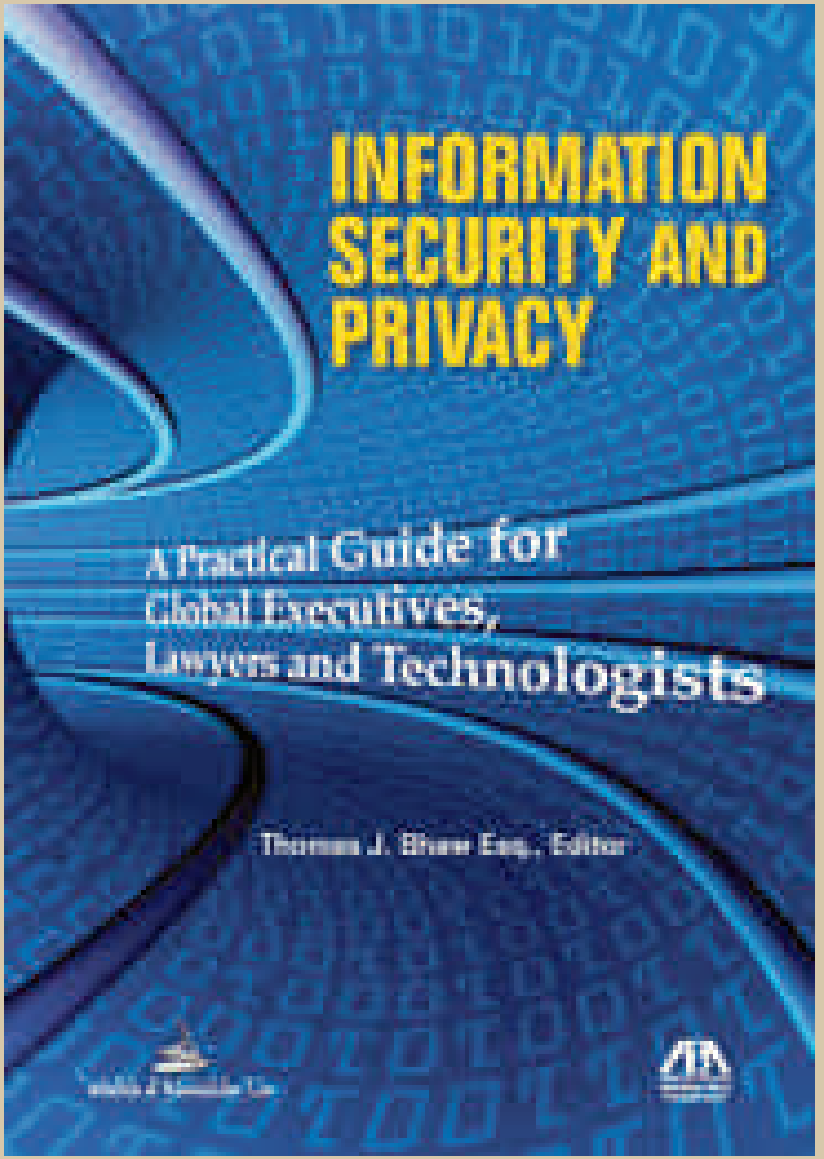
March, 2012

Information Security Law Update 2012

David G. Ries, Esq.

412-394-7787
dries@thorpreed.com


Information Security Committee
ABA Home > Sections > Section of Science & Technology Law > Information Security Committee
Section Home
Membership
News & Annoucement
Events & CLE
Committees
Publications
Resources
About Us
Contact Us
Information Security Committee
About the Committee
Resources
Documents
ABA Section of Science & Technology Law
Information Security Committee Home
Announcements
WINTER 2012 VOLUME 3 ISSUE 1 11/22/2011 10:00 AM
by Maria Gamboa
INFORMATION SECURITY & PRIVACY NEWS
Inside This Issue
Privacy Innovations at the U.S. Federal Trade Commission
By Mari Frank
Who Let the Data Out? An Overview of Access Controls and Why They Matter
By Rebecca H. Davis
A Work in Process: ...


INFORMATION SECURITY AND PRIVACY
A Practical Guide for Global Executives, Lawyers and Technologists

1. Background

U.S. Information Security Law

"A Patchwork Quilt"

Data Governance

- Information Security
- Records & Information Management
- Privacy

- E-Discovery / Litigation Holds

Information Security

Process

- People
- Policies & Procedures
- Technology

Information Security

Protect

- Confidentiality
- Integrity
- Availability

Information Security

- Assign responsibility
- Training
- Security awareness

Current Trends

- Generally increasing duties
- High level legal duties better defined
- Still substantial uncertainty
- Generally greater potential for liability

Information Security Laws

1. Laws protecting computers, networks and communications
2. Laws requiring safeguards
3. Other laws

Computer Protection Laws

1. Computer Fraud and Abuse Act
2. Electronic Communications Privacy Act
3. State Laws

Laws Requiring Safeguards

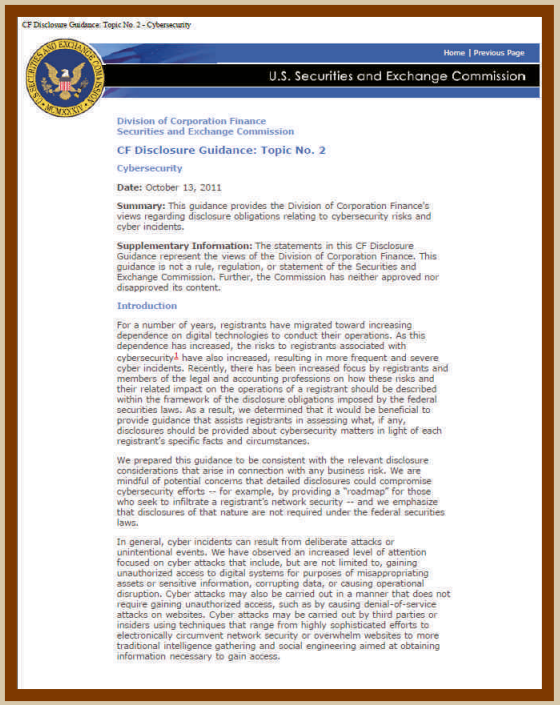
- Federal Information Security Management Act
- Financial Industries Modernization Act (GLB)
- Health Insurance Portability and Accountability Act (HIPAA)
- Children's Online Privacy Protection Act
- Fair Credit Reporting Act (FACTA)

Laws Requiring Safeguards

- Sarbanes-Oxley Act
- Family Educational Rights and Privacy Act
- Federal Trade Commission Act
- State Laws

SEC Cybersecurity Guidance

- October 13, 2011
- disclosure of risk and cyber incidents



CF Disclosure Guidance: Topic No. 2 - Cybersecurity

Home | Previous Page

U.S. Securities and Exchange Commission

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

Supplementary Information: The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content.

Introduction

For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity[1] have also increased, resulting in more frequent and severe cyber incidents. Recently, there has been increased focus by registrants and members of the legal and accounting professions on how these risks and their related impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities laws. As a result, we determined that it would be beneficial to provide guidance that assists registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant's specific facts and circumstances.

We prepared this guidance to be consistent with the relevant disclosure considerations that arise in connection with any business risk. We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts -- for example, by providing a "roadmap" for those who seek to infiltrate a registrant's network security -- and we emphasize that disclosures of that nature are not required under the federal securities laws.

In general, cyber incidents can result from deliberate attacks or unintentional events. We have observed an increased level of attention focused on cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.

2. The Emerging Legal Standard

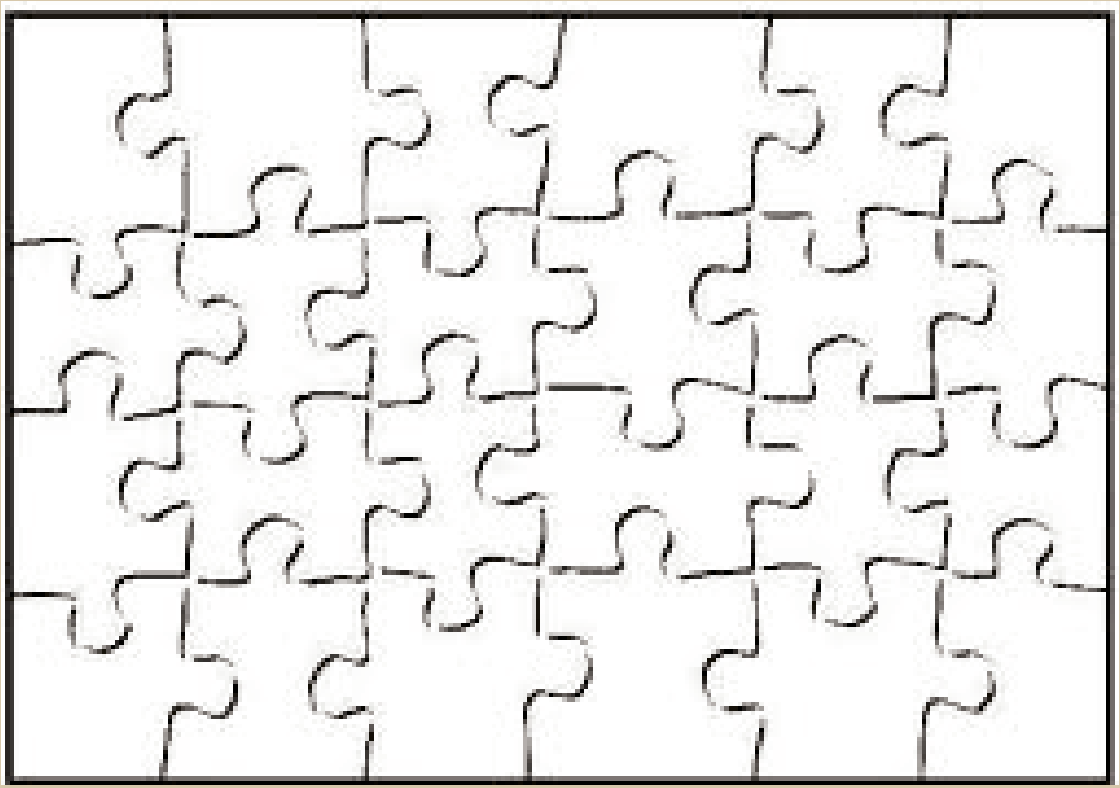
- High level legal duties
- Better defined
- Consistent

- Develop, implement and maintain
- A comprehensive information security program
- Written

- Administrative, technical and physical safeguards
- Appropriate to:
  - Size and complexity
  - Nature and scope of activities
  - Sensitivity of information

- Based on a risk assessment
- Designate responsibility
- Training
- Third parties

Emerging Standard



“Reasonable” “Appropriate”

- Legal requirements
- Standards and benchmarks

Legal Requirements

- Federal Agencies
  - GISRA / FISMA
  - National Institute for Standards and Technology (NIST) (U.S. Dept. of Commerce)
  - National Security Agency (NSA)
- G-L-B, HIPAA, COPPA, state laws

Standards / Benchmarks

- ISO Standards
  - 27002:2005
  - 27001:2005
- FFIEC
- Center for Internet Security
- CERT
- US-CERT
- Legal Standards as guides:
  (NIST, NSA, OMB)
  (G-L-B, HIPAA, COPPA)

3. Data Breaches Continue

- High profile consumer data breaches
- Commercial data / intellectual property

Data Breaches

- Steal $
- Steal IP
- Steal national security info
- Hactivism

Consumer Data Breaches

2011

- Breaches: 419
- Exposed: 22,918,441

2010

- Breaches: 662
- Exposed: 16,167,542

High Profile Breaches

BJs Wholesale Clubs	✓
ChoicePoint	✓
DSW Shoe Warehouse	✓
CardSystems	✓
Dept of Veterans Affairs	X
TJX	✓
Hannaford Bros.	✓
Heartland Payment Sys.	✓

Consumer Data Breaches

Privacy Rights Clearinghouse

www.privacyrights.org/ar/ChronDataBreaches.htm

DataLossDB

http://datalossdb.org/

Interhack

Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry

http://web.interhack.com/publications/breach-taxonomy

Bloomberg

China-Based Hackers Target Law Firms to Get Secret Deal Data

By Michael A. Riley and Sophia Pearson - Jan 31, 2012

China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer by an Australian mining giant zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal.

4. Federal Enforcement Escalates

- Federal Trade Commission
- Dept. of Health and Human Services
- Securities and Exchange Commission
- Financial Industry Regulatory Authority (independent regulator)

FTC Enforcement

- Violation of laws & regulations
- Misrepresentations or false promises
  -"Deceptive trade practices"
- "Unfair trade practices"

FTC Enforcement
Lookout Services

- software to keep track of the immigration requirements of their employees
- Employee of customer was able to access info about 37,000 persons
- Inadequate security ="unfair trade practices"

Mass. V. Briar Group
(Mass. Superior)

- 2009 data breach exposing debit and credit cards
- failure to implement basic data security measure
- failure to comply with PCI DSS
- $110,000 + corrective measures

Department of Justice

FOR IMMEDIATE RELEASE
Tuesday, August 6, 2008
WWW.USDOJ.GOV

AG
(202) 514-2007
TDD (202) 514-1888

Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers

More Than 40 Million Credit and Debit Card Numbers Stolen

BOSTON – Eleven perpetrators allegedly involved in the hacking of nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers have been charged with numerous crimes, including conspiracy, computer intrusion, fraud and identity theft, Attorney General Michael B. Mukasey, U.S. Attorney for the District of Massachusetts Michael J. Sullivan, U.S. Attorney for the Southern District of California Karen P. Hewitt, U.S. Attorney for the Eastern District of New York Benton J. Campbell and U.S. Secret Service Director Mark Sullivan announced today. The scheme is believed to constitute the largest hacking and identity theft case ever prosecuted by the Department of Justice.

Three of the defendants are U.S. citizens, one is from Estonia, three are from Ukraine, two are from the People's Republic of China and one is from Belarus. One individual is only known by an alias online, and his place of origin is unknown.

Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers

More Than 40 Million Credit and Debit Card Numbers Stolen

data in encrypted computer servers that they controlled in Eastern Europe and the United

- TJX Companies
- BJ's Wholesale Club
- DSW Shoe Warehouse
- OfficeMax
- Boston Market
- Barnes & Noble
- Sports Authority
- Forever 21
- Hannaford Brothers
- 7 Eleven
- Heartland Payment Systems

Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks.

5. States Lead in New Laws

- Data Breach Notice
- Credit Freeze
- Reasonable Security
- Encryption
- Secure Disposal
- Liability for Breaches

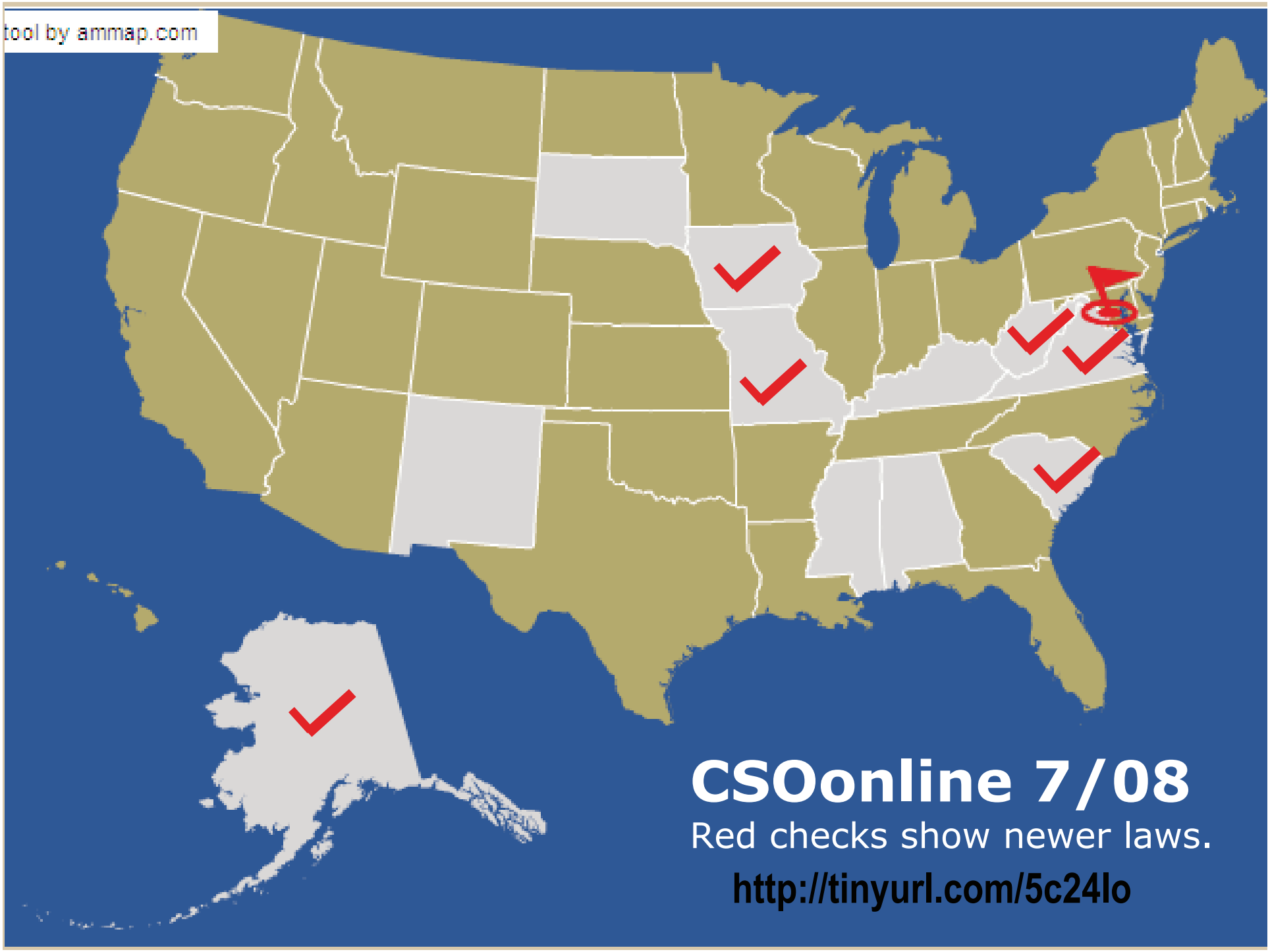
States Lead in New Laws

- Data Breach Notice - 46
- Credit Freeze - 47
- Reasonable Security - 10
- Encryption - 6
- Secure Disposal - 23
- Liability for Breaches - 3
- SSN Protection - 34

State Laws

- **Breach notification**
  - **Cal Database Security Breach Notification Act**
  - **46 states**
  - **PA law 73 P.S. §2301-2329**
  - **List of laws:** http://tinyurl.com/pmyrmb

"Doing Business"


tool by ammap.com
CSOonline 7/08
Red checks show newer laws.
http://tinyurl.com/5c24lo

Notice of Breaches

- Information covered
- Entities covered
- Definition of "breach"
- Who must be notified
- Risk of harm
- Time of notice
- Form or method of notice
- Exceptions
  - Safe Harbor
  - Encryption

New Mass. Law - M.G.L. c. 93H

- "persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts"

- "shall develop, implement, maintain and monitor a comprehensive, written information security program"

New Mass. Law - M.G.L. c. 93H

Office of Consumer Affairs and Business Regulation

- **201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth**
- **Effective March 1, 2010**
  - www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

6. Economic Stimulus

- The American Recovery and Reinvestment Act of 2009

- Health Information Technology for Economic and Clinical Health (HITECH) Act
  - promote the use of electronic health records by all hospitals and physicians by 2015
  - enhanced privacy & security

HITECH

- HIPAA privacy & security rules extended to business associates
  - Definition of "business associates" expanded
- Breach notice requirement
- Increased enforcement and penalties

7. Victims Face An Uphill Battle

- **Consumers**
  - Increased Risk
  - Victims of ID Fraud or ID Theft
- **Financial Institutions**

Common Law

- Contract
- Negligence
- Products Liability
- Directors' & Officers' Liability

Losses

- Financial Institutions
  - Unauthorized transactions
  - Closing/replacing accounts
- Retailers
- Victims
  - Identity Theft / Fraud
  - Data Breaches

Consumer Cases

- Negligence barred by economic loss rule
- Increased risk of identity theft is insufficient

In Re Hannaford Bros. Customer Data Security Breach Litigation

(D. Me.)

(1st Cir.)

Patco Construction Co., Inc. v. People's United Bank (D. Me.)

- Summary judgment on commercial customer's claims
- UCC Article 4A claims dismissed because bank applied reasonable security measures
- No conversion or unjust enrichment
- Other tort claims preempted by UCC

Experi-Metal, Inc. v. Comerica Bank
(E.D. Mich.)

- Claim by commercial victim of phishing attack that resulted in unauthorized wire transfers of more than $1.9 million
- In a nonjury trial, the court found for the plaintiff, finding that the bank violated its duty of good faith under the UCC by failing to detect and stop the transactions .

8. Contracting for Security

- Reasonable and appropriate safeguards
- Current industry standards
- Comply with all applicable laws and regulations
- Questionnaire
- Inspection / audit
- Notice of material changes

Contracts Requiring Safeguards

- HIPAA, G-L-B, etc.
- Payment Card Industry Data Security Standard (PCI)
- Outsourcing / Cloud
- Business partners

Questions

THORP REED & ARMSTRONG

- Based on a risk assessment
- Designate responsibility
- Training
- Third parties