



Building an Effective Information Security Program: Segment 2 – The Risk Assessment

Joseph J. Lazzarotti, Esq.
Jackson Lewis LLP

© 2010 Jackson Lewis LLP

This presentation provides general information regarding its subject and explicitly may not be construed as providing any individualized advice concerning particular circumstances. Persons needing advice concerning Particular circumstances must consult counsel concerning those circumstances.



An Overview of Our Firm

- Jackson Lewis is one of the largest law firms in the country dedicated exclusively to representing management on workplace issues. The firm has successfully handled cases in every state and is admitted to practice in all Circuit Courts of Appeal and in the United States Supreme Court. With 46 offices and over 600 attorneys, the firm has a national perspective and sensitivity to the nuances of regional business environments.
- For over 50 years we have represented a wide range of public and private businesses and non-profit institutions in a vast array of industries. When issues arise, we devise optimal solutions that minimize costs and maximize results. Whether we are counseling on legal compliance or litigating a complex case, we assist our clients in achieving their business goals.
- In addition, we help employers create policies and procedures promoting positive employee relations. We have built our practice and earned our national reputation over the years by helping companies reduce workplace-related litigation by educating management on legal trends, judicial developments, and statutory and regulatory compliance in the rapidly evolving area of workplace law. Our state-of-the-art preventive law programs utilize the firm's expertise and unmatched experience to evaluate employment trends and related litigation, minimizing the risk of exposure in future lawsuits.

What is a Risk Assessment?

- **Critical to development of WISP**
- **Identify and assess**
 - *information possessed* – clients, patients, customers, employees
 - *applicable laws* – federal, state, local and international
 - *current safeguards* – administrative, physical, technical, organizational
 - *gaps/vulnerabilities*
 - *vendors, subcontractors, agents*



What is a Risk Assessment?

- Team approach – divide and conquer
- Project leader
- Team members
 - *By department* – legal, human resources, IT/IS, government relations, sales, public relations/marketing communications
 - *By location* – facility, state, region, country
 - *By information classification* – consumer, employee, patient



Identify Applicable Law

- Federal, state, local, and international
- Type of information
 - E.g., medical, SSN, credit card, photograph, biometric, genetic
- Use of information
 - E.g., employment, health plan, retail sale, treatment
- Who “owns” the information
 - E.g., company, health care provider, retailer, benefit plan



Identify Applicable Law

- Does the company sponsor a group health plan?
- Does the company maintain Social Security, DL#, or financial account numbers?
- Does the company process credit/debit card transactions?
- Does the company maintain medical, genetic, biometric information?
- Has the company entered into an agreement with data privacy and/or security obligations



Identify Applicable Law

- Is the company a “financial institution,” insurance company, or a “creditor”?
- Does the company belong to trade or other associations?
- What ethical obligations/privileges apply?
- Does the company transmit information internationally?
- Does the company maintain information on behalf of others?



Personal Information

- Take into account applicable laws
- Cast a wide net in terms of substance and form
- Eliminate categories later, if possible



Tracking Information Flows

- **Identify information systems**
 - Networks, hardware, software, devices
 - Contractors, vendors, service providers
 - Alternative work arrangements
- **Categorize information**
 - E.g., employee, consumer, trade secret, SSNs, medical, genetic . . .



Tracking Information Flows

- **Map data flows**
 - **Intra-departmentally or intra-personally**
 - **To and from third parties, and between third parties**
 - **Received/maintained on your behalf by third parties**
 - **Across state/national boundaries**



Vulnerabilities and Safeguards

- Compare current policies against legal and other requirements to safeguard personal information
- Examine data flows
- Eliminate unnecessary information
- Address remaining gaps



Vulnerabilities and Safeguards

- **Take into account:**
 - **The Company's size, complexity, and capabilities.**
 - **The Company's administrative, physical and technical infrastructure, including its hardware, and software security capabilities.**
 - **The costs of data privacy and security measures.**
 - **Reasonableness standard.**



Take Aways

- **Have a sense of your organization, its needs and related risks.**
- **Know the law.**
- **Be thorough.**
- **Build a team!**



**Questions?
Thank you!!**

Joseph J. Lazzarotti, Esq.

Jackson Lewis LLP

White Plains, NY

914-328-0404

lazzarottij@jacksonlewis.com

Visit our blog:

<http://www.workplaceprivacyreport.com/>