washington, the evidentiary issues of document authentication, the signer's identity, and the signer's intent are rebuttably presumed. See Ch. 19.34 of the Revised Code of Washington. In other words, by satisfying certain requirements, the burden of proof with respect to enforcing a contract is switched from the relying party to the signing party. This issue is highly controversial, and the drafters of UETA and other electronic contracting statutes chose not to address this issue.

[4] Federal Financial Institutions Examination Council, Authentication in an Electronic Banking Environment, August 8, 2001. The FFIEC guideline is available online at http://www.ffiec.gov/PDF/pr080801.pdf.

such as digital signatures, can be used to help establish the validity and integrity of data. Unfortunately, because this technology can by difficult and costly to implement, it is not a panacea. For example, implementing digital signature applications involve the creation of a public key infrastructure, the issuance of digital certificates, and distributing special software to the involved parties. To date, cost-effective, practical uses of digital signature applications have not been available or widespread.

Alternatively, companies can rely on their own information practices to help address the problem of verification and authentication. Decisions about what types of policies and procedures to implement, however, must be analyzed on a case-by-case basis. For example, if a company has a high number of low value transactions, their information security practices may have less significance. – e.g. a dispute over a $100 transaction will never be litigated. If a company has high value transactions, especially with customers or vendors with whom it rarely conducts business, the risks of relying on electronic data will become more significant, and their information security practices will have a much higher importance.

4. CREATE FORMAL INFORMATION SECURITY PRACTICES STATEMENT

After analyzing your company's information security risks and reviewing the applicable legal requirements, the next step is to adopt, or make sure your company is in compliance with, appropriate information security practices. Planning for and implementing such policies is a topic discussed in this session by Charles H. Le Grand, Director of Technology Practices of The Institute of Internal Auditors, Inc.

As part of this process, you should consider how to document your company's information security practices. As discussed in Section 3.1, new laws such as the Gramm-Leach-Bliley Act require companies to create and maintain a formal information security practice statement. Even though such documentation may not be legally required for your company, it may nevertheless be prudent to internally document and manage your information security issues. In addition, some companies may need to prepare such documentation for the benefit of their customers. On the other hand, if a company creates an information security practice statement but fails to comply with such statement, it may be creating a dangerous sword to hand to litigation adversaries. Consequently, in-house lawyers should understand the reasons for creating an information security practices statement before such a statement is written and adopted, and make sure there is an appropriate compliance program in place.

Documentation of information security practices can take many forms. Some companies have informal statements about specific issues. Other companies use outlines from resources such as the AICPA/CICA SysTrust$^{SM/TM}$ Principles. The author of a company's information security practices statement should tailor the documentation to the risks faced by the company. An example of an information security practices statement is shown in Exhibit B.

Exhibit A

G-L-B Safeguard Standards

INTERAGENCY GUIDELINES FOR BANKS ESTABLISHING STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

66 FR 8616

FEB. 1, 2001

II. STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

A. Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

B. Objectives. A bank's information security program shall be designed to:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

III. DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SECURITY PROGRAM

A. Involve the Board of Directors. The board of directors or an appropriate committee of the board of each bank shall:

1. Approve the bank's written information security program; and

2. Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk. Each bank shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

C. Manage and Control Risk. Each bank shall:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;

e. with responsibilities for or access to customer information;

f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

2. Train staff to implement the bank's information security program.

3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

D. Oversee Service Provider Arrangements. Each bank shall:

1. Exercise appropriate due diligence in selecting its service providers;

2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and

3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by section D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. Adjust the Program. Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. Report to the Board. Each bank shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank's compliance with these Guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. Implement the Standards.

1. Effective date. Each bank must implement an information security program pursuant to these Guidelines by July 1, 2001.

2. Two-year grandfathering of agreements with service providers. Until July 1, 2003, a contract that a bank has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of section III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of customer information, as long as the bank entered into the contract on or before March 5, 2001.

Exhibit B
Sample Information Security Policies

SAMPLE
INFORMATION SECURITY POLICIES

Exhibit B
Sample Information Security Policies

Overview

The following policies are designed to ensure that all transactions are properly authenticated and authorized, are processed accurately and completely, are completed in a timely manner, and that customer data is safeguarded against unauthorized disclosure or other inappropriate access. They can be summarized into two broad categories, general administrative controls and application controls.

The general administrative controls are those which ensure the integrity and consistency of the overall data processing environment and which impact all application systems. The policies upon which these control structures are based include management and organization, physical security, network security, environmental protection, disaster recovery, hardware maintenance, and data center operations.

Application controls, on the other hand, are more specific to individual application systems or services and are designed to ensure the secure transmission and storage of data, accuracy and consistency of transaction processing, adequacy of information retained for periodic quality assurance and policy compliance reviews, and accuracy of management reporting. Application controls would include data preparation controls, user security validation, edit checks, reasonableness limits, processing controls, restart and recovery, backup and recovery of data, and output distribution controls.

The integrity of the overall environment is safeguarded by the development and continuous improvement of policies and procedures, which ensure that:

- The data processing activities of this company and each of its partner organizations are well managed, that activities are adequately planned, organized, controlled and that proper staffing and direction is provided, and that efforts support the Company's mission and goals.

- There is a current master plan, which properly integrates short term and long-term goals and objectives, and supports the department's master plan and goals.

- Computer hardware is protected from unauthorized access and damage.

- Customer information is protected from unauthorized access, modification, or deletion.

Exhibit B
Sample Information Security Policies

- All transactions entered are verified as to whether or not they have been processed accurately and have appropriately signed and authorized supporting documentation.

Following standard industry practices, these data security practices address the issues of:

1. Integrity of the physical computing environment
   - 1.1 Environmental controls
     - 1.1.1 Power
     - 1.1.2 Fire and moisture monitoring
     - 1.1.3 Temperature and humidity
     - 1.1.4 Fire suppression
   - 1.2 Physical Computing Environment
     - 1.2.1 Security systems
     - 1.2.2 Monitoring
     - 1.2.3 Administrative Controls
2. Integrity of the logical computing environment
   - 2.1 Systems Architecture Definition
     - 2.1.1 Documentation of Infrastructure Architecture
   - 2.2 Change management processes
     - 2.2.1 System Architecture
     - 2.2.2 Infrastructure Architecture
     - 2.2.3 System Software Modification
     - 2.2.4 Application Software Modifications
     - 2.2.5 Administrative Program Modifications
     - 2.2.6 Ad Hoc System Maintenance
   - 2.3 Server operating system access controls
   - 2.4 Other system software access controls
     - 2.4.1 Database
     - 2.4.2 Web servers
     - 2.4.3 Applications
3. Integrity of the data
   - 3.1 Administrative policies
     - 3.1.1 Formal approval for access requests
     - 3.1.2 Formal administrative access policies
     - 3.1.3 Formal administrative password policies
     - 3.1.4 Formal user access (username, password) policies
     - 3.1.5 File backup and retention policies
     - 3.1.6 Security of data transmission

Exhibit B
Sample Information Security Policies

PHYSICAL COMPUTING ENVIRONMENT
1.1 Environmental Controls

1.1.1 Power –

Policy Statement

Reasonable measures will be taken to minimize the possibility of equipment damage or other disruptions to service from line voltage fluctuations and to ensure the continued operation of the data center in the event of failure of the public electrical distribution systems.

Company Practices

Voltage and frequency of incoming power is regulated by dedicated power distribution equipment to within the specifications of the manufacturers of the installed server and network hardware. This protects all critical components from damage or service outages from over/under voltage situations.

Sufficient battery capacity exists to maintain data center operations for 30 minutes in the event of a total electrical outage. The building management, in the event of a longer-term failure of the public power distribution system, provides generator power to the computer facility sufficient to maintain all core services indefinitely.

Exhibit B
Sample Information Security Policies

PHYSICAL COMPUTING ENVIRONMENT
1.1 Environmental Controls

1.1.2 Fire and moisture monitoring –

Policy Statement

Data processing facilities will be safeguarded against damage from fire or water.

Company Practices

Fire and moisture detection apparatus monitors all areas of the data processing facility. Alarms are monitored on-site, as well as by a third party alarm service on a 7 day, 24-hour basis. The alarm company performs regularly scheduled maintenance and testing.

Exhibit B
Sample Information Security Policies

PHYSICAL COMPUTING ENVIRONMENT
1.1 Environmental Controls

1.1.3 Temperature and humidity –

Policy Statement

Temperature and humidity in all areas housing mission critical computing equipment will be maintained within the range specified by the manufacturer.

Company Practices

Consistent environmental conditions are maintained by equipment dedicated to the computing facility. There is sufficient redundant capacity to maintain constant environmental conditions in the event of the failure of a single unit.

Exhibit B
Sample Information Security Policies

PHYSICAL COMPUTING ENVIRONMENT
1.1 Environmental Controls

1.1.4 Fire suppression –

Policy Statement

Fire suppression systems installed in data processing facilities will meet or exceed all local fire district requirements. These systems will be designed to minimize secondary damage to the equipment from the suppression system itself, i.e. the use of inert gas systems or similar technologies in areas containing equipment easily damaged by water.

Company Practices

Fire suppression is based on an FM200 inert gas system that meets both local building code and EPA requirements for non-water based fire suppression systems.

. . . [remaining sections not shown]

eDiscovery: Managing Digital Data with a Smart Document Retention Policy

By Richard Corbett and Virginia Llewellyn
Richard Corbett and Virginia Llewellyn, "eDiscovery: Managing Digital Data with a Smart Document Retention Policy," *ACCA Docket* 19, no. 9 (2001): 18–37.

Richard Corbett is the founder, vice president, and general counsel of Applied Discovery®, a Seattle-based developer of electronic discovery solutions. Previously, Corbett was an attorney with Lucent Technologies, Inc., and Mosaix, Inc.

Virginia Llewellyn is corporate counsel for Applied Discovery®. A former litigator, Llewellyn served on the board of ACCA's Washington State Chapter.

Your company's stock drops more than 80 percent in the market downturn. In the midst of corporate layoffs and departmental budget cuts, you receive a complaint for a class action suit claiming securities fraud. Then a request for production of documents arrives.

As in-house counsel, you work with outside counsel to argue that the request is overly broad and unduly burdensome. A heated and expensive discovery battle ensues. The judge ultimately disagrees with your position and orders you to produce everything requested within 15 days. Outside counsel scramble to comply. You realize that the requested information primarily involves 20 key employees and that most of the relevant data is stored electronically on their hard drives and the central server backup tapes.

One of the 15 attorneys now on site from your defense firm informs you of the bad news: in addition to the employee hard drives at issue, your company has 200 backup tapes on site, with another 700 tapes stored off site, none of which is organized or labeled. The tapes represent daily, weekly, and monthly backups spanning the three-year period involved in the suit. The electronic discovery vendor assisting with your document production calculates the amount of data stored on these tapes to be anywhere from two to four billion pages. The costs of complying with the court's discovery order could cripple your company. What do you do?

This example may seem extreme, but similar discovery situations occur more often than company executives would like to think. Most in-house counsel can relate to this predicament if they have been involved in litigation during the past few years. The typical corporate infrastructure for information storage has evolved from a traditional paper base to an electronic environment. The department-wide email has replaced the department-wide hard copy memorandum. Whereas people once handwrote board meeting minutes and documented them on paper, they now type them into a laptop, which stores them electronically. Whether contracts, financial records, and marketing presentations or calendars and casual communications, the corporate world is creating and storing information electronically.

Companies realize that they can leverage technology to make employees more efficient and profitable, but they generally have not learned to manage the resulting surplus of electronic data. To protect your company from unnecessary risk and expense in

litigation, you should create and implement an effective electronic document retention policy.

Electronic Discovery Law

Before formulating your edocument policy, you need to know the state of electronic discovery law, especially the legal duties and standards applicable to production, preservation, and retention.

Although federal courts have recognized electronic data as discoverable evidence for more than 30 years, ediscovery has become routine in litigation only during the past five years. Federal Rule of Civil Procedure 34, which governs the production of documents between parties, includes electronic data in the description of documents subject to production.[1] The 1970 amendments to Rule 34 specifically state that the definition of documents shall include "electronic data compilations," even when a party can obtain the data only with the use of "detection devices" or from "the electronic source itself."[2]

Discoverability of Electronic Data

Despite Rule 34's longstanding application to electronic data, many lawyers have been slow in exploiting the opportunity to request this restricted and potentially very damaging stockpile of corporate information. Several possibilities may explain why electronic discovery is only now becoming a routine part of litigation and mergers and acquisitions:

- In a word, email.

Most businesses have used computers for years, but employees did not go online with their thoughts, strategies, and complaints until the advent of email. With such technology advancements as personal digital assistants ("PDAs"), laptops, and wireless phones, employees do not even have to be in the office to be working or communicating.

- New tools and affordable technologies have made ediscovery accessible to anyone willing to ask for it.

Once, only firms with deep pockets and high-end technological resources undertook electronic discovery, meaning that it occurred in the largest class action lawsuits or the highest profile mergers and acquisitions. Today, companies specializing in ediscovery can assist any corporate counsel with sorting, searching, and categorizing electronic documents more efficiently than you could review and process paper documents in traditional discovery. With the intimidation and cost factors removed from electronic discovery, corporations can be sure that requests for electronic data will continue to rise sharply.

- Courts are no longer reluctant to allow an investigation of a corporation's electronic data.

The air of mystery surrounding computerized systems is long gone. Courts now permit discovery of corporate electronic data whenever there is a chance that a company has stored relevant information in digital format. Courts also regard with disfavor counsel's argument that a corporation has deleted or cannot retrieve its electronically stored

information. Judges routinely require businesses to turn over electronic data, regardless of claims of hardship or inconvenience.

The law of discovery does not treat information differently because it is stored on a hard drive as opposed to on paper in a filing cabinet.[3] Federal and state discovery rules apply with equal force to both media, including the threshold requirements that the requested information be relevant, not privileged, and reasonably calculated to lead to the discoverability of admissible evidence.[4] The legal equivalency between paper and pixels is good news for lawyers because an estimated 30 to 50 percent of data stored on computers never appears in printed form.[5]

You can introduce discovered electronic documents into evidence as if they were paper documents as long as you properly authenticate them.[6] And like the fabled hunts through warehouses of paper documents, you may freely search through discoverable electronic data to find that case-critical "smoking gun." (See sidebar for a list of tips on avoiding ediscovery disasters.)

Legal Duties

Three legal duties are relevant to document requests in ediscovery. They pertain to the production, preservation, and retention of documents.

Duty of Production

When presented with a discovery request, you cannot merely look in your company's file rooms for responsive documents. Instead, you must examine and identify all places where employees can store data, meaning all in-office computers, hard drives, networks, laptops, floppy disks, backup tapes—sometimes, even Palm Pilots and home computers. The December 1, 2000, "mandatory disclosure" amendments to Federal Rule 26(a)(1) further increased the burden on corporations to disclose the existence of electronic documents and other information at the time of a lawsuit's commencement, before receiving a discovery request.[7] Even information never reduced to paper format and stored by the corporation only in electronic form is discoverable.[8]

In some cases, courts have required companies to make their computers available to the opposing party's forensic expert so that he or she could recover relevant deleted files during discovery.[9] If corporations are unable or unprepared to examine their own data to produce relevant information, the opposing party may be entitled to hire experts to find the information and even perform keyword searches of entire electronic databases in an effort to find requested data.[10]

In the past, recipients of electronic discovery requests have attempted to thwart the opposition's efforts to review electronic data in its native form by producing the requested documents in print form. When the courts get involved, however, this tactic usually backfires. Judges have allowed requesting parties to obtain data in their original electronic form, especially when they specifically request that data be produced in this format.[11] Courts may even require a producing party to construct or recreate a software program to enable the requesting party to access the information in its electronic form.[12]

Duty of Preservation

Your duty to preserve electronic information begins long before a lawsuit commences. If you or another party breaches this duty, the court may find spoliation of evidence has occurred. Spoliation is "the destruction or significant alteration of evidence or the failure to preserve property for another's use as evidence in pending or future litigation."[13]

If a court finds spoliation of evidence, its usual remedy is to levy sanctions on the offending party. Common sanctions include entering a judgment, allowing an adverse inference (such as a jury instruction about the missing data), and awarding attorneys' fees.[14]

In one particularly contentious case, the Seventh Circuit upheld a trial court's spoliation sanctions that had limited a party's ability to present evidence in its defense and subsequently resulted in a default judgment. *Crown Life Ins. Co. v. Craig*[15] began as a dispute between the insurance company and an independent sales agent over the alleged wrongful withdrawal of sales commissions. During discovery, the agent requested written documents related to the calculation of commissions. Not only did Crown withhold some of this information, but also its general counsel submitted a signed affidavit swearing that the company had conducted a reasonable search and had produced all relevant materials.

The lawyer had evidently spoken too soon. At trial, one of Crown's witnesses testified that another database indeed existed that contained information about how Crown calculated commissions. This revelation disturbed the appeals court as much as it had the trial court. The Seventh Circuit rejected Crown's arguments, including the company's insistence that it could no longer retrieve the information in the database. If such a database existed, the court ruled, Crown had a duty to inform Craig and to make it available to him to decipher.[16]

In a policy-holder class action suit, a New Jersey federal district court sanctioned an insurance company $1 million when it destroyed documents at four company locations after the court had issued an order requiring all parties to preserve documents and records.[17] The court did not believe that the company had intentionally destroyed the records, nor did it find that it had acted in bad faith. Instead, it determined that the insurer's preservation efforts or lack thereof were "haphazard and uncoordinated" and held the company accountable for its failure to observe the order.[18] According to the court, the company's senior management should have initiated a comprehensive plan to preserve evidence and distributed the plan to all employees after the court had entered the order.

Spoliation can become an even bigger problem if your company must defend in a state that allows the tort of intentional or negligent spoliation. States that have recognized this cause of action include California, Alaska, Florida, and Kansas.[19] Elements of intentional and negligent spoliation differ from state to state, but commonly include the existence of pending or probable litigation and the defendant's knowledge of it, willful destruction, the intent to interfere with litigation, and damages.[20]

Duty to Retain

Clearly, courts take a dim view of a party withholding and destroying evidence during litigation—especially when there is a court order requiring its preservation. A company must save all electronically stored information that could become the subject of future litigation. But for how long?

Unfortunately, there is no bright-line rule setting out a time period for the retention of electronically stored information. Because all data are not equal—a customer complaint, for example, would likely be more relevant than an interoffice email announcing a company golf tournament—you must maintain some data longer.

To determine your obligations for electronic document retention, start by examining state and federal laws that can subject your company to an affirmative legal requirement to keep certain records for a specific amount of time. Such regulations include those set forth by the Occupational Safety and Health Act, the Fair Labor Standards Act, and their state law equivalents.[21]

Of course, not all electronically stored business documents will fall within regulations. A good rule of thumb for other documents is to retain them for at least as long as the statute of limitations for any cause of action—such as defamation, employment discrimination, or fraud—in which they may become material.[22] Using this guide, you can usually calculate retention times in years.

Some experts suggest that, regardless of an applicable retention time, you should keep electronically stored information longer than paper records. Their rationale is that corporations have a legitimate interest in reducing storage costs and, thus, are justified in destroying paper documents, but that, if the information is electronic, society's interest in retaining records reasonably likely to be relevant in current or future litigation outweighs any burden of cost and space.[23]

The foregoing factors mandate that businesses prepare for potential electronic discovery requests. The best method of preparation is to implement an effective digital data retention policy. Such a policy will help ensure that your company's electronic information is in order, allowing you to work efficiently with outside counsel, when the need arises, in conducting the necessary review and preparation for production.

Retention "Reasonableness" Standard

For your electronic document retention policy to be effective, it must be valid and consistently enforced. Many jurisdictions have defined standards for determining the validity of a document retention policy. In most cases, a reasonableness test applies.

The Eighth Circuit first addressed the reasonableness of document retention policies in 1988. In *Lewy v. Remington Arms Co.*[24] which is one of the cases cited most often in every federal circuit on the subject, the Eighth Circuit reviewed the document retention program of a defendant corporation that had been penalized by the trial court for its destruction of documents. The corporation, a firearms manufacturer, had appealed the lower court's submission of a "general negative inference" jury instruction, based on the company's inability to produce certain documents, including information about

customer complaints, that its employees had destroyed pursuant to its record retention policy.

In a remand of the issue, the Eighth Circuit instructed the trial court to evaluate Remington's document retention policy according to a reasonableness test, which included consideration of the following issues: (1) whether the defendant's policy on retention times related to the documents' importance (for example, a three-year retention period may be sufficient for standard documents, such as appointment notes or telephone messages, but may not be sufficient for records of customer complaints), (2) whether lawsuits concerning the complaints or related complaints had been filed and how frequent and how serious these complaints were, and (3) whether the document retention policy had been instituted in bad faith.[25]

The *Lewy*court concluded that some circumstances may compel the retention of certain documents, notwithstanding the dictates of a general retention policy, such as when a corporation knows or should know that the documents could become material in the future. The court also determined that a corporation may not blindly destroy documents pursuant to a stated policy and expect to be shielded from liability in all circumstances.[26]

If challenged, your company's document retention plan will most likely be subject to a reasonableness standard similar to that set out by the *Lewy*court. After applying elements of the *Lewy*analysis, a federal court in New York, for example, refused to impose sanctions on a party that had destroyed documents pursuant to a valid document retention policy, but had had no notice that the documents held any potential relevance.[27] The lack of notice was key.

Although a corporation need not retain every document in its possession upon receipt of a complaint, it has a duty to preserve what it knows or reasonably should know could be relevant to the action, what is reasonably calculated to lead to the discovery of admissible evidence, and what is reasonably likely to be requested in discovery or become subject to a pending discovery request.[28]

You must educate your internal clients about the legal requirements for data retention and the grave consequences that may result from invalid or improperly enforced recordkeeping policies.

Developing an Electronic Data Retention Policy

The corporation in our introductory ediscovery example found itself in the undesirable position of having to review and potentially produce billions of pages of electronic documents. A massive amount of electronic data was stored—uncataloged and essentially unnoticed—until it came to the attention of the general counsel in the middle of a discovery crisis. How does an otherwise efficiently run corporation let its document storage procedures get so far out of control that a discovery request could threaten the company's financial viability?

Many companies are in a similar position for a variety of reasons, the most common one being that they do not perceive a document retention policy as relevant to the bottom line. They simply do not view the implementation and enforcement of a policy in day-to-day business as practical. It is your job as general counsel to inform the appropriate

decision makers that document retention policies are as critical to the business as other preventive measures, such as general liability insurance.

Beyond this most basic issue, companies may simply fear technical hassles, be ignorant of the rate at which electronic data accumulate without notice, and lack resources to devote to a seemingly tedious project.

Corporate counsel face additional challenges when a policy so critical to their own work runs head-on into the methodologies employed by the information technology ("IT") department. In most companies, it is unlikely that attorneys discuss system backup procedures and electronic storage capacities unless an electronic discovery request is already in hand.

Companies operating without valid electronic document retention policies or even those failing to observe existing policies place themselves in a position of unnecessary risk on several fronts. If you keep too much information, you may experience overwhelming costs when it comes time to review documents for production. If you keep too little information or are unable to provide good records of your document retention protocol you may have to contend with claims of spoliation, which could result in sanctions and even an independent tort action. (See sidebar for handy list of how to develop an electronic document retention policy.)

As you will discover, a document retention policy is not a static system, but rather a continuing process that adapts to the changing ways that your company conducts business. Every company has to start somewhere, however, and the best place to begin is with a candid assessment of your company's current preparedness to respond to an electronic document request. If you already know that you will need help, you may want to consult an electronic data management professional at this point in the beginning to save your company time and money down the road (see list of vendors in the sidebar).

Assessing Current Production and Storage Systems
When assessing your company's current situation, you need to ask some basic questions, including the following: Does your IT department have a storage room full of backup tapes? Can you find and produce documents from even a few months ago? Does your company operate without a formal plan for document retention and destruction?

If you have a general document management policy in place, you can pat yourself on the back, but you cannot relax. If your policy does not include electronic data, it will be of little help in an ediscovery process. Courts treat paper documents and electronic data quite differently.

Five important distinctions explain why you must manage digital data in a unique manner:

- Electronic data accumulate rapidly.

Unlike with paper documents, you can store large amounts of electronic data in a small space, thus keeping years' worth without any outward sign of accumulation. This situation results in the retention of both useless and potentially damaging information.

- Electronic data exist in numerous locations.

Copies of electronic documents usually exist in numerous locations in your company's "electronic filing cabinet." When you create or revise a document, you store a copy of the document in a temporary file. Your company's backup system generates another copy when it backs up the file. Today's mobile workforce presents additional location challenges, because employees frequently save copies of documents in laptops, on disks, or in various other drives.

- "Delete" does not really mean delete.

Even when a computer user intends to discard electronic data, the task is much easier said than done. The "delete" key creates a false sense of security for many people. Although a deleted document may no longer be visible to the user, copies remain in temporary files and on backup tapes. An adverse party may discover all of these sources and, thus, uncover documents presumed deleted or multiple drafts of a document intended to be saved only in final form.

- Electronic documents are easily shared and transferred.

Email is not just a form of communication, it is also a vehicle for transmitting other documents. In many circumstances, email transmission of documents has replaced transmission by fax machine and traditional mail. Whenever you circulate documents for review by email, you generate multiple copies, and the messages and attachments reside in the archive of the author and each recipient.

- Metadata tell the story.

In the "old" days of paper storage, a company could save only the final draft of a contract or letter and be reasonably certain that previous drafts had gone the way of last night's trash. Today, electronic creation and storage of business documents mean that revisions and rewrites are available and discoverable, along with the final versions of the documents. Each copy of an electronic file preserves metadata, telltale imbedded data that include, for example, comments made with "track changes" features, the identities of the original author and any "bcc" recipients, and the dates of document creation and modification.

To assess your company's system, you must interview the people responsible for maintaining its network, hard drives, desktops, laptops, backup procedures, and any other data creation and storage infrastructure that may be in place. Be sure that you understand the potential locations of all kinds of electronic documents. Record these locations. In the past, corporate counsel may have thought that such knowledge could be dangerous. Today, however, the smart in-house counsel realizes that courts will not tolerate pleas of ignorance about the location of electronic data. Such ignorance may lead to court orders exposing more data than you would have produced originally.

Creating a Profile of the Document Retention Policy

After you have assessed your company's current electronic data situation, you must strategize. A document retention policy formalizes a company's procedure for saving and discarding documents received or created in the ordinary course of business. You need to outline a profile for what will go into your data management policy.

When formulating your policy, you should keep in mind the same parameters necessary for traditional retention policies. As previously noted, you must retain some corporate documents, such as tax and employment records, for a time period specified by federal or state law. But many business documents, including routine communications and other electronic data, fall outside of these mandates and often contain key evidence sought by an opposing party. Your retention rules for these documents must be reasonable in light of your company's workforce and business practices and the potential materiality of the data.

Spend time talking with the IT department. Bear in mind that, when litigation occurs, you will have to call upon IT employees to help you with document production. Involve them in decisions regarding the policy's parameters and the methods for its enforcement. They will appreciate being informed up front, instead of being blindsided with an impossible request down the road. Ask them the following questions:

- Does the IT department conduct daily, weekly, monthly, or other regular backups of the systems?
- If so, how long does the department keep backup tapes before recycling or destroying them?
- What happens to the hard drive of an employee who leaves the company?
- Does the department create a "mirror image" of the employee's data in the event that the data may have a future use, or does it wipe the hard drive clean for use by another employee?
- Does the company's email system have an autodelete feature, or does the owner of the individual email account have to "empty" the deleted folder associated with the mailbox? Even when users delete messages from their machines, does the email server store copies elsewhere?

Remember that the IT department has the responsibility of ensuring that the system does not lose data and may not realize the implications of keeping too much data for too long. The opposite situation may occur when there is a stringent corporate policy in place to destroy data on a regular basis.

A competent and consistently enforced document retention policy ensures that you handle electronic data properly before and during litigation. Your policy may assist you in litigation when document destruction occurs pursuant to it. Conversely, your failure to enact a competent policy may undermine your company's position in litigation.[29]

Devising and Drafting a Policy

Once you have identified the profile for your company's document retention policy, it is time to start the actual drafting. This step may seem overwhelming at first. After all, you likely did not specialize in information science policy in law school. The key is to involve others, tapping the knowledge of those who have an intimate and ongoing understanding of the company's current information structure.

If your company has only one physical location or fewer than 100 employees, you may be able to include everyone in the planning process in a relatively personal way. If you work in the law department of a large corporation with hundreds or thousands of employees and/or multiple locations, you should designate departmental representatives to participate in planning. In either case, your first goal is education. If employees do not understand the ramifications of their actions or inactions in creating and storing electronic data, they are less likely to comply with the policy.

During your initial system assessment, you may have learned that your company is needlessly storing years' worth of unnecessary data. After you have checked state and federal laws related to the retention of tax records, employee files, and other regulated documentation, consider whether you can immediately destroy backup copies of routine business documents. Housing too much data for too long can place your company in an unfavorable position in the face of electronic document requests. At a minimum, you will have to expend the time and money necessary to review all of the available data for relevance for production, and in more extreme cases, you may find that your company has kept damaging evidence in records for no reason at all.

Once you have gained control over the electronic data already in your company's archives, develop a plan for the regular deletion of electronic documents created in the future. You may need assistance from your IT department to reconfigure backup schedules for your network. You will definitely need cooperation from employees to maintain a consistent deletion schedule for their hard drives. Consider designating a semiannual cleanup effort that encourages employees to delete unnecessary files from laptops, floppy disks, servers, and desktop hard drives.

You also may wish to consider segregating employees' business email and personal email by applying different retention standards. Although most companies try to limit the use of email to business purposes, the fact of the matter is that both personal email and business email flow through the server. You may decide to set standards for automatic deletion of email, unless the author or recipient makes a conscious decision to store the message as a business record.

It is also important to make sure that the employees responsible for physically carrying out data retention and destruction procedures are aware of the policy's parameters, as well as any changes in the policy. Be sure to include enforcement measures in your plan. And as a final step, establish a schedule for reevaluating the policy's effectiveness. If your company purchases new equipment for executives or reconfigures networks, your plan may need updating.

Whether you are deciding which documents to produce in response to a particularly critical document request or managing a massive review of company records for a

corporate merger, knowing that you have a firm grasp on your company's data creation and storage methods will give you confidence. You will know that you have done everything possible to protect your company from unnecessary risk.

Implementing the Policy

With a policy in place and methods for enforcement clearly defined, you are well on your way to implementing an effective electronic data management plan. As part of your implementation, be sure to educate all of your company's computer users about the pitfalls of electronic communications. Tell them that a good rule of thumb for email is to send only those messages that they would not mind their boss, their mother, or a jury reading. If they would withhold an email from any of these recipients, they should not send the message. Employees should have no false expectations of privacy in any information on the company's computer system.

Teach employees how to manage their electronic data. Inform them about your decisions regarding which business documents they must keep and which they can discard on a regular basis. Advise them about the legal ramifications of deleting information once the company is on notice of a lawsuit or other legal document request. Most employees are unaware of how their actions may affect legal proceedings, and it is your job to help them understand.

Immediately reconsider and be prepared to suspend regular retention and destruction procedures when litigation or another legal document request is pending or imminent. Immediately involve the IT department. Make informed decisions about how best to alter the company's usual retention policy, if necessary, in order to preserve critical documents.

Enforcing the Policy

No document retention policy can provide a fail-safe plan for avoiding liability buttressed by electronic data, but an educated, methodical approach to the retention and destruction of electronic documents will serve your business needs and should stand up to judicial scrutiny.

Cooperate with IT management on enforcing your electronic data management protocol. Designate representatives from the law and IT departments to act as champions of the ultimate cause: protecting your company from unnecessary risk and expense. Along the same lines, prepare a plan for notifying individuals involved in regular retention and destruction to suspend these practices, such as in anticipation of or after notice of a lawsuit filing.

Establish clear enforcement procedures and make a habit of sending out periodic reminders to employees about the policy. Judges are impressed by efforts to ensure employee awareness. Although an executive-level IT employee may be responsible for overall plan enforcement, you should educate all staff members who handle the daily procedures about the policy's importance and hold them accountable. Know in advance whom you would call to testify about your company's document retention procedures, and prepare that person for this role.

If your policy states that certain unnecessary records will be purged at regular intervals, be sure that employees consistently carry out this purging. Conduct internal audits and surprise inspections. Reward compliance.

Continually practice effective prelitigation planning. Stay on top of things; do not sit idly by once you have enacted the plan. Stay in touch with your IT group so that you know what data it is storing and where. Also stay informed about how long the company must keep certain data to comply with applicable statutes and court rulings in your jurisdiction.

Evaluating and Auditing the Policy

You should periodically conduct an internal audit of the document retention policy. It will be easier for you to argue that the policy is reasonable if you regularly reexamine it and make any necessary adjustments. If you find that some of the assumptions that you made in the policy do not work in the daily course of business, change the policy. The more flexible you are about modifying the policy to fit business realities, the more likely you are to gain cooperation from employees. Of course, you also must keep current on the law in your jurisdiction so that your policy always reflects the latest rulings and statutes.

Benefits of an Electronic Data Policy

Whether you are a one-person law department or a member of a large group of in-house counsel, you will recover your investment in preparing and implementing an electronic data management plan many times over when your company receives an ediscovery request. Consider these benefits:

- You save time and money.

An effective document retention policy reduces the time and costs involved in searching for, retrieving, reviewing, and producing discoverable documents. By avoiding the costs associated with gathering data stored in multiple locations and reviewing duplicate documents stored on backup tapes, you will be able to respond to document requests more efficiently. This savings can be critical for small companies or even large companies with small law departments when a major case consumes all available resources.

- You can identify trouble spots in advance.

With organized electronic data, you improve your ability to foresee and react to potential documentation problems. Just knowing where your company stores various kinds of documents allows you to address legal retention requirements. A retention policy also highlights problems in the system, thus preventing the scenario in which hundreds of backup tapes accumulate without notice. The ability to assess your company's vulnerability reduces the chance of having to disclose potentially damaging evidence at a later date.

- You maintain control over discovery.

When your company properly organizes and maintains its records, you enjoy a greater degree of control over the discovery process in litigation or the due diligence phase of a

merger or an acquisition. Instead of facing the possibility of opening all of your corporate records to outside counsel for examination, you are in the enviable position of being able to find and produce only those records directly relevant to the document request.

- You present a consistent public message and avoid becoming a discovery target.

When a company gains a reputation for being disorganized or even obstructionist in discovery, potential adversaries are quick to take advantage. Disorganization can lead to an inability to access documents when adversaries request them. If a company finds documents late in the discovery phase or uncovers them from some other source, it may appear that the company purposefully withheld or fabricated the information. Courts have little empathy for the "can't find it" response to valid discovery requests and frequently respond to such arguments with discovery sanctions. Conversely, a company that can quickly find and produce only those documents relevant to the matter at hand is likely to gain favor in any discovery dispute and earn a reputation for being a formidable opponent.

Conclusion

The company described in the opening hypothetical would have benefited significantly from a digital document retention plan. Instead of suffering the shock of learning about the existence of billions of pages of electronic data in the face of a pending document request, it would have been able to respond to the request by conducting a routine, manageable review of data stored only for a reasonable period of time.

Electronic discovery law favors companies that are proactive in their document management. Your company can easily meet the legal standards for data production, preservation, and retention when you know the potential pitfalls in advance and plan for the most likely scenarios. You should know the general principles of ediscovery law and have a plan in place that treats the review and production of electronic data with the same degree of care and preparation as other documents created and stored in the regular course of business.

The most difficult aspect of developing an electronic data policy is getting started. As you begin the process of organizing a policy, you will likely face resistance from employees. After you have started, however, and informed employees of the effects of their actions, you will likely find employees receptive to the idea of a formal plan. Observing the simple process guidelines discussed in this article and listed in the sidebar "How to Develop an Electronic Document Retention Policy" will help to make your efforts successful.

An electronic data retention policy will save your company money and give it a strategic advantage in litigation. You will have a much better understanding of how and where your company is creating and storing information, thus increasing your ability to protect its long-term business interests in the face of electronic discovery requests.

Notes:

[1] "Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, any designated documents (including writings, drawings, graphs, charts, photographs,

phonorecords, and **other data compilations** from which information can be obtained, translated, if necessary, by the respondent through **detection devices** into reasonably usable form), ..." FED. R. CIV. P. 34(a)(1).

[2] *See* FED R. CIV. P. 34, Notes of Advisory Comm. on 1970 Amendments to the Rules, Subdivision A: "The inclusive description of 'documents' is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form."

[3] *See* Crown Life Ins. Co. v. Craig, 995 F.2d 1376 (7th Cir. 1993); Linnen v. A.H. Robbins Co., No. 97-2307, 1999 WL 462015 at *6, (Mass. Super. June 16, 1999).

[4] *See* Patricia Nieuwenhuizen, *E-mail: The Smoking Gun of the Future*, NAT'L L.J., Dec. 11, 2000, at B9.

[5] *See* Joan Feldman, *10 Steps to Breakthrough e-Discovery*, 1 DIG. DISC. & E-EVIDENCE, Dec. 2000, at 1.

[6] *See, e.g.* United States v. Siddiqui, 235 F.3d 1318 (11th Cir. 2000); Sola v. Ill. Human Rights Comm'n, 736 N.E.2d 1150 (Ill. App. Ct. 2000); Pope v. State, No. 77A05-0003-CR-118, 2000 WL 1877798 (Ind. App., Dec. 28, 2000).

[7] According to the December amendments: "[A] party must, without awaiting a discovery request, provide to other parties: . . . (B) a copy of, or a description by category and location of, all documents, data compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment; . . . ." . FED. R. CIV. P. 26(1)(a)(1)(B), Dec. 1, 2000, required disclosures. The language "and that the disclosing party may use to support its claims or defenses, unless solely for impeachment" replaced the previous qualifier that a party had to provide a copy or description of all documents and so forth within its possession, custody, or control that "are relevant to disputed facts alleged with particularity in the pleadings."

[8] *See* Playboy Enter., Inc. v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999); *see also* Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639 (S.D. Ind. 2000).

[9] *See* Playboy Enter., 60 F. Supp. 2d at 1053; *see also* Simon Property Group, 194 F.R.D. 639 (both cases include discussions of accepted computer inspection procedures).

[10] *See* Procter & Gamble Co. v. Haugen, 179 F.R.D. 622 (D. Utah 1998), *aff'd in part, rev'd and remanded in part*, 222 F.3d 1262 (10th Cir. 2000).

[11] *See* American Brass v. United States, 699 F. Supp. 934, 935 (Ct. Int'l Trade 1988) (ruling that the provision of a computer printout in lieu of computer tapes prevented the plaintiffs from mounting a meaningful appeal).

[12] *See* Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934 at *3 (S.D.N.Y. 1995).

[13] Willard v. Caterpillar, Inc. 48 Cal. Rptr. 2d 607, 616 (1995).

[14] *See* Ian C. Ballon, *How Companies Can Reduce the Costs and Risks Associated with Electronic Discovery*, originally published in "The Essentials of Computer Discovery Seminar" course materials at 3 (Glasser Legal Works 1999). This article is available at http://library.lp.findlaw.com/scripts/getfile.pl?FILE=legpub/glass/glass000014.

[15] 995 F.2d 1376 (7th Cir. 1993).

[16] *Id.* at 1383.

[17] In re Prudential Ins. Co. of Am. Sales Prac. Litig., 169 F.R.D. 598 (D.N.J. 1997).

[18] *Id.* at 615.

[19] *See* William R. Clayton & Antonio D. Morin, *Spoliation of Evidence: The Trend to a New Tort*, Pt. II, 49 FED'N INS. & CORP. COUN. Q. 225 (1999). This article is available on the website of the Federation of Insurance and Corporate Counsel at www.thefederation.org.

[20] *See* Willard, 48 Cal. Rptr. 2d at 618 (citing Foster v. Lawrence Mem'l. Hosp., 809 F. Supp. 831, 836 (D. Kan. 1992)).

[21] *See* Christopher V. Cotton, *Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Era*, 24 IOWA J. CORP. L. 417, n. 22 at *8 (Winter 1999) (discussing retention periods under antitrust laws, OSHA, FLSA, and ERISA). This article is available at http://cyber.law.Harvard.edu/digitaldiscovery/library/preservation/cotton.html.

[22] *See* Ballon, *supra* note 14, at 5.

[23] *See* Cotton, *supra* note 21, n. 110 at *17.

[24] 836 F.2d 1104 (8th Cir. 1988).

[25] *Id.* at 1112.

[26] *Id.*

[27] *See* Hansen v. Dean Witter Reynolds, Inc., 887 F. Supp. 669, 675-76 (S.D.N.Y. 1995).

[28] *See* Wm. T. Thompson Co. v. Gen'l. Nutrition Corp., Inc., 593 F. Supp. 1443, 1445 (C.D. Cal. 1984).

[29] *See, e.g.*, Willard, 48 Cal. Rptr. 2d 607; Telectron, Inc. v. Overhead Door Corp., 116 F.R.D. 107 (S.D. Fla. 1987).

From this point on . . .
Explore information related to this topic

Online:

- ABA's Working Group on Electronic Evidence is preparing a publication that will include forms, checklists, and recommendations for dealing with electronic documents in business and litigation. Postings about the group's work appear at www.abanet.org.

- Catherine Aman, *What's in Your Electronic Closet?*, CORP. COUN. (July 17, 2000), available at www.law.com.

- Applied Discovery® maintains an electronic discovery resource center on its website at www.applieddiscovery.com/LawLibrary/lawLibrary.stm.

- "Applying the Attorney-Client Privilege to Email," an InfoPAK℠ available on ACCA Online℠ at www.acca.com/protected/infopaks/email/amoroso.html.

- Jeffrey Beard, *Keeping Track of Electronic Evidence Discovery*, LAW. MEDIA (July 18, 2001), available at www.law.com.

- Bobbi Cross and Michelle Ayers, *When Discovery Begins, Think Electronic*, THE LEGAL INTELLIGENCER (Feb. 22, 2001), available at www.law.com.

- DIGITAL DISCOVERY & E-EVIDENCE newsletter is published monthly by Pike & Fischer, Inc., a subsidiary of The Bureau of National Affairs, Inc., and is available by paid subscription only. For more information, log on to Pike & Fischer's website at www.pf.com. For ordering information, call 800/255-8131, or email pike@pf.com.

- Michael F. Fleming, *How to Prepare for Electronic Discovery before the Lawsuit Arrives* (Feb. 2001), available on the American Bar Association's website at www.abanet.org/litigation/periodicals/resources/new.html.

- Virginia Llewellyn, *Discovery the E-Way*, TEXAS LAW. (Feb. 1, 2001), available at www.law.com.

- Alison B. Marshall, *Learning to E-Manage*, LEGAL TIMES (Mar. 3, 2000), available at www.law.com.

- "Managing Access to Your Company's Electronic Communication Assets" available through ACCA's Virtual Library℠ on ACCA Online℠ at www.acca.com/vl/electronic/managing/index.html.

- Pia L. Potter, *Manual Processing of Electronic Data is Outdated*, N.J. L.J. (June 11, 2001), available at www.law.com.

- George J. Socha Jr., *Discovering and Using Electronic Evidence* (Feb. 2001), available on the ABA's website at www.abanet.org/litigation/periodicals/resources/new.html.

- "Suggested Electronic Information and Communications Policy," an InfoPAK[SM] available on ACCA Online[SM] at www.acca.com/protected/infopaks/email/accaemail.html.

- Kenneth J. Withers, *Computer-Based Discovery in Federal Civil Litigation*, 2000 FED. CTS. L. REV. 2, available at www.fclr.org/2000fedctslrev2.htm.

On Paper:

- Matthew J. Bester, *A Wreck on the Info-Bahn: Electronic Mail and the Destruction of Evidence*, 6 COMM. L. CONSPECTUS 75 (1998).

- ALAN GAHTAN, ELECTRONIC EVIDENCE (Carswell 1999).

- Corrine L. Giacobbe, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*, 57 WASH. & LEE L. REV. 257 (Winter 2000).

- Richard Raysman & Peter Brown, *Discovery of Computer-Based Evidence*, N.Y.L.J., Oct. 13, 1998.

- Mark D. Robins, *Computers and the Discovery of Evidence: A New Dimension to Civil Procedure*, 17 JOHN MARSHALL J. OF COMPUTER & INFO. L. 411 (1999).

- JOHN WILLIAM STRONG ET AL., MCCORMICK ON EVIDENCE (5th ed. 1999). Not a specific chapter reference to electronic evidence, but relevant issues are evidentiary privilege (chapter 9), authentication (chapter 23), and hearsay exception for regularly kept records (chapter 30).

Electronic Data Management Vendors

Electronic Discovery Vendors:

- **Applied Discovery**®, at www.applied.discovery.com.

- **Daticon, Inc**., at www.daticon.com.

- **Electronic Evidence Discovery, Inc.,** at www.eedinc.com.

- **Fios, Inc.,** at www.fiosinc.com.

- **Ibis Consulting**, at www.ibisconsulting.com.

- **OnTrack Data International** at www.ontrack.com.

Electronic Data Forensics and Recovery Services:

- **CoreFacts** at www.corefacts.net.
- **Ernst & Young** at www.litigation.ey.com.
- **New Technologies, Inc**., at www.forensics-intl.com.
- **PriceWaterhouseCoopers** at www.pwcglobal.com.

Tips for Avoiding eDiscovery Disasters

- Practice effective prelitigation planning.
- Involve the company's technology department in decisions regarding the policy's parameters and methods for enforcement.
- Establish clear enforcement procedures.
- Know in advance whom you may call to testify about the company's document retention procedures, and prepare that person.
- Educate all of the company's computer users about the pitfalls of electronic communications.
- Teach employees how to manage their electronic data.
- As a routine matter, decide which business documents employees must keep and which ones they can discard on a regular basis.
- If your policy states that certain unnecessary records will be purged at regular intervals, purge them consistently.
- Conduct internal audits and surprise inspections.
- Reward compliance.
- Consider segregating business email and personal email by applying different retention standards.

- Immediately reconsider and be prepared to suspend regular retention and destruction procedures when litigation or another legal document request is pending or imminent.

- Immediately involve the IT department when litigation or another form of document request is imminent.

- Periodically conduct an internal audit of the company's retention policy.

How to Develop an Electronic Document Retention Policy

- Candidly assess your company's current preparedness to respond to an electronic document request. Remember that electronic data accumulate rapidly, exist in many locations, and can be easily shared and distributed.

- Outline a profile for what will go into your formal policy. Remember to include your IT department when planning the guidelines for the policy.

- Gather all of your research and formalize the guidelines in a corporate policy.

- Implement the plan and distribute it to employees. Be sure to teach employees how to manage their electronic data and educate all of the company's computer users about the pitfalls of electronic communications.

- Enforce the policy. Establish clear enforcement procedures, and make a habit of sending out periodic reminders to employees about the policy.

- Periodically conduct an internal audit of the company's retention policy to keep it up to date, and modify the policy to adjust for business realities.

- Ensure that the policy is valid and consistently enforced. It must meet a reasonableness standard.

The Audit Role in Information Security and Critical Infrastructure Protection

Charles H. Le Grand
Director of Technology Practices
The Institute of Internal Auditors, Inc.

Information Security

- Integrity, Confidentiality, Availability
- Information Infrastructures
  - Fragile
  - Changing
  - Poorly defined
  - No clear indicators of adequacy
- Global Scope

Critical Infrastructure Protection

- **What is CIP?**
  - Business, Industry, National Defense, Economy
  - Infrastructures support critical industries.
    - IT and Communications
    - Energy: Oil & Gas,and Electrical Power
    - Transportation: Air traffic, Railroads, Highways, Bridges, Trucking, Buses
    - Banking & Finance
    - Government Services:Emergency Services, Water, Law Enforcement,

Critical Infrastructure Protection

- Interconnectivity increases vulnerability.
  - System and Network Failures
  - Cyber Attack
- Potential Consequences
  - Disruption of critical infrastructures and all who depend on them
  - Decreased confidence in electronic information and transactions
- Ability to Respond and Recover

Critical Infrastructure Protection

- **How does auditing figure into CIP?**
  - Validity of Information: Current and Future
  - Technologies and Infrastructures
    - acquisition, processing, communication, storage, and reporting of information

Auditors and CIP

- Growth and Pervasiveness of eBusiness
- Critical Infrastructures are More Than 90% Private Sector
- Government Protection / Control Not a realistic Expectation
- Influence "Tone at the Top"

The Auditing Profession

- Independent, Objective Appraisals, Assurance
- Materiality
- Consulting, Recommendations
- Growing Stakeholder Base
- Continuous Audit Services

Internal Auditing

*"Internal auditing is an **independent**, **objective assurance** and **consulting** activity designed to **add value** and **improve** an organization's **operations**. It helps an organization accomplish its objectives by bringing a **systematic**, **disciplined** approach to **evaluate** and improve the effectiveness of **risk management**, **control**, and **governance** processes*."

Internal Auditing (continued)

- Reliability and Integrity Information
- Compliance with Policies and Regulations
- Safeguarding of Assets
- Economical and Efficient use of Resources
- Operational Goals and Objectives
- Financial Activities
- Operations: Systems, Production, Engineering, Marketing, Human Resources
- Increasing Interaction with Outside Organizations

External Auditing

- Third-party (service) audits of IT
- Collaboration with Internal Audit
- SAS 70
- SysTrust

  System reliability is a fundamental building block in the profession's goal to provide continuous assurance, as discussed in the AICPA/CICA research report "Continuous Auditing."

Information Systems Auditing

- "Specialist" IT Auditor
- Auditor Uses of IT Tools
- IT Competence of All Auditors
- IT Audit Guidance
  - ISACA — COBIT, ISACA.org, ITGovernance.org
  - IIA — SAC, ITAudit.org,TheIIA.org, "Information Security Management and Assurance: A Guide for Directors & Executives"

Auditor Interaction with Other Professional Bodies

- Guidance on Auditors' IT Roles
- Lack of IT "Standards"
- "Effective Practices"
- "Business Case"
- Board of Directors
  - Duty of Care
  - Audit Relationship
  - Assurance

Business Case for CIP

Information security and CIP issues of interest to governance and executive management include:

1. Potential negative impacts on shareholder values
2. Insurance issues, for the organization and for directors and officers liability;
3. Third-party liability for cyber attacks and privacy violations; and
4. Increasing regulation and legislation.

- Nancy J. Wong, Critical Infrastructure Assurance Office, on ITAudit.org Forum, October 1, 2001 (See also CIAO.gov)

Measuring Assurance

- Electronic Commerce and Dependence on IT
- Need for Improved Security
- Public versus Private Sector
- Cyber Attacks
- Measures of effective information security management — "Generally Accepted"
  - ISACs, ISO 17799, CIS, GASSP
- Tone at the Top

CIP and The IIA

- IIA CIP Projects
  - Partners and Sponsors (NACD crucial role)
  - Increased Visibility of CIP, Auditing, IIA
- Products
  - *Information Security Management and Assurance: A Guide for Directors and Executives*
  - *Critical Infrastructure Assurance Conference Series*
- "Audit Summit" Media Coverage
  - Web-casting, onsite reporters, television evening-news, transcriptions of speakers' messages on the web, Report of the POTUS to Congress on CIP Activity

IIA Affiliates Around the World

- IIA Affiliates' Programs
  - Outreach
  - Awareness
  - Education
- International Outreach
  - PCIS, CIS, GASSP,
  - UK, Australia, Canada,
- See www.ITAudit.org

Critical Infrastructure Protection

- Progress Through Sharing -
  - Leadership in the electronic era,
  - On a global scale.

The Audit Role in Information Security and Critical Infrastructure Protection

Charles H. Le Grand, Director of Technology Practices
The Institute of Internal Auditors

Information Security

All organizations as well as our individual and collective infrastructures depend heavily on the reliability and security of information. But the information security elements of business and infrastructure protection are often fragile, changing, and poorly defined with no clear indicators of what constitutes adequate security. Efforts are underway around the world to improve understanding and awareness of information security issues in corporate governance, government, management at all levels, and within the legal and auditing professions.

What is CIP?

Critical infrastructure protection is a broad concept recognizing that organizations, industries, governments, nations, and even the global economy are all interdependent on infrastructures that are necessary for their continuity and success. Everyone depends on the availability and reliability of electrical power, communications, transportation, oil and gas, banking and finance, water, emergency services, and functional governments.

The increasing connectivity and openness of computer networks are expanding the vulnerabilities of organizations and critical industries to system and network failures and to "cyber attack." The potential consequences of cyber incidents include disruption of critical infrastructures and all who depend on them, and decreased confidence in electronic information and/or transactions. These consequences can impact national security and the economy.

The physical attacks of September 11, 2001 illustrated the potential for unexpected destructive actions. The need for CIP clearly goes beyond cyber attack to include the ability to respond to and recover from disruptions and attacks in all forms. But one can see how a well-coordinated cyber attack against the information and communications infrastructures supporting critical industries could have serious, long-term consequences.

How does Auditing figure into CIP?

Auditors have historically attested to the validity of information – typically financial information relative to a period of time, or point in time. But contemporary auditors must relate to current and future information reliability. And the integrity of information today is linked to the technologies and infrastructures that manage the acquisition, processing, communication, storage, and reporting of information. Auditors clearly must address the full spectrum of threats as they plan and conduct their work.

Auditors provide independent, objective appraisals. They provide assurance regarding the reliability of information. They provide consulting and other valuable services. Auditors deal with issues that are material to the success and continuity of the organization and the interests of the organization's stakeholders. Auditors must necessarily address the environments and issues related to information security. The recipients of audit services are demanding improved timeliness and relevance in attestations and assurance. The logical extension for such audit services would be continuous monitoring and real-time assurance.

Internal Auditing

Risk management has taken on increased importance in the defined roles of auditors. In 1999 The Institute of Internal Auditors (IIA) adopted a new definition on internal auditing:

> "*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*"

Internal auditing reviews the reliability and integrity of information, compliance with policies and regulations, the safeguarding of assets, the economical and efficient use of resources, and established operational goals and objectives. Internal audits encompass financial activities and operations including systems, production, engineering, marketing, and human resources.

The auditor's role in assessing the reliability of information necessarily requires ever-increasing emphasis on information systems, networks, operating environments, and all other elements of managing information technology (IT). As auditors become more involved in providing assurance relative to critical infrastructure protection, their work will necessarily involve more interaction with outside organizations, other professional groups, and governments.

External Auditing

Historically, external auditors (typically firms providing public accounting, auditing, and other professional services) have offered third-party audits (service audits) of information processing facilities, operations, and related management. External IT audits are an important element of the external auditor's ability to attest to the validity of information. Internal and external auditors routinely collaborate on the scope of work each will perform with regard to an organization and its business partners. Such collaboration is necessary to assure full audit coverage and to reduce redundant coverage. Professional auditing standards are an important element of the ability for internal and external auditors to each rely on the work of the other.

The service auditor's engagement to report on controls related to financial statement assertions is described in the AICPA's Statement on Auditing Standards (SAS) No. 70. The elements of **SAS 70** reviews are selected and agreed for each engagement, and the resulting report provides information and opinions on the design of the systems and controls covered in the review.

Recently the AICPA and CICA developed a new assurance service for the reliability of systems. The **SysTrust** assurance service is provided by CPAs and CAs as part of a broader future vision to supply real-time assurance on informational databases and systems. In announcing this service and specifying the terms and conditions of its licensing agreement, the AICPA and CICA stated: "System reliability is a fundamental building block in the profession's goal to provide continuous assurance, as discussed in the AICPA/CICA research report 'Continuous Auditing.'"

Information Systems Auditing

Information systems auditing is often regarded as a "specialty" within both internal and external auditing. There is a significant need for auditors to specialize in IT, the use of IT tools in auditing, and the control of system and network components and management. There is also an ongoing and increasing need for auditors at all levels to understand the impacts of technology on security, controls, management, and auditing across all activities of the organization.

Guidance for auditors conducting technical IT audits comes from two primary sources. The Information Systems Audit and Control Association (ISACA) publishes technical guidance in "Control Objectives for Information and Related Technologies" (COBIT). The IIA publishes more general guidance in products like the "Systems Auditability and Control" (SAC) reports. IIA and ISACA also both provide other products and services including IT guidance via the web on www.ITAudit.org and www.TheIIA.org (IIA) and www.ISACA.org and www.ITGovernance.org (ISACA).

Auditor Interaction with Other Professional Bodies

Significant guidance is available to auditors concerning IT regardless of their level of responsibility or technical specialty. However, technical "standards" do not exist for many IT areas subject to audit, so innovative auditors must often identify "effective practices" or other measures to use as benchmarks or baselines in audit assessments or appraisals. Thus much IT audit work is not in the realm of "compliance with generally accepted standards or principles," but involves providing a business case supporting the auditor's activities and recommendations.

An important customer of audit services is the board of directors. The board has a duty of care that requires board members to be aware of threats of all types to the organization, and to seek assurances regarding the organization's ability to protect against and recover from the potential consequences of those threats. Assurances come from management and independently from the auditors. So the board has a close relationship with its auditors.

In order to get the attention of the board, CIP and information security must be presented in the context of the business case. The business case for CIP is described by CIAO's Nancy J. Wong in an article on the ITAudit.org Forum, October 1, 2001. Information security and CIP issues of interest to governance and executive management include 1) the potential for negative impacts on shareholder values; 2) insurance issues, both for the organization and for directors and officers liability; 3) third-party liability for cyber attacks and privacy violations; and 4) increasing regulation and legislation. (For more on this subject, see www.CIAO.gov)

The growth and pervasiveness of electronic commerce, and the increasing dependence on information technology are well recognized. Information security professionals and auditors also recognize the need to improve security in virtually all areas of critical infrastructures. A key message is that most of the critical infrastructures we depend on are managed in the private sector. Today, no government alone can protect any nation from cyber attacks — from common denial of service attacks, to serious hacker intrusions, to outright cyber warfare — the private sector and government must cooperate to provide effective protection.

The measures of effective information security management will come primarily from the private sector, but with close government coordination. Improvements in "generally accepted" practices will come out of the work of the CIP ISACs (Information Sharing and Analysis Centers), improvements in standards initiatives such as the one resulting in ISO 17799, collaborative works like the products of the Center for Internet Security (CIS), and the Generally Accepted Systems Security Principles (GASSP) committee.

The IIA and the auditing profession can best use our leverage to address information security issues in governments, in corporate boardrooms, with senior management, and with other professional groups to influence the "tone at the top" which will improve the security and preparedness climate throughout all levels of the organization.

What is The IIA doing?

The IIA has conducted a series of CIP projects. The emphasis has been on communicating information security issues to the board. The National Association of Corporate Directors helped IIA address this often technical subject in the language of board members and senior executives. Numerous other partner and sponsor organizations helped ensure the effectiveness of this work.

IIA's CIP work has greatly increased the visibility and positive perception of internal auditing in the eyes of many who previously knew little about us. For example, many leaders in IT and security now regard auditors as professionals who can help get concerns addressed at the highest organizational levels. Many government entities, too, are seeing auditing in a new light. And it is not so much that we have changed, but CIP has brought our profession much more attention.

Products

The IIA provides numerous products and services relative to the auditor's roles in information security, including reports on electronic commerce and corporate governance. IIA's CIP projects produced three reports and seven conferences dealing with governance, management, and assurance for information security.

Reports

IIA provides a three report series titled "*Information Security Management and Assurance: A Guide for Directors and Executives*." The first report, "*Information Security Management and Assurance: A Call to Action for Corporate Governance*," is written for board members. It emphasizes information security principles and sound management practices and provides 10 questions board members should ask to begin assessing information security assurance for their organizations. The second report, "*Information Security Governance: What Directors Need to Know*," is also for board members, and provides answers for the 10 questions in the first report. The third report, "*Building, Managing, and Auditing Information Security*," is for management below the board level. The reports are supported by case studies from leading corporations: BellSouth, GM, Home Depot, IBM, Intel, Microsoft, Oracle, Sun, and more.

Conferences

IIA and its partners and sponsors held six Critical Infrastructure Assurance Conferences in 2000. The first conference, held April 18, 2000 at the White House, included such speakers as the president's chief of staff, two Cabinet Secretaries, a Federal Reserve Board director, the "National Coordinator for Security, Infrastructure Protection and Counter-Terrorism," and numerous representatives from leading corporations. The most recent conference was held May 15, 2001 in Washington, D.C., at the U.S. Chamber of Commerce.

Media coverage at the "*Audit Summits*," as they have become known, included live Web-casting, onsite reporters from all media, television evening-news spots, and transcriptions of speakers' messages on web sites. In January, the "*Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities*," presented to the Congress, mentioned the work of The IIA, our partners, our conferences and reports, even our corporate sponsors and conference speakers. Internal auditing is in the spotlight, and IIA will continue our work in information security.

IIA Affiliates Around the World

IIA headquarters provides presentation packages to affiliates telling about the CIP project, providing a copy of the "*Guide for Directors and Executives*" reports, a scripted PowerPoint presentation, and a videotape. The videotape features key conference speakers, a TV newscast from our Dallas conference, and a two-minute segment taped for The IIA by then president Bill Clinton. IIA field services representatives help affiliates find CIP speakers, including staff from the U.S. Critical Infrastructure Assurance Office (CIAO) and the U.S. Secret Service.

IIA members have been some of the best speakers at the "Audit Summits." From chief audit executives to technical audit specialists, they told stories and provided insights that put our published guidance in a real-world perspective. Information provided by the Summit speakers also provided much of the materials to produce the second and third reports in the series.

Where do we go from here?

IIA is working with the Partnership for Critical Infrastructure Security to take the Audit Summits outside the USA. (See: www.PCIS-Forum.org.) Canada's Associate Deputy Minister of National Defense expressed interest in working with The IIA. We are talking with IIA-UK about the Information Assurance Advisory Council (www.iaac.ac.uk, a U.K. organization similar to the PCIS) and about working with the European Confederation of Institutes of Internal Auditing to hold a CIP conference in Europe. IIA Australia is participating in a bilateral project between industry and government in the U.S. and Australia. The PCIS is opening doors in Japan, Germany, and elsewhere.

The IIA has other CIP initiatives. IIA is a founding partner in both the PCIS and the Center for Internet Security (CIS, see www.CISecurity.org). IIA continues to support the efforts of the Generally Accepted Systems Security Principles (GASSP) committee of the International Information Security Forum (I^2SF). IIA will stay active with as many CIP partners as possible in researching and publishing new SAC reports. To keep up with us, visit www.ITAudit.org.

IIA is stepping up to the challenges of the electronic economy and critical infrastructure protection in a big way. With the outstanding leadership examples among our membership, some hard-working staff members, and new opportunities to arrange partnerships and alliances, "Progress through Sharing" has never worked better than it is working now in the eBusiness era.

