



September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY



**Defending the Fortress:
New Threats Meet New Defenses**



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Mitigating Risk By Evaluating 7 Key Areas of Your Business

Nick Akerman
Trial Group Partner
Dorsey & Whitney, LLP



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Companies Can Mitigate Their “Risk” by Re-Evaluating 7 Areas of Their Business

- Hiring Practices
- Company Rules
- Appropriate Agreements
- Use of Technology
- Termination Practices
- Protocols for Response
- Company Compliance Program





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

HIRING PRACTICES



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

The Hiring Process

- Honor Prior Employment Agreements
- Explain Company Obligations
 - Company Policy
 - Employment Agreements
- Criminal Exposure for the Company





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

COMPANY RULES



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Computer Fraud and Abuse Act Provides Proactive Tool to Protect Data

- Title 18 U.S.C. § 1030 – Enacted in 1984
- Criminal statute
- Civil remedy in 1994 amendment
- Computers used in interstate commerce
- Amended in 2001 and 2008
- Provides for damages and injunction





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Various Causes of Action

- Stealing valuable computer data
- Schemes to defraud
- Trafficking in a computer password or similar information with intent to defraud
- Damaging computer data
- Hacking
- Extortion
- Sending computer viruses





THE SECURITY STANDARD™

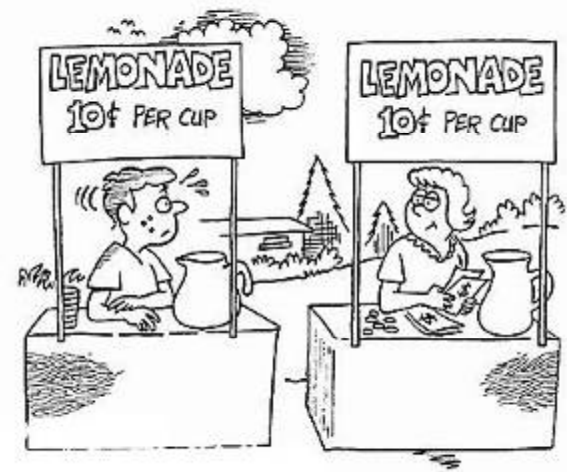
September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

EF Cultural Travel v. Explorica

- Ex-employees set up competing student travel company
- Information was accessed through public website
- Robot created with confidential information
- Used robot to download pricing data
- First Circuit upheld injunction based on confidentiality agreement
- Authorization established by contract
- Pricing data was valuable





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Authorization Established by Company

- First Circuit: the CFAA “is primarily a statute imposing limits on access and enhancing control by information providers.”
- Companies can set predicate for CFAA violation
- Rules on authorized access
- Agreements can set limits
- Similar to criminal trespass



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Company Rules

- Employee Handbook
- Corporate Computer Policies
- Code of Conduct
- Training





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Website Terms of Use

- Protect business and customers
- Require users to provide accurate registration information
- Limit use of account to registered user at one computer at a time
- Prohibit use of web crawlers, robots and similar devices
- Post acceptable use guidelines that prohibit abuse, harassment and similar conduct
- Specify limitations on use of materials obtained (commercial use)





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

APPROPRIATE AGREEMENTS



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Agreements

- Officers/Employees/Third Parties
- Among related companies
- Confidentiality/Non-Disclosure
- Post employment restrictive covenants
- Anti-Raiding Covenants
- Agreement to search personal computers
- Permissions re use of the computers
- Customer agreements
- Data vendor agreements





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Working with Vendors

- Warranty and representation on compliance
- Indemnification
- Certification of compliance with EU Safe Harbor Framework
- Adequate insurance coverage
- General due diligence





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

USE OF TECHNOLOGY



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Use of Technology

- Password protection is simplest
- Access based on need to know
- Risks re transportable media
- Encryption
- Audit trail
- Forensic review





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

TERMINATION PRACTICES



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

The Termination Process

- Employees must return all company property
- Standard Exit Interview Form
- Explain post employment obligations
- Retain evidence





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

PROTOCOLS FOR RESPONSE



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Notification California Database Security Breach Act

- Effective July 1, 2003
- Companies must notify individuals of security breach that could lead to identity theft
- Security breach is “unauthorized access”
- Does not apply to public information
- Applies to all companies doing business in California regardless of where data is kept
- Authorizes private actions and does not bar class actions
- 46 states have enacted similar laws





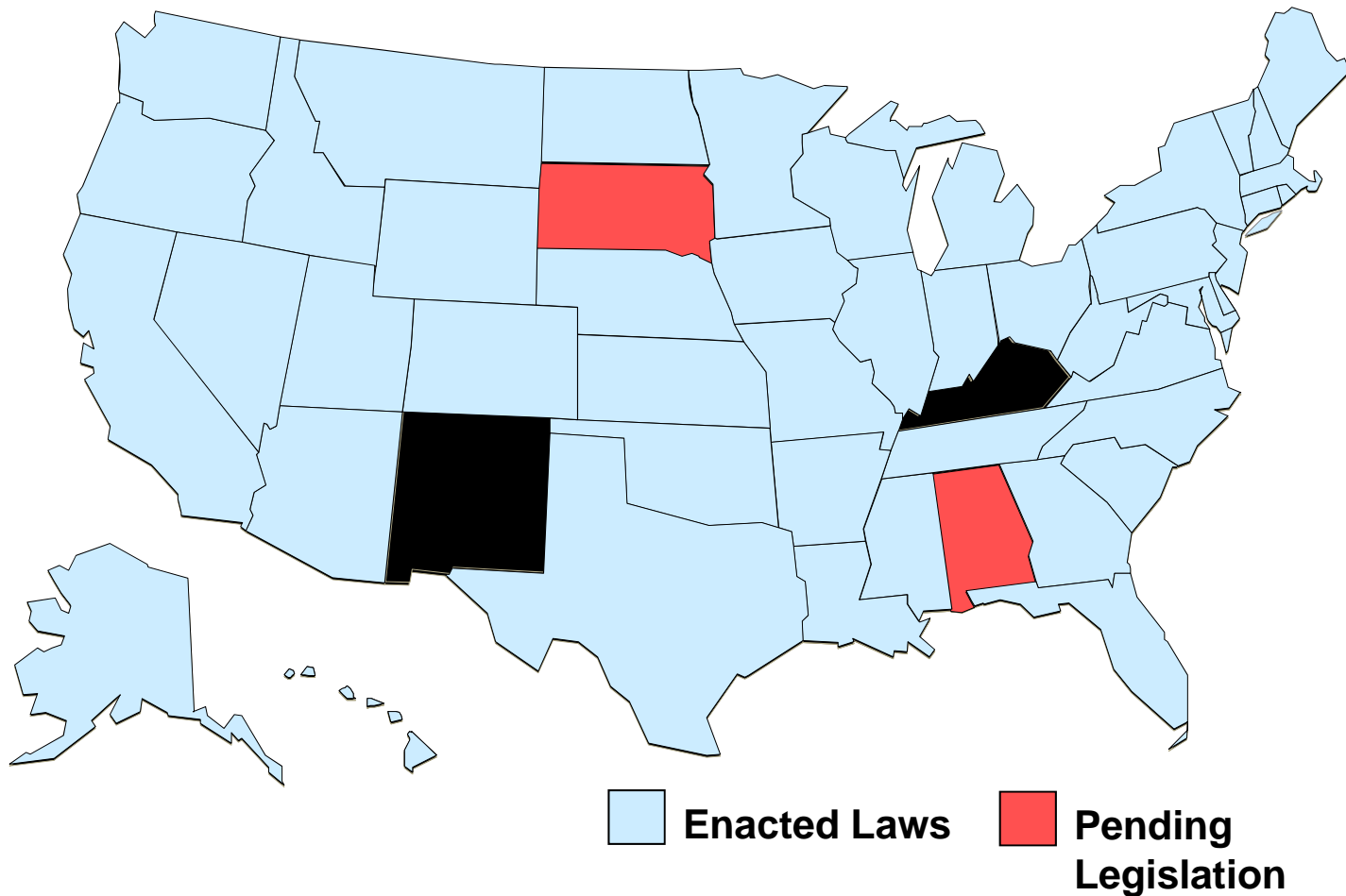
THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

States That Have Enacted Breach Notification Laws





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Provisions of the Statutes

- Notification requirement to consumers varies among states
- Third party vendors
- Different remedies
- Certain states exempt encrypted and/or redacted data from the notification process
- Timing standard varies
- Law Enforcement Exception
- Key issue is the ambiguous situation
- Investigation requirement





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

HITECH Act – 2009 Stimulus Package

- Amends HIPAA to include notification, September 2009
- Breach of protected information
- Breach as of date discovered or should be known
- Name alone is breach
- Electronic and paper records
- Encryption has to meet certain standards
- Notice to media in certain circumstances





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Protocols for Response

- Speed is of the essence
- Designate a coordinator
- Be investigative ready
- Be prepared to memorialize actions
- Notify law enforcement
- Prepare standard court papers with company policies and agreements





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

COMPANY COMPLIANCE PROGRAM



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Compliance

- New York Stock Exchange listed company compliance program must protect confidential information that “might be of use to competitors, or harmful to the company or its customers, if disclosed.”
- Effective as of October 31, 2004
- Part of Compliance standards and procedures
- Annual CEO certification





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

State Data Compliance Statutes

- Nevada – personal information must be encrypted when it is transferred – effective October 1, 2008
- Connecticut – businesses must “safeguard the data, computer files and documents containing the information from misuse by third parties.” – effective October 1, 2008
- Massachusetts Data Compliance rules effective March 1, 2010
 - Applies to a business located anywhere that stores or maintains personal information about a Massachusetts resident
 - Mandates a compliance program consistent with the Federal Sentencing Guidelines
- Washington State – personal information encrypted effective July 1, 2010



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Massachusetts – Administrative, Technical and Physical Safeguards

- Develop Security Policies that are enforced through encryption
- Appoint Security Coordinator
- Minimize risks from third parties terminated access to former employees and ensuring compliance by vendors
- Train the workforce on importance of personal information security
- Conduct regular audits at least annually
- Enforce the policies through disciplinary measures and document responsive actions
- Respond to incidents encouraging employees to report violations



THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

TJX Multi-State Settlement

June 24, 2009

- 2007 data breach to cardholder data and other personal data
- Investigation and action by 41 States
- TJX agreed to implement and maintain a comprehensive data security program
- Must report regularly to the State Attorney Generals on the efficacy of the security program
- \$9.75 million paid to the States





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Federal Trade Commission Requirements

- Failure to secure personal data is an unfair trade practice – Title 15 U.S.C. Section 45(a)
- Claims about data security should be accurate
- Protect against common technology threats
- Know the identity of third parties with whom sharing customers' sensitive information
- Do not retain unneeded sensitive consumer information
- Dispose of sensitive consumer information properly





THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Nick Akerman

Dorsey & Whitney LLP

akerman.nick@dorsey.com

212-415-9217

<http://www.computerfraud.us>