



Tuesday, October 21
4:30 pm-6:00 pm

706 Data and Information Security: What are the Rules and Can Technology Help With Compliance?

Karen Litsinger
General Counsel
Mirixa Corporation

Mike Newman
Senior Vice President and General Counsel
Websense, Inc.

Keith Omsberg
Vice President, General Counsel
Tier Technologies, Inc.

Faculty Biographies

Karen Litsinger

Karen Litsinger joined Mirixa Corporation as general counsel. Ms. Litsinger brings to the Mirixa management team years of experience assisting companies in the technology arena.

Immediately prior to joining Mirixa, she served as a partner in the corporate and Internet, communications and data protection (ICDP) practice groups at Sonnenschein, Nath & Rosenthal LLP. Before joining Sonnenschein, Ms. Litsinger participated in the tremendous growth of America Online, Inc., where she served as vice president and associate general counsel. Ms. Litsinger began her career as an associate at Arent Fox handling real estate and corporate matters.

Ms. Litsinger serves on the board of directors of Ayuda, Inc., a nonprofit legal services organization, and on the board of directors of the Holton-Arms Alumnae Association.

She earned her bachelor's, cum laude, from Duke University and her JD, cum laude, from Georgetown University Law Center.

Mike Newman

Michael Newman is senior vice president and general counsel for Websense, Inc. An experienced attorney in the technology sector, he is responsible for all areas of legal guidance, including contracts, intellectual property, strategic partnerships, securities and finance, employment and benefits, and litigation.

Prior to joining Websense, Mr. Newman served as senior staff counsel for securities, finance and corporate development at Gateway Inc., a leading PC manufacturer. In this role, he negotiated and closed numerous equity investment, merger and acquisition, stock sale and asset divestiture transactions, in addition to forming strategic alliances with companies such as America Online and OfficeMax. He also maintained Gateway's SEC and international corporate compliance. Before Gateway, Mr. Newman was an attorney with the law firm of Cooley Godward LLP, a leader in the representation of high-growth information technology and life sciences companies. Prior to Cooley Godward, he was an attorney with Latham & Watkins, one of the world's largest law firms.

Mr. Newman graduated magna cum laude from Georgetown University with a BS and received his JD, cum laude, from Harvard Law School.

Keith Omsberg

Keith Omsberg is the vice president, general counsel, and secretary of Tier Technologies, Inc., a provider of financial transaction processing, payment solutions, and software

systems based in Reston, Virginia. He is responsible for company legal functions including general corporate law, governance, compliance, mergers and acquisitions, technology licensing, intellectual property, litigation, and employment law.

Prior to joining Tier, Mr. Omsberg served as senior counsel at Peoplesoft, Inc., in Pleasanton, California where he was responsible for corporate law matters, commercial transactions, intellectual property, and technology licensing.

Mr. Omsberg is a member of the California bar.

Mr. Omsberg received his BA from University of Southern California, and is a graduate of Golden Gate University School of Law.

ACC Association of Corporate Counsel

Data and Information Security: Laws and Regulations

Keith Omsberg
General Counsel
Tier Technologies, Inc.

By in-house counsel, for in-house counsel.SM

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

The Role of In-House Counsel

- Privacy – data/information security - confidentiality
- Loss prevention and risk management
- IT, HR and inter-department relationships
- Investigation of data loss incident
- Compliance

By in-house counsel, for in-house counsel.SM

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Why is data and information security so important?

- The value of data, identity, and privacy
- Loss and theft of sensitive data is high profile
- Significant exposure
 - Costs (fines, notifications, remedial measures)
 - Loss of reputation and business

By in-house counsel, for in-house counsel.SM

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Applicable Laws and Regulations

- A “patchwork” of federal and state laws (FTC, FCRA, FACTA, HIPAA, GLB, state laws, industry regulations, and more....)
- Federal Trade Commission (FTC) enforcement
 - Unfair trade practices
 - ChoicePoint and the Fair Credit Reporting Act (FCRA)

By in-house counsel, for in-house counsel.SM

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Applicable Laws and Regulations

- **State Notification Laws** - most states now have laws requiring notification to consumers where personal information may have been misappropriated.
 - Several states follow notification rules similar to CA SB 1386 (California Security Breach Notification Act) providing for notification where "reasonable belief" that personal information was acquired by an unauthorized person.
 - Some states have detailed requirements for destruction, encryption, written policies, and other specifics which can create significant exposure. For instance, new Connecticut Public Act No. 8-167 (effective October 1, 2008) presumes causation and harm, and requires a published privacy protection policy with significant fines for failure to comply.

By in-house counsel, for in-house counsel.SM

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Applicable Laws and Regulations

- **Gramm-Leach-Bliley Act** - requires financial institutions to establish safeguards to protect the security, confidentiality and integrity of consumer information
- **Industry Standards:** Coso; CoBIT; ISO; PCI DSS

By in-house counsel, for in-house counsel.SM

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Applicable Laws and Regulations

- **Sarbanes Oxley Act** - Although information security is not explicitly mentioned, SOX mandates that organizations ensure the accuracy of financial information and the reliability of systems that generate it.
 - Section 404 requires an assessment of internal controls over financial reporting. Information security is essential in ensuring the reliability of these systems.
 - Section 302 requires certification of effectiveness of controls and attaches personal liability.
- **Health Insurance Portability and Accountability Act (HIPAA)** - provides mandatory standards for protecting the privacy of patients including physical safeguards, data integrity, confidentiality, unauthorized access and digital signatures.

By in-house counsel, for in-house counsel.SM

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Industry Example: Payment Card Industry Data Security Standards (PCI DSS)

- Mandated by major credit card companies
- Applies to financial institutions, merchants, payment processors, point of sale (POS) vendors, payment networks and card holders
- 12 primary security controls for protecting cardholder data
 - Access
 - Authentication
 - Encryption
 - Transaction logging

By in-house counsel, for in-house counsel.SM

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org




Compliance and Best Practices

- Board level compliance
 - Audit and Special Technology Committees
 - Reporting and documentation
 - Officer Position
- Policies and procedures
 - Document Management Policy
 - Privacy Policy
 - IT Security Policy
 - SEC reporting

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.com




What do I do next?

- Educate to get “buy in” from the top
- Form a committee to evaluate the risk
- Audit systems and controls
- Develop and implement an action plan

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.com



Additional Protections and Risk Prevention Considerations

- Data Security and Privacy Breach Insurance
 - Coverage under existing traditional policies?
 - Network Risk Insurance (Cyber Liability)
 - First Party/Third Party and exclusions
 - Underwriting requirements
- Contractual Allocation of Risk
 - Indemnification for information security and identity theft
 - Pass through of rules and regulations
 - Mandatory notification requirements
 - Cooperation and rights to investigate

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.com



Implementing Security Controls

Karen Litsinger, Esq.
General Counsel
Mirixa Corporation

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.com

ACC Association of Corporate Counsel

What all laws have in common:

- Authority
- Responsibility
- Guiding Principles
- Internal Controls
- Information Management and Security Policies

- Relevance
- Cost Benefit
- Threat/Vulnerability = Risk "Acceptable Risks"

- HIPAA
- GLBA
- FISMA
- FTCA
- SOX
- EU Directives
- APEC Directives
- Other Federal & State Laws & Regs

The common subject areas are Administrative, Technical, and Physical Safeguards.

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

By in-house counsel, for in-house counsel.™

ACC Association of Corporate Counsel

Administrative Safeguards contd.

- ✓ Authorized Access
 - Limit access to those with a legitimate business need
 - Outline rules in advance so decisions are not personal or political
 - Consider background checks (sometimes required)
 - Terminate access immediately upon termination of employment or specific duties which required access
- ✓ Responsible Officer

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

By in-house counsel, for in-house counsel.™

ACC Association of Corporate Counsel

Administrative Safeguards

- ✓ Policies and Procedures
 - Guidelines that establish the security framework for your organization
 - Developed based upon risk analysis of your organization and steps required to mitigate the identified risks
 - Policies are not effective alone; must have appropriate implementation, consistent enforcement, and security-conscious company culture
- ✓ Training
 - One of the best weapons you have in preventing security incidents is an educated and vigilant workforce
 - Regular reminders, not just one-time training
 - Encourage employees to report anything "odd"

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

By in-house counsel, for in-house counsel.™

ACC Association of Corporate Counsel

Administrative Safeguards contd.

- ✓ Regular Review and Enforcement
 - Responsible Officer and others should constantly monitor activity and identify suspicious behavior
 - Develop and document investigation procedures
 - Must remediate any inappropriate behavior; don't let personal or political factors interfere with consistency
- ✓ Disaster Planning
- ✓ Breach Response Plan

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

By in-house counsel, for in-house counsel.™

ACC Association of Corporate Counsel

Physical Safeguards

- ✓ Facility Access
 - Secure perimeter, limit access to those with legitimate need, escort visitors, revoke access when no longer needed
- ✓ Workstation Access
- ✓ Device and Media Controls
 - Consider limitations on movement of devices containing sensitive media
 - Remove all sensitive data before re-use or disposal

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Technical Safeguards contd.

- ✓ Audit Controls
 - Ability to track and examine access to and uses of sensitive information
- ✓ Integrity
 - Prevent unauthorized modification or destruction of sensitive information
 - Detect changes or attempts to change

Much more on technical safeguards is coming up . . .

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Technical Safeguards

- ✓ Access Controls
 - Unique user names and passwords, forced change of passwords regularly, automatic logoff
 - Encryption of hard drives
- ✓ Authentication
 - Ensure identity of individual before allowing access (incl. before issuing user name or password)
- ✓ Transmission Security

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Resources:

- “Protecting Personal Information: A Guide for Business,” from the Federal Trade Commission
www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf
- California Office of Information Security and Privacy Protection, Guidance for Businesses

http://www.oispp.ca.gov/consumer_privacy/business/default.asp
- “Prevent Identity Theft with Responsible Information - Handling Practices in the Workplace,” from the Privacy Rights Clearinghouse
www.privacyrights.org/ar/PreventITWorkplace.htm

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

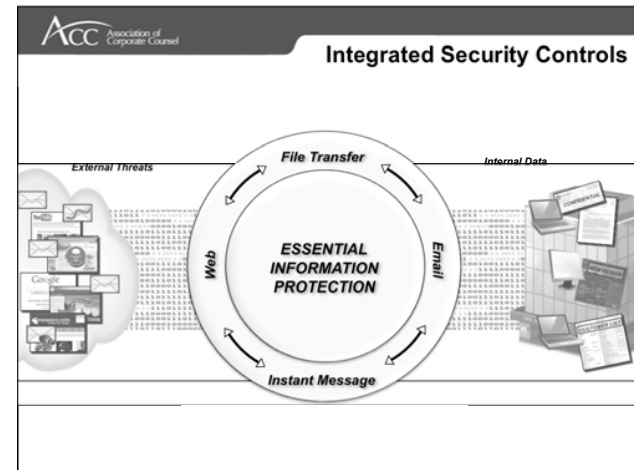
ACC Association of Corporate Counsel

Summary

- Security controls have to be interwoven as part of the business process and procedure tapestry not bolted on after the fact
- It takes administrative AND technical AND physical safeguards (as well as organizational, personnel, process controls) to adequately protect assets
- Controls should always be commensurate with the level of **RISK**

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org



ACC Association of Corporate Counsel

How Data Loss Prevention Technology Can Help

Michael Newman
Sr. VP and General Counsel
Websense, Inc.

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 19-23 | Seattle, WA | acc.org

ACC Association of Corporate Counsel

Traditional Technologies

- Antivirus – Known malware
- Firewalls – Great walls
- IDS/IPS – Anomaly detection
- Email Filtering – Malware & simple filters for Email
- Web Filtering – Employee productivity
- Web Security – Web-based malware

ACC Association of Corporate Counsel

CXO Concerns Around DLP

Can sensitive and regulated data be identified and loss prevented?

The situation: Data is exchanged inside and outside the organization with vendors, partners, end-users, consumers, etc.

The problem: Data is often stored, used, and exchanged inappropriately.

ACC Association of Corporate Counsel

Data Loss Prevention

Solution Benefits

- Prevent Data Loss
- Manage Compliance and Risk
- Secure Business Processes

ACC Association of Corporate Counsel

Technology Landscape

Enterprise Rights Management (ERM/DRM)

Can a specific user access this data?

Device Control

Can my data be copied to this device?

Encryption

Is my data secured in the event it is lost?

Data Loss Prevention

- What is my confidential data?
- Where is it stored?
- Who is using it and how?
- Is it secure?

ACC Association of Corporate Counsel

Business Intelligent Controls

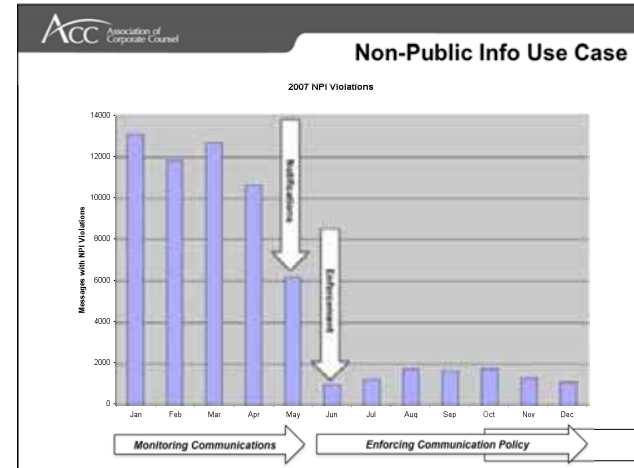
Who	What	Where	How
Human Resources	Source Code	Benefits Provider	File Transfer
Customer Service	Business Plans	Internet Auction	Web
Marketing	Customer Information	Business Partner	Instant Messaging
Finance	M&A Plans	Blog	Peer-to-Peer
Accounting	Patient Information	Customer	Email
Sales	Financial Statements	Spyware Site	Network Printing
Legal	Customer Records	North Korea	
Technical Support	Technical Documentation	Competitor	
Engineering	Competitive Information	Analyst	

ACC Association of Corporate Counsel

HIPAA Use Case

The situation: Nurses visited patients throughout the day and regularly updated patient records.

The problem: They would store the records on GoogleDocs so they could update them from any computer.



ACC Association of Corporate Counsel

Intellectual Property Use Case

The situation: Firm hired contractors to develop custom, back-end applications for payment processing.

The problem: Contractors wanted to keep copies of the code they developed for use on future projects.

