



*Liability for
Security Breaches
Myth or Reality?*

THORP REED
—  —
ARMSTRONG

David G. Ries, Esq.

412-394-7787
dries@thorpreed.com

A Chronology of Data Breaches Reported Since the ChoicePoint Incident

Posted April 20, 2005.
Updated August 5, 2006.

Privacy Rights
CLEARINGHOUSE

Web: www.privacyrights.org

Contact Us:

www.privacyrights.org/inquiryform.html

HOME

A Chronology of Data Breaches Reported Since the ChoicePoint Incident

The data breaches noted [below](#) have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. A few breaches that do NOT expose such sensitive information have been included in order to underscore the variety and frequency of data breaches. However, we have not included the number of records involved in such breaches in the total because we want this compilation to reflect breaches that expose individuals to identity theft as well as breaches that qualify for disclosure under state laws.

The running [total](#) we maintain at the end of the Chronology represents the approximate number of *records* that have been compromised due to security breaches, not necessarily the number of *individuals* affected. Some individuals may be the victims of more than one breach, which would affect the totals.

For tips on what to do if your personal information has been exposed due to a security breach, read [our guide](#).

The catalyst for reporting data breaches to the affected individuals has been the California law that requires notice of security breaches, the first of its kind in the nation, implemented July

		and private medical history of chiropractic patients were found in a dumpster.	
Feb. 21, 2007	Georgia Institute of Technology (Atlanta, GA) 404-894-2499 hr@gatech.edu	Personal information of former employees mostly in the School of Electrical and Computer Engineering including names, addresses, Social Security number, other sensitive information, and about 400 state purchasing card numbers was compromised by unauthorized access to a Georgia Tech computer account.	3,000
Feb. 22, 2007	Speedmark (Woodlands, TX)	Thieves stole several computers, one of which contained a database with personally identifying information including names, addresses, e-mail accounts, and Social Security numbers of Speedmark's mystery shopper employees and contractors.	35,000
Feb. 23, 2007	Rabun Apparel Inc., former subsidiary of Fruit of the Loom (Rabun Gap, GA)	Names and Social Security numbers of former employees were accessible on the Internet from Jan. 15 until Feb. 20.	1,006
Mar. 1, 2007	We apologize for the delay in updating this listing. We expect to be back on track by March 7th or 8th. Thank you for your patience.	In the meantime, you can keep up to date on the latest security breaches here: http://attrition.org/dataloss/	
TOTAL number of records containing sensitive			104,106,513

104,106,513





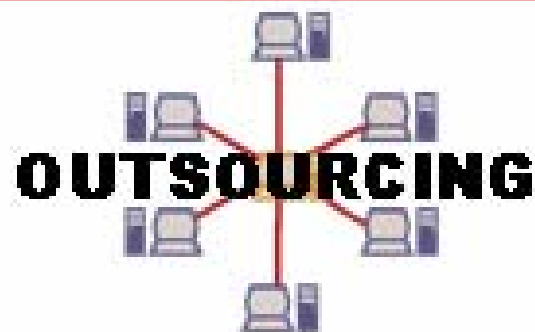
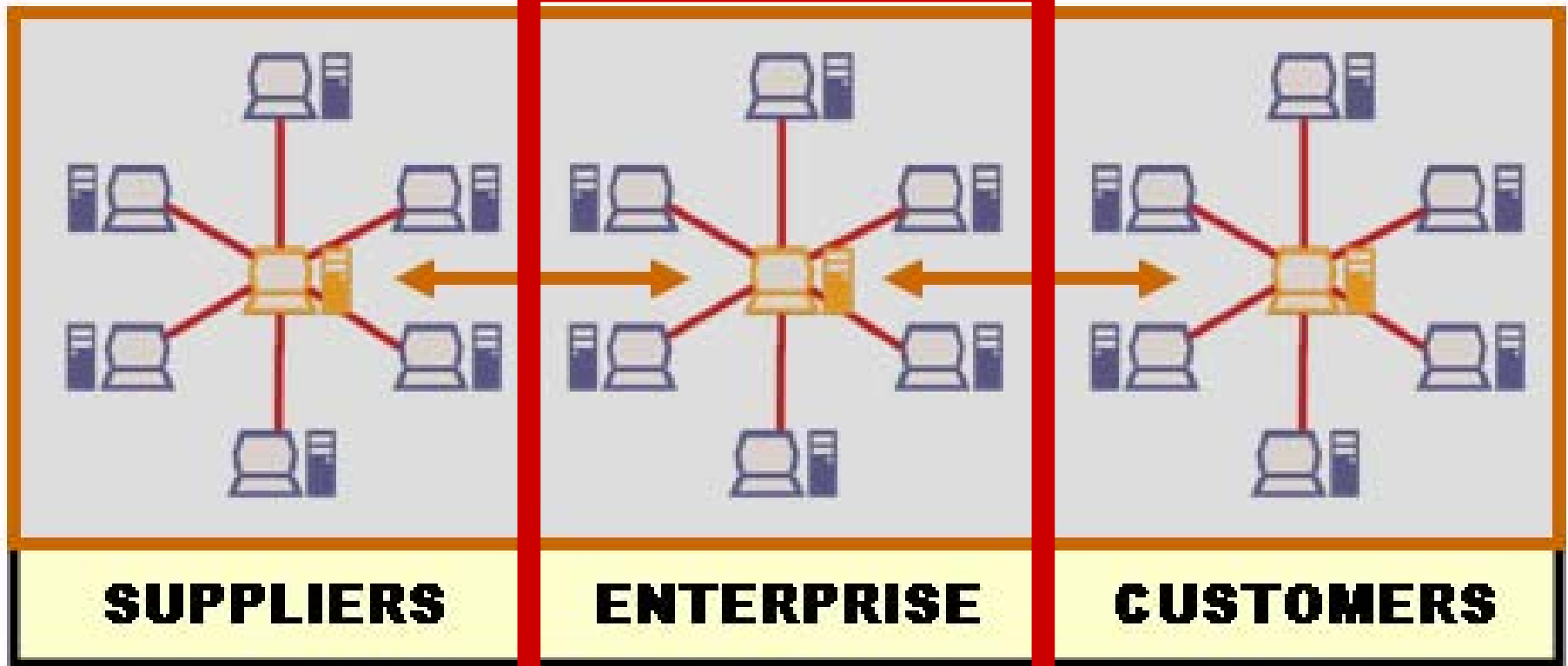
High Profile Breaches

- ❑ ChoicePoint
- ❑ Lexis/Nexis
- ❑ Colleges
- ❑ DSW Shoe Warehouse
- ❑ CardSystems
- ❑ Dept of Veterans Affairs
- ❑ UCLA
- ❑ Boeing



High Profile Breaches

 Dupont





Legal Outfall ?

- Substantial uncertainty
- Generally increasing duties
- Generally greater potential for liability

- 
- 1. *Statutes***
 - 2. *Security Standards***
 - 3. *Common Law***
 - 4. *Cases***



Statutes



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
- Health Insurance Portability and Accountability Act
- Children's Online Privacy Protection Act
- Sarbanes-Oxley Act
- New state laws



Federal Information Security Management Act (FISMA)



Financial Industries Modernization Act (Gramm-Leach-Bliley)



Health Insurance Portability and Accountability Act (HIPAA)



Sarbanes-Oxley

Conferences: Corporate Security

Corporate Security

Experts Debate Whether Sarbanes-Oxley Act Requirements On Internal Controls Mandate Information Security Policies

SAN FRANCISCO--Security experts speaking Feb. 24 on a panel at the RSA Conference 2004 in San Francisco offered differing views on whether the Sarbanes-Oxley Act implicitly requires companies to adopt information security policies.

“Sarbanes-Oxley: The Stealth Information Security Law?”

and procedures for financial reporting,” and (2) an assessment of the effectiveness of the internal controls and procedures for financial reporting.

Section 302 of the act requires the chief executive officer and chief financial officer to certify that they have reviewed the filed report, that they are responsible for overseeing disclosure controls, and that the report contains no material misstatements or omissions.

Burton said the certification requirements of Section 302 give the act “teeth.” He said that disclosure controls include, “without limitation, controls and procedures designed to ensure that information required to be disclosed by an issuer in its Exchange Act reports is accumulated and communicated to the issuer’s management” in a timely manner.



New California Law

Cal. Assembly Bill 1950

-signed 9/04

- Businesses that own or license personal info about Cal residents**
- Must implement and maintain reasonable security practices and procedures to protect**



Proposed Laws

- **Licensing of data brokers**
- **Require reasonable security
(Extend Gramm-Leach-
Bliley Safeguards Rule)**
- **Notification of compromises**




Reasonable Security

- Cal law
- Ariz, Nev, RI, Tex, Utah
- Mass – shift liability to entity responsible for breach (pending)



Notice of Breaches

 **California Database
Security Breach
Notification Act
-in effect**

 **Federal Notification of
Risk to Personal Data Act
-pending**



State Laws

 **Breach notification**
35 states

–New PA law

 **Credit freeze**
24 states

Federal law with preemption?



State Laws

Proposed Maryland law

- Notice of breaches
- Reasonable information security
- Secure disposal

The new model?



Secure Disposal

■ FTC Disposal Rule
(FACTA)

■ Ark, Ky, Hi, NJ, NC, Tex,
Utah



Other Laws

1. **FTC Act**
 2. **Securities Laws**
 3. **Fair and Accurate Credit Transactions Act**
-
4. **IP Laws**
 5. **PATRIOT Act**
 6. **Identity Theft and Assumption Deterrence Act of 1998**
 7. **CAN SPAM**



Federal Trade Commission Act



Securities Laws

- Disclosure of adequacy of information security program?
- Disclosure of risks?
- Disclosure of intrusions?



***Security
Standards***



Legal Standards

Federal Agencies

–GISRA / FISMA

–National Institute for
Standards and Technology
(U.S. Dept. of Commerce)

–National Security Agency

G-L-B, HIPAA, COPPA



Standards / Benchmarks

- ISO Standards

 - 17799:2000

 - 27001:2005

- NIST

- NSA

- OMB

- FFIEC

- Center for Internet Security

- CERT

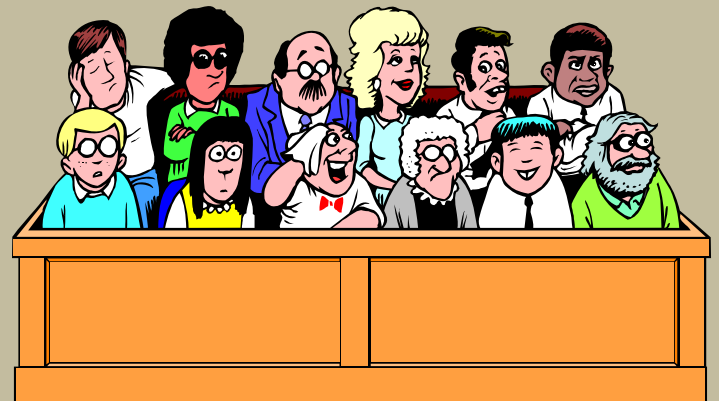
- US-CERT



Common Law

Common Law

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





Contracts

- **Agreements**
- **Generally binding only on parties**
- **Terms generally enforced**



Contracts

- ❑ Exclusions or limitations of warranties
- ❑ Limitations of damages
- ❑ E.g., software EULA



Negligence

**Failure to exercise
reasonable care**



Negligence

 **Duty**

 **Breach**

 **Causation**

 **Damages**



Negligence

Duty

- Reasonable care
- Foreseeability



Negligence

- Failure to comply with industry standards
- Negligence per se - failure to comply with a law or regulation



Negligence

Standard of Care

- Industry standards
- Best practices
- Benchmarks



Negligence

❑ Economic loss rule

❑ Foreseeability

❑ Intervening criminal act



Products Liability

- ❑ **Defect-**
unreasonably dangerous
to persons or property
- ❑ **Strict liability**
- ❑ **Unlikely to apply to usual
infosec situations**



Directors & Officers

■ Business Judgment Rule

■ *Caremark Int'l Inc.*
Derivative Litigation
698 A.2d 959 (Del. Ch. 1996)

■ AICPA

*Information Security
Management and Assurance:
A Call to Action for
Corporate Governance*



Cases




Legal Outfall

- Generally increasing duties
- Generally greater potential for liability
- Substantial uncertainty




FTC Enforcement

1. Violation of laws & regs
2. "Deceptive trade practices"
3. "Unfair trade practices"



In re
BJ's Wholesale Club, Inc.
FTC 9/23/05
No. 042-3160
Consent Order



U.S. v. ChoicePoint, Inc.
N.D. Ga.
FTC Civil Action



***BJ's Wholesale Club
Litigation***



***ChoicePoint, Inc.
Class Actions***



***Guin v. Brazos Higher
Education Service Corp.***



TJX Cos, Inc. Litigation



Conclusions

Myth or Reality?



Avoiding Liability

- Understand all legal requirements.
- Conduct a risk assessment.
- Implement a sound information security program.
- Conduct training.
- Plan for incident response.
- Monitor, audit and update.



Questions

THORP REED
— & —
ARMSTRONG