Michael Power, a partner in the Ottawa office of Gowling Lafleur Henderson LLP, provides strategic and legal advice to public and private sector clients in the areas of privacy, information technology security and electronic government. Mr. Power also serves as Gowlings’ Chief Privacy Officer. He currently is a member of the National Executive of the Privacy Law Section of the Canadian Bar Association; the Canadian Information Technology Law Association, and the American Bar Association’s Cyberspace Law Committee.


Prior to joining Gowlings, Mr. Power held various positions within the Department of Justice, Treasury Board of Canada Secretariat and the Department of Foreign Affairs and International Trade, which included responsibilities for legal advice, policy development and issue management pertaining to information technology, electronic commerce and international trade and investment issues.

He recently collaborated in writing “Sailing in Dangerous Waters: A Director’s Guide to Data Governance” to be published by the American Bar Association in August 2005.

Contact him at michael.power@gowlings.com

Recent publications:


"Franchising and data protection in Canada" (2005) 3 International Journal of Franchising Law 7 (with Louis Benoit)

"Ontario & Health Information Privacy: Legislation Finally Arrives" (2005) 2 Can. Privacy Law Rev. 73 (with Louis Benoit)

Roland Trope is partner in the New York offices of Trope and Schramm LLP. He advises multi-national companies, investment firms and foreign governments on cross-border transactions, compliance with privacy and information security laws and regulations, trade sanctions, export and defense trade controls, antitrust, development and protection of intellectual property portfolios, cyberlaw, e-commerce, corporate governance and defense procurements.

Mr. Trope serves as Adjunct Professor in the Department of Law at the United States Military Academy at West Point and at the U.S. Defense Institute for Security Assistance Management at Wright-Patterson Air Force Base. He is a co-editor of the Digital Protection Department and the Privacy Department columns in the journal Security & Privacy published by the Institute of Electrical and Electronic Engineers (IEEE).

Mr. Trope earned a Juris Doctor from Yale Law School in 1980, a B.A. and M.A. in English Language and Literature from Oxford University in 1972 and 1976 (as a Marshall Scholar and Danforth Fellow), and a B.A. in Political Science from the University of Southern California in 1969.

He is an active member of the Information Technology Committee of the Association of the Bar of the City of New York and Cyberspace Law Committee of the American Bar Association.

He co-authored the book Sailing in Dangerous Waters: A Director's Guide to Data Governance, which will be published by the American Bar Association in August 2005. His recent publications include:

- **Checkpoints in Cyberspace:** Best Practices for Averting Liability in Cross-Border Transactions (co-author), a treatise published in April 2005 by the American Bar Association;
- **Directors’ Digital Fiduciary Duties,** IEEE Security & Privacy, January/February 2005;
- “Staple Article”: In Defense of Betamax and Its Progeny, (co-author), Business Lawyer, November 2004;
- **A Warranty of Cyberworthiness,** IEEE Security & Privacy, March/April 2004;
- **Guarding Against Terrorism – And Against Liability,** IEEE Spectrum, January 2004.
Bar Admissions:
1982, New York
1984, Minnesota
2004, U.S. Southern District and Eastern Districts of New York

Memberships:
American Bar Association
Association of the Bar of the City of New York
Bar Committees in ABCNY:
    2002 – present  Information Technology
    1999 – 2002  Trademarks and Unfair Competition
    1996 – 1999  Copyright and Literary Affairs
    1993 – 1996  Military Affairs and Justice
Japan Society
New York – Singapore Association, Board of Directors (2004 – present)
Nippon Club
SAILING IN DANGEROUS WATERS

A Director’s Guide to Data Governance

by

E. Michael Power and Roland L. Trope
ORGANIZATIONS AS SUBMARINES

WHY DATA GOVERNANCE IS IMPERATIVE
OVERVIEW

• ORGANIZATIONS AS SUBMARINES
  ✦ Data Governance: an imperative

• WEATHER REPORT
  ✦ Digital Perfect Storm?

• PRESENT & EMERGING SEASCAPE
  ✦ Legal obligations & risks

• VIEW THROUGH THE PERISCOPE
  ✦ Questions from Directors to Management

• CONCLUSION
OBJECTIVES

• Provide Board a briefing on *data governance* highlighting:

  ✦ Why the Board should monitor it.

  ✦ Recently emerged “legal drivers” that make it a priority.

  ✦ Questions that Board should ask senior management.

  ✦ Criteria to evaluate management’s responses.
“DATA GOVERNANCE”

• Mechanisms to manage the risks are:

  ✦ Company policies and procedures for ensuring proper control of:

  ❖ Information security

  ❖ Record or document retention, and

  ❖ Data privacy.
“DATA GOVERNANCE”

• Formal definition

✧ Risk management to minimize damage that unauthorized handling of data may cause.

✧ Risks of physical, procedural or technical errors or omissions that cause unauthorized
  ❖ Collection or use
  ❖ Access or disclosure
  ❖ Modification or destruction
  of information generated or entrusted to organizations.
IMPORTANCE OF DATA GOVERNANCE

- Breakdowns in data governance can cause company crisis
  ✦ Adverse publicity ("headline" risks)
  ✦ May incur liability
    ✤ For company
    ✤ For officers & directors
  ✦ Weakens integrity
  ✦ Undermines reputation
  ✦ Cause financial loss
  ✦ Less costly to reduce than remediate
“Human history is more and more a race between education and catastrophe”

--H.G. Wells
AVOID REGARDING YOUR ENTERPRISE AS A CASTLE

(A STATIC TARGET, WITH CLEAR VIEW OF THREATS ON HORIZON)
CONSIDER YOUR ORGANIZATION A SUBMARINE

(A MOVING TARGET, SEEKING TO DETECT DYNAMICALLY CHANGING THREATS)
ANALOGY:

COMPANIES TO MODERN SUBMARINES

- Companies resemble modern submarines in that they:
  - Use information technology
  - Operate in high-risk environment
  - Need to readily identify emerging risks and threats
  - Must continuously scan against incoming attacks
  - Need their information technology systems to remain operational
WEATHER REPORT: A DIGITAL PERFECT STORM?
“Professor,” replied Captain Nemo, “you must not confuse static and dynamic situations, or you will fall into serious error.”

Jules Verne

20,000 Leagues Under the Sea
DIGITAL “PERFECT STORM”

• Impending “perfect storm” in electronic environments means companies face:
  ✦ False sense of information assurance
  ✦ Imperiled internal controls
  ✦ Reduced margin of error of security
  ✦ Weaker protection of information assets
  ✦ Increased frequency of serious incidents
ELEMENTS OF DIGITAL “PERFECT STORM”

1. Unabated Severity & Growing Diversity of Internal Risks

2. Decline in Relative Importance of Perimeter Defenses

3. Rapid Evolution of External Threats

4. Continued Production & Use of Vulnerable Software
5. Legal Trends Towards Imposing Liability

6. Investor Scrutiny of Company Information Security

7. Reliance on the Wrong Assumption
GROWING SEVERITY OF INTERNAL RISKS

• RISK:
  ✦ Most successful attacks come from *inside* target company
  ✦ *Weakest link* is not technology, but people

• RESPONSE:
  ✦ Directors must ensure greater diligence in managing internal risks
PERIMETER DEFENSES: NECESSARY, BUT NOT SUFFICIENT

• RISK:
  ✦ Over reliance on perimeter defenses
  ✦ Threats are more complex
  ✦ Boundaries between “inside” and “outside” company are blurring
    ✤ From increased IT outsourcings
    ✤ From integrated supply-chains

• RESPONSE:
  ✦ *Think dynamic, not static*
  ✦ Focus security on protecting information wherever accessed, as opposed to protecting corporate systems
RAPID EVOLUTION
OF
EXTERNAL THREATS

• RISK:
  ✦ Companies will have far less time to react to security threats
    ❖ Strains of malicious code are rapidly evolving
    ❖ Cyber-attacks no longer take months to exploit a disclosed vulnerability
    ❖ Exploits occur in days or hours

• RESPONSE:
  ✦ Anticipate “zero-day” attacks -- launched before a defensive “patch” is available
  ✦ Promote early awareness of emerging means of attack
PRODUCTION AND USE OF VULNERABLE SOFTWARE

• RISK:
  
  ✦ Inadequate “patch” management by:
    
    ❖ Failing to patch in a timely manner
    
    ❖ Using automated downloading of “patches without testing for system compatibility”

• RESPONSE:
  
  ✦ Ensure “patch” management strategy is in place:
    
    ❖ Minimize installation of insecure code
    
    ❖ Be aware that patching cannot keep pace with emerging threats
Legal Trends
Towards
Imposing Liability

• RISK:
  ✦ Federal & state legislation create information-related obligations
    ✤ Existing and emerging *duties to disclose* breaches of information security
  ✦ Judicial decisions hold supervisory personnel liable for security deficiencies
    ✤ Directors potentially liable for failure to fulfill fiduciary duty to remediate deficient security

• RESPONSE:
  ✦ Directors need to review fiduciary obligations in light of recent legal decisions
  ✦ Companies need to manage required or pressured disclosures
Advent of Digital Lockbox Alters Information Security

• In Digital and Internet Eras:

  ✦ Mode of storage of information asset is **digital lockbox** (computer hard drive)

  ✦ Putting the asset into digital lockbox makes **asset and storage unit inseparable**.

  ✦ Attacks on the lockbox are attacks on the assets (the digitized data).

• *Protection, security and accounting* of asset merges with protection, security and accounting of *method of storage*. 
INVESTOR SCRUTINY OF COMPANY DATA GOVERNANCE

• RISK:

  ✦ Security breaches can cause long-term disruptions of operations:

• RESPONSE:

  ✦ Investors can be expected to judge such companies harshly
    ✦ ChoicePoint shares lost 18% of value

  ✦ Directors must avoid negative market reaction to poor data governance
Disclosure Risks

“Our outside auditors have identified weaknesses in our internal controls that could affect our ability to ensure timely and reliable financial reports.”

Warner Music Group Corp
Preliminary Prospectus for $750M IPO
March 2005
RELIANCE ON THE WRONG ASSUMPTION

• **RISK:**
  ✦ Directors’ share common misconception -- that their company information technology (IT) systems are “presumptively” safe
  
  ✤ Reflects misplaced trust in insufficiently examined IT systems & internal controls

• **RESPONSE:**
  ✦ Presume IT systems are *insecure* until proven otherwise
“Presumptively Safe”
IT Systems of Banks

- Automated, malicious code: *Troj/BankAsh-A*
  - Secretly downloads onto a computer
  - Waits until user seeks connection with one of several bank web sites -- targets:
    - Barclays
    - Bank of Scotland
  - Hijacks user’s computer & displays counterfeit log-on page
  - Records victims’ account information as they type it in
PRESENT AND EMERGING SEASCAPE:

LEGAL OBLIGATIONS AND RISKS
LEGAL OBLIGATIONS AND RISKS

1. Fiduciary Duty of Care

2. Sarbanes-Oxley Act

3. Health Insurance Portability and Accountability Act

4. Gramm-Leach-Bliley Financial Services Modernization Act

5. U.S. Sentencing Guidelines

6. State Laws
LEGAL OBLIGATIONS
AND RISKS

7. Basel II

8. International Privacy Laws


10. Export Controls

11. Contractual Requirements

12. “Litigation Hold” Orders
“Our outside auditors have identified weaknesses in our internal controls that could affect our ability to ensure timely and reliable financial reports.”

*Warner Music Group Corp*
*Preliminary Prospectus for $750M IPO*
*March 2005*
**The Effect of Regulatory Interest**

“The Federal Reserve has told **Citigroup** to delay plans for big takeovers until it tightens internal controls and addresses regulatory problems at home and abroad.”

“Citigroup Told to Fix Problems Before Any Mergers”
"In our opinion, because of the effects of the material weaknesses described above on the achievement of the objectives of the control criteria, Tasty Baking Company has not maintained effective internal control over financial reporting as of December 25, 2004 ..."

PricewaterhouseCoopers LLP
Tasty Baking Co.
10-K
Filed, March 25, 2005
Lessons From Review of “Legal Drivers”

• Directors should pursue these priorities when discussing data governance with senior management:
  ✦ Data governance policies
  ✦ Information systems
  ✦ Information security risk assessment
  ✦ Avoidance of internal risks
  ✦ Lines of authority and responsibility for information security
  ✦ Awareness of when activities trigger additional compliance duties for information security

• These provide the “tactical picture” that Directors need.
QUESTIONS FOR DIRECTORS TO POSE TO MANAGEMENT
FRAMEWORK FOR QUESTIONS

• Plan the lines of inquiry to construct clear “tactical picture”

• Obtain “snapshots” of critical assets and risks

• Develop a “tactical mosaic” of status of company data governance
KEY
“SNAPSHOTS” NEEDED FOR TACTICAL PICTURE

• Organization’s business context
  ✦ Identify critical information assets
  ✦ Its “information sharing” activities
  ✦ How it limits access to information
  ✦ Risks and threats to information assets

• Organization’s data governance
  ✦ Organization’s policies and procedures pertaining to information
  ✦ Legal rules applicable to information
“TACTICAL PICTURE” OF INFORMATION

- Full picture should include:
  - Data flows,
  - Information assets,
  - Policies, procedures & agreements
  - Threat detection & assessment
  - Defenses and counter-measures
  - Security downgrades & upgrades
  - Applicable legal rules
  - Evidence for attestation of internal controls
  - Audits, deficiencies & corrections
OBJECTIVE ACHIEVED WITH “TACTICAL PICTURE”

• These “snapshots” reveal:
  ✦ Information assets at stake
  ✦ Probable risks and threats to assets
  ✦ Strengths and weaknesses in company’s protective measures
  ✦ Needs for additional safeguards

• Directors need to exercise business judgment and determine
  ✦ Appropriate level of firm’s security commensurate with value and sensitivity of information assets that a breach would compromise
PRACTICAL QUESTIONS FOR DIRECTORS TO CONSIDER

• Questions arranged in 4 broad categories:

1. Policies and Procedures
2. Organizational Measures
3. Assessments and Updates
4. Mitigation and Responses to Security Incidents

• Each question is accompanied by commentary for assessing answers
QUESTIONS
ON
MITIGATION AND RESPONSES
TO SECURITY INCIDENTS
ARE OUR SYSTEMS AUDITED FOR SECURITY?

DO THE AUDITS COVER OUTSOURCED SERVICES?
SYSTEM AUDITS

• AIM:
  ✦ Ensure that hardware & software controls are correctly implemented

• ASSESSMENT:
  ✦ Audits should conduct:
    ❖ Reconnaissance testing (check for surveillance -- a prelude to an attack)
    ❖ Vulnerability assessments
    ❖ Penetration testing (check if personnel promptly detect & properly react to intrusions)
  ✦ Audits should be:
    ❖ Well defined & documented
    ❖ Adequately funded
    ❖ Conducted annually
    ❖ Required of third-party outsource vendors
DO WE CONDUCT SECURITY REVIEWS OF EVERY NEW TECHNOLOGY THAT IS FORMALLY OR INFORMALLY INTRODUCED INTO THE ORGANIZATION?

ARE THOSE REVIEWS A HIGH PRIORITY?
SECURITY REVIEWS OF NEW TECHNOLOGIES

• AIM:
  ✦ Avert introducing unsuspected vulnerabilities

• ASSESSMENT:
  ✦ Omission of security checks of new technologies is material deficiency
  ✦ Such checks should be high priority
  ✦ Reviews should reflect best countermeasures, e.g.,
    ✦ FDIC guidance on Instant Messaging security risks
    ✦ NIST guidance on VoIP security risks
    ✦ GAO guidance on Wireless Network risks
HAVE WE ESTABLISHED “INCIDENT MANAGEMENT” PROCEDURES?

WHAT DO THE PROCEDURES COVER?
INCIDENT MANAGEMENT PROCEDURES

• AIM:
  ✦ Procedures must address critical incidents:
    ❖ Information system failures
    ❖ Loss or denial of service
    ❖ Errors from incomplete or inaccurate data
    ❖ Breaches of confidentiality

• ASSESSMENT:
  ✦ Absence of procedures is concern
  ✦ Procedures should:
    ❖ Identify cause of incident
    ❖ Execute corrective & preventative measures
    ❖ Collect audit trail records
    ❖ Alert third parties of possible risks
DO WE HAVE SECURITY INCIDENT REPORTING PROCEDURES IN PLACE?

DO WE LEARN PROMPTLY AND CLEARLY OF SERIOUS INCIDENTS?
SECURITY INCIDENT REPORTING

• **AIM:**
  ✦ Minimize damage from incidents
  ✦ Learn lessons from each incident

• **ASSESSMENT:**
  ✦ Request evidence that all personnel and contractors:
    ❖ Are aware of procedures for prompt reporting
    ❖ Can differentiate the different types of incidents and the risks they pose
CONCLUSIONS

• Data governance has intrinsic importance beyond risk-of-investment calculations
  - Breaches occur despite good security
  - Deficient security exists where breach has not yet occurred

• Data governance is continuous process

• Management must ensure vigilance against evolving threats.

• Directors must ensure efforts are effective for organization’s assets, environment and risk tolerance.
TAKE AWAY: SIX MESSAGES

1. Data security paradigms are changing (from inside & outside companies).

2. Information assets are at risk, and both practices and problems will be subject to regulatory scrutiny and/or legal liability.

3. Accountability remains with company that creates or gathers the data.

4. Replace obsolete, static “fortress” model with dynamic, continuous process model.

5. Adopt life-cycle view of data governance.

6. Extrapolate from risks and regulations to best practices before needed or required.
QUESTIONS
DATA GOVERNANCE ISSUES

Francoise Gilbert  
IT Law Group Palo Alto, CA  
www.itlawgroup.com

Compilation of published and unpublished articles prepared by Francoise Gilbert, alone or in cooperation with other authors, as indicated.

1. Sample Checklist for an Information Security Program  
2. Drafting and Maintaining a Privacy Program  
3. FACTA – New Shredding Rules as of June 1, 2005  
4. Document Retention and Destruction

Francoise Gilbert is the founder and managing director of the IT Law Group, based in Palo Alto, California – www.itlawgroup.com. She concentrates her practice on information management legal issues, including information technology transactions, information privacy, and information security counseling. Ms. Gilbert also serves on the Board of Directors or Board of Advisors of several technology start-ups and non-profit organizations based in Silicon Valley.

Ms. Gilbert is an Adjunct Professor of Law at the University of Illinois, Chicago Campus, and a Co-Chair of the PLI Privacy Law Institute. Ms. Gilbert has advised lawmakers on policy and regulatory issues, including the Western Governors Association and a U.S. Senator. She has held leadership positions with the American Bar Association and the Chicago Bar Association.

Before founding the IT Law Group, Ms. Gilbert was a partner in two national law firms based in Chicago, IL and in Palo Alto, CA. Ms. Gilbert holds laws degrees from Loyola University (Chicago, Illinois) and University of Paris (France), and a BS, an MS and a graduate degree in Mathematics. She is admitted to practice law in California, Illinois, and France.

Contact information:

Phone: 650-804-1235

Email: fgilbert@itlawgroup.com
Information security protections are necessary to maintain the confidentiality, integrity, and availability of personally identifiable information, which are essential for healthy electronic commerce. A company that lacks adequate protections risks inadvertent disclosure or misuse of critical data, with resulting loss of public trust, and potential legal action. For example, poor access controls and procedures might expose to hacking of the company’s databases. A misdirected email may reveal the identity of individuals who legitimately expected their personal information to remain confidential. Hacking and other security violations may be widely publicized, and can seriously damage the company's community standing, result in identity theft, or cause personal embarrassment. Class action lawsuits and investigations by government agencies may ensue.

US and foreign data privacy and security laws and regulations require companies to implement information security measures to protect certain personal data they maintain about employees, customers or prospects. For example, corporate governance legislation requires public companies to ensure that they have implemented appropriate information security controls with respect to their financial information. California AB 1950, which became effective on January 1, 2005 requires companies to implement security measures to protect the security of specified information of California residents. In addition, the Federal Trade Commission and State Attorneys General have adopted a consistent approach in their actions against perceived offenders (companies whose security did not match the representations made to the public), which has begun to establish “best practices.”

This document attempts to summarize the activities, subject matter, and documents that are typically involved in defining an enterprise information security protection program. Since these plans can apply equally to the protection of personally identifiable information as well as other company data or materials, such as financial data or corporate records, this document uses the generic term “data” to refer to the information, documents, or technologies to be protected.

Components of an Enterprise Security Program

The goal in creating a security program is to protect data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to:
- Preserve the confidentiality of information in order to protect individuals’ privacy and company’s proprietary information
- Guard against improper modification or destruction of data, or ensure data integrity, authenticity and non repudiation of the communication
- Ensure timely and reliable access to information
- Assuring the identity of the users and validating their access.

Numerous considerations determine the security parameters. These include, for example: the data, application, and networks of the company; the company’s business plan and strategic goals; the company’s culture; the legal environment; technical technological considerations; business continuity requirements, standards and best practices; or return on investment and financial constraints.

To establish a successful enterprise security program, a company should first outline a plan to define the overall strategy that will serve as the guide to securing its systems, networks, and data. Security policies and the related procedures should then be drafted and implemented. Security policies are high-level statements about the measures to be taken, while the procedures move the policies into action through the organizations’ people and processes.

A security program is usually developed in several phases:

- Governance: e.g. identify assets to be protected, the potential threats and the risks; identify the legal requirements, laws and regulations regarding information security, information privacy, documents retention, etc.; integrate into financial constraints
- Security integration and security operations: e.g., determine the controls needed, develop policies and procedures
- Implementation and evaluation: implementation, training, testing, evaluation, and correction of weaknesses.

**WHAT IS REQUIRED FOR A SECURITY PROGRAM?**

There are many technological standards, such as ISO 17799, which is becoming a recognized practice for security management in many private and public organizations.

The legal standards are beginning to emerge. While most laws have simply established a requirement to provide security, regulations issued in connection with the Gramm Leach Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) have provided guidelines that are more detailed. The Federal Trade Commission and the State Attorneys General have also established certain requirements in their respective consent decrees issues at the completion of investigations of companies that had suffered breach of security and data spills.

The trends in these different regulations and rulings would require companies to:
- Conduct periodic risk assessments
- Develop and implement a security program to manage and control the risks identified
- Oversee third party service providers
- Implement security awareness, training and education
- Monitor and test the program to ensure its effectiveness.
- Review and adjust the program in light of ongoing technical and legal changes
- Obtain regular independent audits and reporting.

Measures designed to provide information security are generally grouped in three categories, which are typically referred to as:
   - Physical security measures
   - Administrative security measures
   - Technical security measures.

The remainder of this document provides examples of typical physical, administrative or technical security measures. It is not meant to be exhaustive, more to provide a complete checklist of required items in the creation of an enterprise security program.

**PHYSICAL SAFEGUARDS**

Physical security measures are designed to protect the tangible items that comprise the physical computer system and network that stores the data, including servers, terminals that have access to the system, storage devices and the like.

Examples of physical security measures follow:
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>EXAMPLE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FACILITY ACCESS CONTROLS</td>
<td>- Accessories Accessories</td>
<td>Physical safeguards are security measures to protect the company's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. Company should defined the measures required to limit access to specific areas of the company, the physical components of a facility that are related to security for example, hardware, walls, doors, and locks. Facility access controls include, for example, policies and procedures for verifying access authorizations before physical access, maintenance records, need-to-know procedures for personnel access, sign-in for visitors, visitor escort, if appropriate, equipment control (into and out of site).</td>
</tr>
<tr>
<td></td>
<td>- Facility security plan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Access control and validation procedures</td>
<td></td>
</tr>
<tr>
<td>CATEGORY</td>
<td>EXAMPLE</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CONTINGENCIES</td>
<td>- Contingency operations</td>
<td>Facility access controls also include limiting physical access to a company in unusual circumstances while ensuring that properly authorized access is allowed such as disaster recovery, emergency mode operation, and testing and revision.</td>
</tr>
<tr>
<td></td>
<td>- Maintenance records</td>
<td>Company should implement policies and procedures to document repairs and modifications to these physical components of its facilities.</td>
</tr>
<tr>
<td></td>
<td>- Repairs</td>
<td>A retrievable, exact copy of the data should be made, where needed, before equipment is moved or software is upgraded.</td>
</tr>
<tr>
<td></td>
<td>- Protection of data in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>migrations</td>
<td></td>
</tr>
<tr>
<td>WORKSTATIONS</td>
<td>- Workstation use</td>
<td>Policy and guidelines on workstation use and security provide instructions and procedures delineating the proper functions to be performed, and the manner in which those functions are to be performed (for example, logging off before leaving a workstation unattended) to maximize data security.</td>
</tr>
<tr>
<td></td>
<td>- Workstation security</td>
<td></td>
</tr>
<tr>
<td>DEVICE AND MEDIA CONTROLS</td>
<td>- Disposal of devices and</td>
<td>Device and media controls involve policies and procedures that govern the receipt and removal of hardware and software (for example, diskettes and tapes) into and out of a facility. This includes static and removable devices, and use, re-use or recycling of media containing mass storage.</td>
</tr>
<tr>
<td></td>
<td>media</td>
<td>Audit trail implementation requires recording a person’s actions relative</td>
</tr>
<tr>
<td></td>
<td>- Media re-use</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Accountability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Data backup and storage</td>
<td></td>
</tr>
<tr>
<td>CATEGORY</td>
<td>EXAMPLE</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to the receipt and removal of hardware and/or software into and out of a facility that are traceable to that person. The impact of maintaining accountability on system resources and services will depend upon the complexity of the mechanism to establish accountability. The data a company needs to backup, and which operations should be used to carry out the backup, should be determined by the company's risk analysis and risk management process. The data backup plan, which is part of the contingency plan, should define exactly what information is needed to be retrievable to allow the company to continue business as usual in case of damage or destruction of data, hardware, or software. The extent to which e-mail backup is needed will be determined through that analysis.</td>
</tr>
</tbody>
</table>
**TECHNICAL SECURITY MEASURES**

Technical security measures involve the use of safeguards incorporated into computer hardware, software and related devices. They are designed to ensure system availability, provide access control, authenticate persons seeking access, protect the integrity of information communicated through the system and stored on the system, and ensure confidentiality where appropriate. Example of technical measures include firewalls, access control software, antivirus software, passwords, PIN numbers, smart cards, biometrics, tokens, encryption, dialup access controls, VPNs or call back systems.

Below are examples of typical technical security measures.

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>EXAMPLE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS CONTROL</td>
<td>- Unique user identification</td>
<td>Access controls include, for example, the use of unique user identification, provision for emergency access procedures, use of encryption, and use of automatic logoff.</td>
</tr>
<tr>
<td></td>
<td>- Emergency access procedure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Automatic logoff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Encryption and decryption</td>
<td>Encryption is a method for denying access to information in a file. It provides confidentiality.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access controls are necessary under emergency conditions, as well, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or other disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed data.</td>
</tr>
<tr>
<td>AUDIT CONTROLS</td>
<td>- Audit controls</td>
<td>Audit control mechanisms are required to record and examine system activity. They provide a means to assess</td>
</tr>
</tbody>
</table>
activities regarding the use of, or access to data in the company's care.

To comply with certain laws, the company may have to provide an accounting of certain disclosures of data to an individual upon request.

**AUTHENTICATION**
- Person or company authentication allows the corroboration that the person or company is who it/he/she claims to be. Numerous mechanisms may be used to authenticate companies, such as digital signatures and soft tokens.

**TRANSMISSION SECURITY**
- Integrity controls
- Encryption

Data must be protected in a manner commensurate with the associated risk when it is transmitted from one point to another. To do so, the company needs to implement appropriate mechanisms to ensure that electronically transmitted information is not improperly modified without detection.

**ADMINISTRATIVE SECURITY MEASURES**

Administrative security measures include, for example, management procedures and constrains, operation procedures, accountability procedures and other administrative controls to prevent unauthorized access to data, and provide an acceptable level of protection for computing resources and data. They frequently include personnel management, training, and discipline.

Below are examples of typical administrative measures.
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>EXAMPLE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURITY MANAGEMENT PROCESS</td>
<td>- Risk analysis</td>
<td>Implementing a comprehensive security program requires a thorough assessment of the potential risks for the data: identifying the foreseeable threats to the data, assessing the likelihood that the threat will materialize, evaluating the potential damage that will result if it materializes, and defining applicable policies and procedures to address the threat.</td>
</tr>
<tr>
<td></td>
<td>- Risk management</td>
<td>This process is required before designing the information security policies and procedures, and must be performed again on a regular basis to update the program in view of changes.</td>
</tr>
<tr>
<td></td>
<td>- Sanction policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Information system activity review</td>
<td></td>
</tr>
<tr>
<td>ASSIGNED SECURITY RESPONSIBILITY</td>
<td>- CPO / CSO</td>
<td>The final responsibility for security should be assigned to one individual with sufficient authority to ensure the progress, and implementation of the program. Responsibilities would include the management and supervision of the use of security measures to protect the data, and the conduct of personnel in relation to data protection.</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>EXAMPLE</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WORKFORCE SECURITY</td>
<td>Authorization and/or supervision</td>
<td>Workforce members, (e.g., operations and maintenance personnel) should be supervised or have authorization when working with data or in locations where data resides.</td>
</tr>
<tr>
<td></td>
<td>Workforce clearance procedures</td>
<td>The need for and extent of a screening process is based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective personnel screening processes may be applied to allow a range of implementation, from minimal procedures to more stringent procedures based on the risk analysis.</td>
</tr>
<tr>
<td></td>
<td>Termination procedures</td>
<td>Restrictions on workforce members will be dependent upon job responsibilities, the amount and type of supervision required and other factors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Termination procedures are essential because of the risks associated with the potential for unauthorized acts by former employees, such as acts of retribution or use of proprietary information for personal gain. The termination procedure documentation should include security-unique actions to be followed, such as, revoking passwords and retrieving keys when a termination occurs.</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>EXAMPLE</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>INFORMATION ACCESS</td>
<td>- Isolating different company functions</td>
<td>Establish and maintain formal, documented policies and procedures defining levels of access for all personnel authorized to access data, and how access is granted and modified.</td>
</tr>
<tr>
<td>MANAGEMENT</td>
<td>- Access authorization</td>
<td>Restrict access to those persons and companies with a need for access is a basic tenet of data security. By this mechanism, the risk of inappropriate disclosure, alteration, or destruction of information is reduced.</td>
</tr>
<tr>
<td></td>
<td>- Access establishment and modification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Which participating parties and access privileges relative to data elements will be appropriate will vary depending upon the company, the needs within the user community, the system in which the data resides, and the specific data being accessed.</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>EXAMPLE</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SECURITY AND PRIVACY AWARENESS</td>
<td>- Security and privacy reminders</td>
<td>Security and privacy awareness requires training of the workforce as reasonable and appropriate to carry out their functions in the facility.</td>
</tr>
<tr>
<td>AND TRAINING</td>
<td>- Protection from malicious software</td>
<td>Most of the security mishaps occur because of poorly trained personnel. Each individual who has access to data must be aware of the appropriate security measures to reduce the risk of improper access, uses, and disclosures.</td>
</tr>
<tr>
<td></td>
<td>- Log-in monitoring</td>
<td>Consider, for example, initial training and refresher, periodic reminders, user education concerning virus protection and other technology threats, user education in the importance of monitoring login success/failure, and how to report discrepancies, and user education in password management.</td>
</tr>
<tr>
<td></td>
<td>- Password management</td>
<td>The amount and type of training needed will be dependent upon a company’s configuration and security risks.</td>
</tr>
<tr>
<td></td>
<td>- Training</td>
<td>Amount and timing of training should be determined by each company. Training should be an on-going, evolving process in response to environmental and operational changes affecting the security of the protected information.</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>EXAMPLE</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| SECURITY INCIDENT PROCEDURES           | - Response and reporting | The program should include security incident procedures: formal, documented report and response procedures so that security violations are reported and handled promptly, and documented.  

Whether a specific action would be considered a security incident, the specific process of documenting incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon a company's environment and the information involved.  

The security incident procedures may involve only internal reporting, or external reporting depending on legal requirements and contractual obligations.  

Improper network activity should be treated as a security incident, because, by definition, it represents an improper instance of access to or use of information.  

Security incidents include misuse of data. |
<p>| CONTINGENCY PLAN                       | - Data backup plan       | A contingency plan must be in effect for responding to system emergencies. It may include an applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures. |
|                                        | - Disaster recovery plan |                                                                                                                                                                                                     |
|                                        | - Emergency mode         |                                                                                                                                                                                                     |</p>
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>EXAMPLE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>operation plan</td>
<td>A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed. The contents of any given contingency plan will depend upon the nature and configuration of the company devising it. Dependent upon its size, configuration, and environment, the company should decide whether and when testing and revision of the contingency plan should be done.</td>
</tr>
<tr>
<td></td>
<td>- Testing and revision procedure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Applications and data criticality analysis</td>
<td></td>
</tr>
<tr>
<td>EVALUATION</td>
<td>- Evaluation</td>
<td>Periodically conduct an evaluation of security safeguards to demonstrate and document compliance with the company’s security policy. Company should assess the need for a new evaluation based on changes to its security environment since the last evaluation, such as, new technology adopted or responses to newly recognized security risks.</td>
</tr>
</tbody>
</table>

**POLICIES, PROCEDURES AND DOCUMENTATION**

The physical, technical, and administrative measures described above must be recorded in writing, and implemented throughout the company, and with its subcontractors as well.
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>EXAMPLE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>POLICIES AND PROCEDURES</td>
<td>- Create written policies, procedures</td>
<td>Create written policies and procedures and maintain the policies and procedures implemented to comply with the requirements above.</td>
</tr>
<tr>
<td></td>
<td>- Documents actions, activities or assessments taken or conducted</td>
<td>Keep a written record of the action, activity, assessment, or designation.</td>
</tr>
<tr>
<td></td>
<td>- Implement policies and procedures</td>
<td>Retain documentation according to company documents retention policy or as required by applicable law.</td>
</tr>
<tr>
<td></td>
<td>- Retain documentation related to policy creation, procedures, actions according to company’s documents retention processes</td>
<td>Make documentation available to those implementing the procedure.</td>
</tr>
<tr>
<td></td>
<td>- Availability to those implementing the procedure</td>
<td>Review the documentation periodically and update it as needed. The need for review and update will vary dependent upon a given company's size, configuration, environment, operational changes, and the security measures implemented.</td>
</tr>
<tr>
<td></td>
<td>- Periodic reviews and updates</td>
<td>Policies and procedures may be changed at any time, if the company documents the changes in accordance with the applicable requirements. There should be a minimum level of documentation of security practices. Documentation must be sufficiently detailed to communicate the security measures taken and to facilitate periodic evaluations.</td>
</tr>
<tr>
<td>THIRD PARTIES</td>
<td>- Contracts with subcontractors and other third parties</td>
<td>Contracts with subcontractors or service providers who have access to data are critical to provide satisfactory assurances that the third party will appropriately safeguard the</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>EXAMPLE</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>information in a manner consistent with the company’s requirements. Among other things, the contract must require the third party to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the data that it creates, receives, maintains, or transmits on behalf of the company;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate safeguards;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Report to the company any security incident of which it becomes aware;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Make its policies and procedures, and documentation required by the contract available for audit by the company; and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authorize termination of the contract by the company if it determines that the third party has violated a material term of the contract.</td>
</tr>
</tbody>
</table>
Privacy policies, privacy notices or privacy statements have become ubiquitous on websites. They tend to follow the same format, use the same wording, which usually follows samples published on the Internet by numerous organizations. Occasionally, it is clear that an online privacy policy was copied from another company’s website, as indicated by inadvertent errors, such as failing to remove the other company’s name or contact information…

Website privacy policies represent the tip of an iceberg that may lead companies to serious legal exposure if not addressed with the adequate scrutiny and understanding of the numerous legal issues and technical implications. There are many different types of privacy policies, from those that apply to online data, to those that apply to data collected by financial institutions, those that pertain to interaction with children under 13, those that apply to individuals protected by certain foreign laws, etc. Of course, there is not a “one size fits all.”

Developing an Enterprise Privacy Program is complex. Typically, a company will need to address privacy in many different aspects of its operation. The website, the marketing department prospect database, the pro-bono charity that involves the children’s club in town, the data received from its Italian distributor, and many other activities.

The creation of the Enterprise Privacy Program usually requires the top-down cooperation of the many players in an enterprise. The C-level executives will set the tone and approve funding for the project. The midlevel managers will develop the details of the online and offline policies and procedures, different from one department to another. The staff will be trained on, and apply the policies and procedures.

The development process and ongoing maintenance of the privacy policies and procedures will require a thorough understanding of the company’s data management practices, the technical capabilities of its computer systems. It will also require knowledge of the legal issues and restrictions imposed by a myriad of federal, state, -- and sometimes foreign -- laws, regulations, and agency rulings, on the collection, use, transfer, and protection of personal data by or on behalf of the enterprise.

This article presents an overview of the strategies and activities, and different phases, in the development of an Enterprise Privacy Program.
WHY DOES YOUR COMPANY NEED AN ENTERPRISE PRIVACY PROGRAM?

There are many reasons why a company should, or would want to implement an Enterprise Privacy Program. While in a few cases, the need may merely come out of peer pressure -- to compete with others in the same market place --, generally, however, there are actual laws and government rulings that may compel a company to pay serious attention to its personal data collection and use practices.

In the past few years, numerous information privacy and information security laws were enacted and are now in effect. As a result, companies are compelled to develop a Privacy Program to comply with the requirements placed on their industry. For example, the HIPAA Privacy Rule requires certain “covered entities” which include health plans, healthcare providers, and healthcare clearinghouses to have a privacy policy, and to communicate it to the patients. This law not only affects these covered entities, but also, as well, any company that does business with a covered entity. The HIPAA Privacy Rule places on business associates of these covered entities obligations that are almost as comprehensive as those for covered entities. However, the HHS does not have jurisdiction on the business associates. It is up to the covered entities to enforce their agreements with the business associates, and require them to comply with the prohibitions, requirements, measures, or restrictions identified in the HIPAA Privacy Rule.

There are also state laws, which complement or supplement federal laws. For example, California has just passed a law that will require any company that does business in California and operate a website, to display a privacy policy on its website. In addition, effective January 2005, California will require any company that discloses a customer’s personal information to a third party for direct marketing to provide the customer, upon request, with the names and addresses of the recipients of that disclosure, and details of what was disclosed.

Privacy policies might also be needed to respond to clients’ requirements in service contracts. For example, companies doing business with financial institutions subject to the Gramm Leach Bliley Act may have to enter into written agreements pursuant to which the subcontractor commits to comply with specific privacy and security requirements for the confidential personal financial information it receives from the financial institution.

Similarly, companies established in foreign countries, for example countries member of the European Union, will not transfer data to the United States without written commitments from their US counterpart. The US Company must agree in writing to protect the privacy, confidentiality, and security of the personal information it receives. In addition, it must agree to offer the data subjects the same rights of access, amendment, and accounting as they obtain under their local laws.

Another incentive for developing a well thought through Enterprise Privacy Program might be to avoid prosecution by the Federal Trade Commission and State Attorney General. In the past few years, several companies were prosecuted for failing to
comply with their published privacy policy. Most consent orders issued as a result of these investigations placed stringent requirements on the companies at fault. They frequently require the company to submit to period audit and reporting to the federal or state agency on its privacy and security compliance for 20 years. As a result, companies have come to realize they must ensure that the representations made in a published privacy policy be truthful and accurate, and followed, internally, by the appropriate procedures. This can only be accomplished through the development and implementation of an appropriate Enterprise Privacy Program.

**WHAT KIND OF PRIVACY PROGRAM?**

An Enterprise Privacy Program would need to address the many different aspects of a company’s activities. For example, while website privacy policies are very popular, other policies are just as important.

Companies collect and process personal information of their personnel as part of their Human Resources functions. These may include salary, promotion, or healthcare data of each individual employee, and frequently similar information about the employee’s spouses and children. The company’s marketing, sales, and accounting department do collect personal information about clients, prospects, and subcontractors. For example, in addition to the name and professional address of a client, the marketing and sales group may also have collected names of client’s children and spouses invited to company function, or the personal taste (e.g. theater v. golf v. sailing) of clients for entertainment purposes.

For companies operating in certain markets, the Privacy Program must address the specific requirements of the laws governing that market. For example, financial institutions must develop Privacy Programs that comply with the Gramm Leach Bliley Act and related financial privacy laws. Companies with global operations would have to incorporate the requirements of the local foreign laws where their clients or employees operate, because these individuals are likely to be protected under these foreign laws.

In addition, most states have enacted numerous privacy laws that directly affect the content of privacy policies and privacy compliance programs. A company doing business in a specific state would have to develop a program that takes into account these recent laws.
DEFINING AN ENTERPRISE PRIVACY PROGRAM

An Enterprise Privacy Program should include policies and procedures, and be based on actual operations of the company. It first requires an assessment of the companies practices to ensure that the representations that will be made in the published policy will adequately reflect how the company handles personally identifiable information it collects, and the rights is provides to the data subjects.

To limit risks of exposure to legal action or litigation, the Enterprise Privacy Program should take into account the numerous legal requirements to which the company is subject. It should, as well incorporate standards, best practices that are in effect in comparable institutions.

Further, the Enterprise Privacy Program should include technology considerations, such that the information systems are programmed to respond to the privacy promises. The development plan for an Enterprise Privacy Program should also allocate time for relations with data subjects and the personnel, to explain the program and communicate it to the personnel. It should, as well, anticipate the need for communications with all data subject, those individuals whose data are collected or stored by the company.

As a result, the development of an enterprise involves multi-disciplinary approach, and top to bottom participation, as all divisions, departments of a company are concerned. In addition, subcontractors, outsourcers, and other third parties that may have access to the personal data collected by the company should as well be consulted, and participate in the program.

POLICIES AND PROCEDURES

An initial development plan should identify the activities required. It is an overall strategic document that serves as the company’s business plan for protecting personally identifiable information of customers, employees, and other individuals.

The privacy policy is a high-level statement of the company’s commitment to privacy. It provides a framework of expected activities, defines what information the company will collect, how it will use it, update it, destroy it, protect it.

Privacy procedures are a detailed statement of how the policy will be implemented: what is collected and how, access rights, uses, security measures used to protected the confidential data.

DEVELOPING A PLAN OF ACTION

The first step in the development of an Enterprise Privacy Program is to create a plan of action. The process will require the involvement of several layers of management.

It is essential that the decision makers, president, chief executive officers participate. They will set the tone, and establish the general direction to be taken. They will also approve the plan.
Providing for funding of the different activities will be crucial. Since the development of an Enterprise Privacy Program requires numerous activities and players, it will inevitably cost time and money. Before initiating the activities required for the establishment of an Enterprise Privacy Program, the company must ensure that sufficient funds are allocated to compensate for the time invested internally by company personnel, as well as to pay for the fees of the consultants and legal counsel involved, and, eventually, the cost of additional software licenses or equipment needed to implement the policies and procedures.

Once the general direction has been defined, and appropriate funds allocated, the definition of an Enterprise Privacy Program should start with the identification of the types of data that are collected, used, needed. This would involve the participation of all major departments and divisions of the company, such as Human Resources, Sales, and even the Research and Development group, which may have a stake in the data collection and processing. They may need the information, for example, to develop new products and offering for the company that would require a knowledge of needs or profile of the potential customers.

Legal considerations also need to be taken into account. The company may be subject to specific laws, such as the Gramm Leach Bliley Act, HIPAA, COPPA, or CAN SPAM. There may be additional restrictions in contracts, such as Confidentiality Agreements or Business Associates agreements, which may dictate how certain information is handled. The company’s document retention program may also need to be revised to be consistent with the information privacy and security program.

Finally, technical considerations are also very important. What kind of technology the company uses, what programs are available to filter data, or to implement opt-in or opt-out decisions by the data subjects. The company needs to have a clear understanding of its technical capabilities before it can attempt to make decisions on the way personally identifiable information will be handled, collected, or processed.

**ASSESSMENT AND ANALYSIS**

To be able to evaluate the current practices of the company, there should be first a thorough, honest assessment of the company’s current practices, and possibly, as well, those of its affiliates, subcontractors, or outsourcers. The investigation should determine what personally identifiable information is needed, by whom, for what purposes.

There may be different types of information needed, for different uses. For example, the Human Resources department may need detailed personal information about the personnel, to be able to provide healthcare insurance. However, the details should remain confidential to the Human Resource department, -- or rather, to specific individuals in the HR department.
On the other hand, some of the information collected by the Human Resources department would also be necessary to the accounting department, which will issue pay checks. The operations group, as well, may need contact information to establish a directory of personnel, so that employees may be contacted outside of business hours, in case of an emergency. Access would have to be limited to specific personal contact information, rather than to other personal information, such as name of spouse or domestic partner.

The assessment of the company’s operations should also include a determination of how the information is obtained or collected. For example, there may be information collected on a website, or information collected by the accounting department, to process invoices. Certain information may be obtained after patient consultation has been completed, and the physician’s notes are collected and input in the hospitals medical files. Does the company need all information that it collects, or are there questions that are not relevant to the primary purpose of the inquiry? For example, is a social security number needed when all the customer wants is to purchase equipment?

Of importance, as well would be how the data is stored. On the company computer systems? On laptops? On Blackberries and other portable PDAs? Is there a daily backup of all devices? Are some devices never backed up?

Knowledge and understanding of the company’s document management, retention and destruction practices are important to avoid discrepancies with legal requirements. For example, the HIPAA rules require companies to keep certain records for 6 years. There are other requirements in litigation for the use of documents as electronic evidence.

The use of the email systems and other company’s practices for marketing, email marketing, or telemarketing would also have to be examined. Compliance with the CAN SPAM act and other commercial marketing laws has become an essential component of an Enterprise Privacy Program.

Most companies outsource certain operations to affiliates or third party subcontractors. These outsourcers may be located within the company’s premises, or elsewhere, even in other countries. The company should understand who among its affiliates or third parties might have access to personally identifiable information. On websites, there might be framing, which may allow a third party to collect data unbeknownst to the users. Alternatively, there may be a link to a third party website, to which users are transferred. That other site may have different practices, of which the users should be made aware.

The assessment of the company’s practices should also provide a clear picture of the different uses of the information. Who has access to what? Who needs access to what? For which purposes is the information used? Are users requested to provide more data than actually needed for a specific activity, because the data collector hopes to be able to use it for other purposes? Is the information transferred to third parties, affiliates, or outsiders?
LEGAL CONSIDERATIONS

There is an increasing number of privacy and security laws in the United States. Some are federal laws, such as the Gramm Leach Bliley Act, the CAN SPAM Act, or the Children Online Privacy Protection Act. Others have been adopted by states, to complement the federal laws. These laws regulate companies’ activities in certain markets. For example, HIPAA Privacy and Security Rules limit how the covered entities can share personal health information with third parties. COPPA defines how companies may collect information from children under 13. Each of these laws also requires the implementation of security measures to protect the confidential data collected.

Most important, each of these laws also affects the myriad of companies that do business with these regulated entities. For example, HIPAA requires each covered entity to enter into specific contracts with each of its business associates. The Privacy Rule defines specific commitments required from the business associates. Each business associate must commit to protect the privacy of the protected health information to which it may have access. It must also agree to respect privacy rights of each individual patient, such as by responding, or assisting the covered entity in responding to, patients’ requests for accounting of data disclosures, or for amendment of erroneous data.

Any company that is a “business associates“ or a subcontractor of a regulated entity, and that has executed a contract that includes information privacy or security promises, would have, in turn, to implement an adequate Privacy Program. The Privacy Program would allow the company to put in place the necessary measure that ensure that the promises made in these contracts are fulfilled.

At the State level, numerous laws do supplement the existing federal laws. For example, in California, state laws place on pharmaceutical companies requirements similar to those placed on health plans and healthcare providers with respect to the handling of patients’ personal information. Other laws extend the restrictions on the use of patient information for marketing.

In addition, recently, many states have introduced bills that would restrict companies’ ability to use outsourcing services locate off shores, in an attempt to ensure the protection of the privacy and security of critical information. An Enterprise Privacy Program would have to take into account these bills if they become laws, to ensure that no restricted data is provided to third parties in a violation of the law.

In addition to laws, the company should also assess and understand the obligations that may stem from recent jurisprudence resulting from class action or government agency actions. For example, recent FTC or State Attorney General actions have focused on ensuring that companies have in place adequate security procedures that are consistent with the promises made on their website privacy policies. Other
legal actions have addressed companies’ ability to transfer databases to third parties as part of bankruptcy proceedings.

Beyond the legal requirements imposed by the legislature and the judiciary, the company should also understand the promises and commitments made in its contracts such as non-disclosure agreements, confidentiality agreements or services agreements. There may be other restrictions established through company’s employee manuals or other pre-existing company policy.

**TECHNICAL CONSIDERATIONS**

The third prong of the assessment of the company’s practices should include an evaluation of the networks, software, and equipment used by the company. These are the crucial components to the collection, processing and handling of the protected data. Some applications may not be totally integrated with the remainder of the operations. This may be a blessing, and may prevent sharing information outside a particular division. On the other hand, this may be a curse, because all requirements and constraints -- such as implementing opt-it or opt-out decisions -- might have to be duplicated, to operate as well on the non-integrated systems.

The company should also understand its use of third party subcontractors in connection with the entry and processing of data. Who else, outside of the company, may have access to the protected data? Data entry personnel located in India? Data processing services obtained through a service provider in another state? Data received from an affiliate located in the European Union? Hosting or communications services?

**ELEMENTS OF PRIVACY PROGRAM**

With all this information in hand, the company should have adequate knowledge of its operations to begin defining its Privacy Policy. Then, the remainder of the program would include, completing an acceptable compliance privacy policies, incorporating these concepts in the creation or updating of the companies procedures. Once these two documents are completed and approved, at the company level or division level, it will be necessary to ensure the implementation. This would include the creation of collateral materials, training, and rollout for communications with third parties, subcontractors, and clients.

Once the program is in place, there should be additional training, enforcement, and audit of the practices. In addition, there should be a periodic evaluation of the company’s evolving needs, as well as the additional restrictions created by new laws or contracts.

**MAIN COMPONENTS OF A PRIVACY POLICY**

Privacy policies generally address the same types of concepts. Numerous organizations have published sample privacy policies. However, this is not an excuse for plagiarizing another company’s privacy statement. Not only this is a
copyright violation, but it also foolish, because it assumes that both companies operate in the same market, with the same clients, are subject to the same laws, and have the same internal procedures. Of course, this seldom happens. There is no “one size fits all” model.

The company should define and draft its own policy. The policy should contain at least the following information:

- What is collected by the company, by third parties?
- How is the information used
- With whom the information is shared
- What choices data subjects have about limiting the collection, use, distribution of information (opt-in, opt-out, etc.)
- Whether data subjects may have access to the information collected about them
- How data subjects may correct any inaccuracy in the information
- What measures the company takes to protect the information under its control
- How the company will ensure compliance with the policy
- How data subjects can contact the company for complaints, questions, enforcement of the policy
- How changes to the policy will be announced and implemented

**ADDITIONAL PRECAUTIONS**

In addition, depending on specific situations, additional disclosure may be necessary, for example, when data subject may be outside the company’s jurisdiction, or when information may be shared with third parties with different privacy policies. Different procedures and policies may be needed for different uses or different parts of the company or the website. Specific disclosure may be required on website privacy policies if cookies linked to a name or other specific identifier.

Consider also addressing the marketing functions of the company, such as defining rules and procedures for email marketing or telemarketing, to provide directions on the implementation of the CAN SPAM Act, Do Not Call lists, and other recent legal requirements. There may also be aspects of the company’s document management and documents retention program that would need to be clarified, to address new legal requirements.

**SECURITY**

There is no privacy without adequate security measures. The company should take the necessary precautions to protect all personal information it collects, using industry-standard security protocols to secure sensitive data during transmission and while stored. In addition, a number of security laws or regulations have recently been enacted (e.g. under the Gramm Leach Bliley Act) or will shortly become effective (e.g. under HIPAA). These laws and regulations contain specific requirements for the security of personally identifiable information.
The company should use appropriate security procedures to avoid misuse of information, including for example, authentication protocols for user identification, passwords, and methods to challenge customers when passwords are forgotten.

In addition, a thorough Privacy Program should include appropriate measures to respond to breach of security, to comply with California’s SB 1386, when personal data pertaining to California residents might be lost through a breach of security.

While most website privacy policies include representations about the security measures taken to protect personal information collected, frequently, companies do not have adequate security measures that are consistent with the representations made. Companies have been prosecuted when their security measures were ineffective or contrary to the representations made. For example, the Federal Trade Commission has completed actions against Guess; Microsoft and Eli Lilly related to defects in these companies’ security measures. Similarly, State Attorney Generals have prosecuted companies, such as Ziff Davis, or the ACLU when holes in security measures were uncovered. In each case, the government determined that the company’s security measures were not consistent with the representations made on the website privacy policy.

**DISPUTES AND PROBLEMS**

A complete privacy protection programs should also include procedures and recourse when problems arise. Several laws already require that the company identify in its privacy policy a contact for customers or employee complaints and requests. When such situations arise, the company should take immediate action. The privacy policy and procedures should anticipate these events, and define as necessary the nature of the response to breach of security and loss of data. Further, companies doing business with California residents should incorporate in their procedures the methods and actions necessary to ensure compliance with California’s SB 1386.

**WEBSITE ISSUES**

Since most companies have a web presence, their privacy policies and procedures should also take into account problems and issues specific to Internet business, such as the data collected and processed through shopping carts and payment systems. The policies should as well clearly disclose the uses of “snooping” technologies such as cookies, web bugs, and web beacons, or software feedback loops, which may result in the collection of information about users.

Websites present additional issues in connection with privacy when they include links to other sites, such as in co branded sites or when framing is used. Further, special precautions and attention will be needed when chat rooms or list serv are used.
PROCEDURES

Once the privacy policy has been approved by the company’s management, it is necessary to establish the detail procedures that will be used to implement the policy. There should be detailed day-to-day operational procedures, specifying each stage of the data collection, use, transfer, storage, and security.

What data can be collected? By HR? By Accounting? By R&D? By the division that is located in Oklahoma.

Who has access to what? What can be disclosed, to whom? What may be transferred outside the company?

What precautions are needed before transferring data to third parties? How to respond to a request or a complaint from a data subject?

What security measures will be taken? How to handle a breach of security?

What contract, releases, non-disclosure agreement, or other agreement should be used with different types of subcontractors?

What language should be used when spending emails that may be restricted under the CAN SPAM Act?

And so on.

The procedures must be sufficiently detailed to address the multiple facets of the company’s business. It must answer most questions that the staff may have on a daily basis, or occasionally, on what to do with specific data under specific circumstances.

The company privacy policy cannot become effective and cannot be published before there are in place adequate procedures to support the representations made in the policy.

IMPLEMENTATION & MAINTENANCE

Once the policies and procedures completed, the company must then implement these procedures so that the policy can be published and launched. This will require that the privacy practices, policy band procedures be communicated to the entire company. Crucial to the process will be the training of the personnel, both before roll out, and again, later, periodically.

For clients, users outside the company, notices and other communications should be distributed to the individuals, to inform them of the new policy. In addition, as may be required by laws, there should be a system in place to ensure that updates and annual reminder notices are distributed.
A crucial component of the policy is its enforcement. The enterprise needs to have in place the necessary mechanisms and checks to monitor compliance by the personnel. In addition, periodic audits and reviews at the global level should be made to ensure that every piece of the puzzle is operating as expected.

Of course, do not forget the policy on a shelf. It is a living document that needs to be updated. Only twenty percent of the job is done after the initial policy and procedures are drafted. The day-to-day application, the continued relevancy of the Privacy Program is essential to its success. Further, practices change, laws change. The documents and related procedures must be modified frequently to adapt to changes.

**BEYOND CURRENT PRACTICES**

If the company determines that its current practices need improvement, it should be careful not to “put the cart before the horses.” Do not write in the policy activities or promises that are beyond the current company’s practices and capabilities. To improve on current practices, make sure first that this is feasible, and that all relevant divisions of the company agree to the change, such as human resources and marketing/sales department. In addition, as for the initial steps, there should be adequate financial resources and funding for the new project, assurance that the company has the adequate technical capabilities to implement the “better” policy, and that these additional features and commitments are in compliance with laws and contracts. Additional training before rollout would, of course, also be required.

**GOLDEN RULES**

The development of an Enterprise Privacy Program is a complex endeavor that requires time, money, resources, and attention. At the conclusion of the effort, there will be published one or several policies that represent the company’s commitment to privacy protection. This is a flagship project. It engages the reputation of the entire company. Therefore, it should be handled carefully.

There are a few Golden Rules:

- Say what you do. Be honest and accurate
- Say it clearly
- Make it easy to find
- Do what you say. Practice what you represent in the policy
- Ensure consistency among company policies
- Think globally
- Revise your policy and procedures periodically
- Train, train, train
- Audit your personnel’s compliance

Failure to observe these rules could cause great harm to the company. While a company’s products or services may be the most inventive, creative, or useful, a
“little glitch” could cause public relations disaster. If there is a privacy or security breach, and personal data is disclosed or lost, or if the company is accused by a disgruntled employee to have violated privacy laws, the information will make the first page of the local newspaper, and from there the news will spread to cause great harm to the company’s reputation, or possibly class action suits or government agency investigations.

CONCLUSION

The creation and development of a company wide Privacy Program is a complex endeavor that requires a great financial and time investment. The collaboration of the entire enterprise is necessary to achieve the development of a privacy policy that makes sense, and is consistent with the company’s practices, expectations, and goals. To achieve such a complex goal, patience and honesty are required. There must be a complete and thorough investigation of the company’s practices and actual needs. Complex legal issues are involved. They cannot be resolved by the mere use of a form. Each company has its own culture and needs.

A company’s most important assets are its personnel and its customers. To survive and be competitive, an enterprise needs to invest the resources necessary to indicate its respect for the privacy of personal information pertaining to them. This can only be achieved through a well thought out, comprehensive, Enterprise Privacy Program.
NEW REQUIREMENTS FOR THE
DISPOSAL OF CONSUMER INFORMATION AND RECORDS

Francoise Gilbert – IT Law Group
Palo Alto, CA

Copyright © 2005 – IT Law Group – All Rights Reserved

As of June 1, 2005, companies will be required to properly dispose of consumer information derived from consumer reports to comply with new obligations under the regulations that implements the Fair and Accurate Credit Transaction Act of 2003 (the "FACT Act"). The purpose of the Rule is to reduce the risk of identity theft and other harm from improper disposal of a consumer report, or records derived from a consumer report. The Rule applies to any entity over which the FTC has jurisdiction that, for a business purpose, maintains or possesses such consumer report information.

Executive summary
Section 216 of FACTA requires that any entity that possesses or maintains "consumer information" or any compilation of information derived from consumer reports to properly dispose of any such information or compilation. The new rule, published as 16 CFR Part 682, defines the requirements for the proper disposal of these records.

The Rule requires the covered entities to take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. The standard for disposal is flexible to allow companies to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and relevant changes in technology over time. The Rule includes specific examples of appropriate measures that would satisfy its disposal standard.

What is protected?
The rule protects "consumer information": any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report or is a compilation of such records.

A “consumer report” is any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, which is used as a factor in establishing the consumer's eligibility for credit or insurance, employment, or any other permissible purposes authorized under the Fair Credit Reporting Act, for example, in connection with an investment or a business transaction.

Information that does not identify an individuals, such as aggregate data or blind data, is not covered by the new disposal rule.
Who is affected?
The Rule applies to any entity that maintains or possesses consumer information derived from consumer reports for a business purpose. In addition to consumer reporting agencies, these would include, for example, lenders or investors, insurers, employers, landlords, government agencies, mortgage brokers, automobile dealers, and other businesses that use consumer reports.

When does the Rule apply?
The new rule requires companies to take reasonable measures to protect consumer information in connection with the disposal of records.

"Disposal" includes:
- Discarding or abandonment of consumer information
- Sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored

Reasonable disposal measures are required
The Rule requires entities that possess or maintain consumer information to take "reasonable measures" to properly dispose of such information, in order to protect the information from unauthorized access or use after its disposal.

The Rule does not define “reasonable”, but allows entities to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and relevant changes in technology over time. The Rule provides several examples of what would constitute "reasonable measures.” These examples are illustrative and intended as guidance only.

1. Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers so that the information cannot practicably be read or reconstructed;

2. Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media so that the information cannot practicably be read or reconstructed;

3. Using the services of a third party who is engaged in the business of record destruction, in order to dispose of the material, provided that the company:
   a. Conducts due diligence, which would include:
      o Reviewing an independent audit of the disposal company's operations or its compliance with the Rule;
      o Obtaining information about the disposal company from several reference or reliable sources;
      o Requiring that the disposal company be certified by a recognized trade association or similar third party;
      o Reviewing and evaluating the disposal company's information security policies or procedures;
Taking other appropriate measures to determine the competency and integrity of the potential disposal company

b. *Notifies the service provider that the information is “consumer information” protected under this Rule*

c. *Enters into a contract that requires the service provider to dispose of the information in accordance with the Rule*

d. *Monitors compliance with the contract*

Service providers are covered as well. Along with the record holder, they bear responsibility for proper disposal of the protected information that they maintain or possess. They must implement and monitor compliance with policies and procedures that protected against unauthorized or unintentional disposal of consumer information. The Rule suggests that these entities should use, for example, the measures listed in #1 and #2 above.

Entities subject to the Gramm Leach Bliley Act are exempt from this Rule, and must, instead comply with the Security Safeguards that were enacted under the GLBA.
In the wake of recent headlines about the inappropriate destruction of business records, there has been much debate about whether records can be legally destroyed without the threat of government sanctions or criminal or civil actions. There are similar concerns about the retention of corporate records. What should be kept? For how long should different records be kept? What are the adequate policies and procedures for organizing a record retention program that complies with applicable laws, regulation, and jurisprudence?

**RECORD RETENTION**

A myriad of laws, federal or state affect record management, and/or specify which records a company must maintain or how long companies must retain records. Retention periods stated for any regulatory or statutory purpose are considered minimum retention periods - the shortest period of time a record must be held. Decisions are frequently made to retain records longer than their prescribed minimum due to other factors, such as an on-going business use, internal audit requirements, or historical value. Whenever retention periods are lengthened, a determination must be made identifying the potential risks and costs to the company.

**Federal Laws**

The following is only a selection of federal laws that affect the retention of corporate documents.

The **Sarbanes Oxley Act** and related regulations contain requirements and restrictions concerning the retention corporate records and other corporate contracts. For example, the mandatory document retention provisions in Section 802 of the Sarbanes Oxley Act direct the Securities and Exchange Commission (SEC) to promulgate regulations relating to the retention of relevant records from an audit or review. It also directs accountants to maintain certain corporate audit records or to review work papers for five years from the end of the fiscal period during which the audit or review was concluded.

While **Title VII of the Civil Rights Act of 1964** does not specify the precise records a company must maintain, it requires that any personnel or employment record made or kept, including records having to do with hiring, must be preserved for six months from the date of making the record or from the personnel action involved. 42 U.S.C. §§ 2000e-8, 2000e-12, 29 I.E. §§ 1602.12; 1602.14.
Moreover, if a charge or discrimination is filed, all records relevant to the charge must be retained until final disposition of the case. 29 C.F.R. § 1602.21(b).

Under the federal **Age Discrimination in Employment Act**, all payroll records must be maintained for three years from the date of last entry. 29 C.F.R. § 1627.3(b). In addition, personnel and employment records relating to hiring, promoting or discharging employees, and job applications and other matters pertinent to a determination whether an action, limitation or classification is based on a factor other than age, must be retained for at least one year from the date of any personnel action to which the records relate. 29 C.F.R. § 1627.3(b).

The regulations implementing **Executive Order 11246** require contractors with 150 or more employees and a contract of $150,000 or more to preserve any personnel or employment record made by the contractor for a least two years from the later of the date of making the record or the personnel action involved. Such records include job advertisements, postings, applications, resumes, and records pertaining to hiring, assignment, promotion, demotion, and termination. If a contractor has less than 150 employees or does not have a government contract of at least $150,000, the minimum record retention period is one year. All contractors, regardless of size, must maintain a current affirmative action plan and documentation of good faith efforts to retain the previous year's affirmative action plan and documentation of good faith efforts for the previous year. 41 C.F.R. § 60-1.12.

Under the **Fair Employment and Housing Act**, unsolicited resumes or job inquiries (i.e., resumes not sent in response to a job posting or advertisement) must be retained for two years from the date a resume was received, if the resume was reviewed in the process of making particular hiring decision. However, if the company did not review or retain the resume for later review (e.g., the company sends a postcard to the individual stating the company does not consider unsolicited resumes), there is no retention requirement.

Under the **Federal Equal Pay Act**, employee wage records (including time cards, wage rate tables used in computing straight-time and overtime, shift schedules, hours and days of individual employees, records explaining wage differentials between sexes) must be retained for three years.

**State Laws**

In addition to federal laws, numerous subject matter specific state laws contain provisions that set specific retention requirements, such as for the retention of employment records or medical records.

For example, the **California Fair Employment and Housing Act**, requires that all personnel records be retained for two (2) years after the records and files are initially created or received or after an employment action (e.g., hiring) is taken regarding the employee. Cal.Govt.Code § 12946; 2 Cal.Admin.Code § 7287.0(c).
Even if there is no specific retention or similar requirement for a particular type of records, other statutes may affect a company's decision to retain or preserve certain records, such as statutes of limitations. These statutes, sometimes called limitations of actions, define the time an organization can sue or be sued on a matter, or the time in which a government agency can conduct an investigation or audit, are critical. While in themselves they do not set required retention periods, they should be a factor in deciding how long to retain records. For example, California has a four-year Statute of Limitations for actions on written contracts. Therefore, consider retaining contracts - and other documentation pertaining to the performance of each contract - for at least for four years after the last event in the contract has been performed. Having appropriate records will allow the company to properly respond to a complaint or other action.

**When there is no specific statute**

When there are no specific statutory or regulatory retention requirements, the courts have generally set a standard for determining appropriate retention periods for all other records, which is based on reasonableness.

**RECORD DESTRUCTION AND TAMPERING**

Records are legally discoverable as long as they are retained, regardless if their retention period has expired. If records are no longer of use in the business context and there are no statutory, regulatory, or investigative reasons to retain the records, then it is in the company's best interest to dispose of them. Caution is necessary when destroying records, as the destruction of materials that constitute evidence is subject to numerous laws and regulations.

For example, Section 802 of the Sarbanes Oxley Act contains restrictions with respect to the destruction or alteration of corporate records and other corporate contracts. Section 802 of the Sarbanes Oxley Act punishes with fines and/or prison the alteration, destruction, mutilation, concealment or falsification of any document or tangible object with the intent to impede, obstruct or influence proceedings involving federal agencies or bankruptcy. Section 1102 prohibits alteration or destruction of a record or other object with the intent to impair the integrity or availability for use of the record or object in an official proceeding.

Several other statutes potentially may apply to the destruction of evidence, such as 18 U.S.C. §§ 1503, 1505, and 1512.

18 U.S.C. §§ 1503 applies to pending judicial and grand jury proceedings, whereas Section 1505 applies to pending federal agency, department, or congressional proceedings, as well as to proceedings in federal court where the agency is a party. Both statutes provide that whoever corruptly influences, obstructs, or impedes, or endeavors to influence, obstruct, or impede, the due administration of justice, due and proper administration of the law, or due and proper exercise of the power of inquiry shall be guilty of a crime.
18 U.S.C. § 1512, commonly known as the "witness tampering" statute, prohibits attempts to have third parties destroy documents that may be relevant to an official government proceeding. Section 1512 provides for criminal liability for causing or inducing a third party to withhold a record, document, or other object, from an official proceeding; or to alter, destroy, mutilate, or conceal an object with intent to impair the object's integrity or availability for use in an official proceeding.

**NONCOMPLIANCE RISKS**

**When there is legislation**

Federal and states laws and regulation that affect the retention or destruction of records may provide for serious fines or imprisonment for these violations.

For example, the Sarbanes Oxley Act contains several provisions for fines or prison. Under Section 802 of the Act, document alteration or destruction may result in fines and/or up to 20 years imprisonment. Section 802 also imposes fines, a maximum term of 10 years' imprisonment or both for violation of the mandatory document retention requirements. The provisions addressing obstruction of justice by tampering with records in Section 1102 of the Sarbanes Oxley Act provide for fines and/or up to 20 years imprisonment for certain instances of document tampering.

**In the absence of legislation**

Courts have severely punished companies who fail to produce evidence. For example, a company was fined One Million Dollars ($1,000,000.00), and was required to take other constructive actions to preserve evidence in a class action alleging deceptive sales practices in the sale of life insurance. During the discovery process in this case, the defendant was ordered to preserve all documents and other records containing information potentially relevant to the subject matter of this litigation. The court issued sanctions based in part on the senior management failure to manage the discovery process and prevent document destruction. The court found that the defendant had no comprehensive document retention policy with informative guidelines and lacked a protocol that promptly notifies senior management of document destruction. In addition to the one million dollar fine, the defendant was required to notify all employees of the action, and to preserve all documents and other records containing information potentially relevant to the subject matter of this litigation.

Similarly, a defendant was sanctioned for its "obstructionist attitude toward production of the materials." The court found that the defendant's document retention policy was, in fact, only a policy for the destruction of detrimental documents, not a policy that covered all records of the company. During litigation, the defendant consistently ignored the requests for production of documents, requested numerous extensions to produce the documents. The defendant's employees testified that the stated purpose of the destruction of records was the elimination of documents that might be detrimental to the defense of a lawsuit, and that the destruction of all potentially harmful documents was an ongoing process.
Ultimately, the defendant admitted that it had destroyed documents despite a court order requiring their protection. The court found that the defendant had "utterly failed to demonstrate that its document retention policy is actually implemented in any consistent manner" and that its "failure to provide any evidence on this issue must be construed as a tacit admission that the policy is a sham." The court ruled that "the good faith disposal of documents pursuant to a bona fide, consistent and reasonable document retention policy cannot be a valid justification for a failure to produce documents in discovery."

**BEST MANAGEMENT PRACTICES: ORGANIZATIONAL STRUCTURES, PROCESSES, AND TOOLS FOR COMPLIANCE**

While a standardized methodology has been developed for creating records retention programs, there is no off-the-shelf program that can be installed one day and in use the next. Successfully addressing these questions requires the development and application of a quality records retention program, which includes:

**Understand the legal requirements**

- Conduct a survey of the laws, regulations and jurisprudence applicable to your company's specific needs, operations, business so that you can create a record retention and destruction policy that takes into account this legal framework.

**Adopt a record retention program**

- Make an inventory of the company's documents, all places where paper and electronic records are kept, all methods in which data can be transferred to/from the company. The inventory includes records created by all departments and users, in all media formats, and found in all locations.

- Determine how long each record is to be retained must be determined. Typically, specific legal requirements apply to less than 25% of a company's business records. For the remainder, an analysis must be done to determine the purpose of the records within the business organization. Why are they created? How are they used in the organization and who uses them? How long are they actively used or referenced?

- For each record, determine where it is located and how many copies are created; and assess the different uses of such record. For example, a record may be created by one department but used for other purposes by another department. Determine whether there are other unique concerns attached to a record, such as privacy.

- Create policies with respect to classifying documents or materials class, determining duration of retention periods, how records are organized, where they are kept.
• Determine to whom each category of document are accessible. Create policies for document access and handling, written communication protocols, data security, data storage, and employee termination/transfer.

**Adopt a record destruction program**

• Create a document destruction policy that includes consideration of backup and archival procedures, online storage repositories.

• Create an index of active and inactive records; and a log of record destruction.

**Empower personnel**

• Assign the responsibility for retaining documents and related materials on specific individuals.

• Train personnel on documents handling, retention and destruction requirements.

**Audit, audit, audit**

• Conduct periodic audits, reviews, and updates of the record retention and destruction program. A records management program is dynamic.

---

\(^1\) This article was first published by OCEG in 2003.

\(^\text{i}\) In re Prudential Inc. Co. of America Sales Litig., 169 F.R.D. 598 (D.N.J. 1997).