PRESENTATION

It is not a Matter of “If” but “When”

May 10, 2013
San Francisco, CA

Alisa L. Chestler
Of Counsel

BAKER DONELSON

EXPAND YOUR EXPECTATIONS℠

It is not a matter of “If” but “When”. . .

- Mondiant- Cyber Security firm identified over 140 organizations in which the Chinese government was stealing valuable intellectual proper blueprints, proprietary manufacturing information; IT space; construction, aerospace & energy.

- Sony’s PlayStation Network was down for nearly a week when Sony finally admitted that an unauthorized person had stolen personal information belonging to **77,000,000** account holders. A class action lawsuit was filed a day later, with several others following.

- Chinese hackers conduct coordinated, covert and targeted campaign of cyber espionage against major Western energy firms. Official dubbed the attacks “Night Dragon” and alerted companies to the hacking tools and exploits used against Microsoft operating systems.

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

More . . .

- Zappos, in January 2012, the company announced that more than 24 million of its customers accounts had been compromised.

- BlueToad- September 2012. Originally thought that the FBI had information stolen from a agent's laptop. Later determined to be the result of hackers entry into BlueToad, which works with online publishers to translate printed content into digital and mobile formats. One million ID numbers (U.D.I.D.) of Apple mobile device users.

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Why are we here?

Corporate Board Member/FTI Consulting 2012 Law and the Boardroom

- Data Security
  - 48% Directors
  - 55% General Counsel
- Operational Risk
  - 40% Directors
  - 47% General Counsel

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

So what does that mean?

- Need to have an understanding of the laws which impact the company and your vendors
- Need to have an understanding of the kind of data collected, not just actively but passively.
- Need to have an understanding of the company's information security policies and procedures, those documented and those undocumented.
- Need to have an understanding of compliance with the laws.

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Legal Framework

- United States

  Sectorial and self-regulatory

- Canada

  Co-regulatory

- EU – Comprehensive

  DPA – Data Protection

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Federal Laws- a few sectorial concerns

- FCRA- Fair Credit Reporting Act
- HIPAA- Health Information Portability and Accountability Act
- GLB- Gramm-Leach-Bliley
- PCI DSS- Payment Card Industry

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

SEC Guidance- October 13, 2011

"This Guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further the Commission has neither approved nor disapproved of its content."

But just ask . . .

- Zappos
- Amazon
- The Hartford
- Eastman Chemical

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

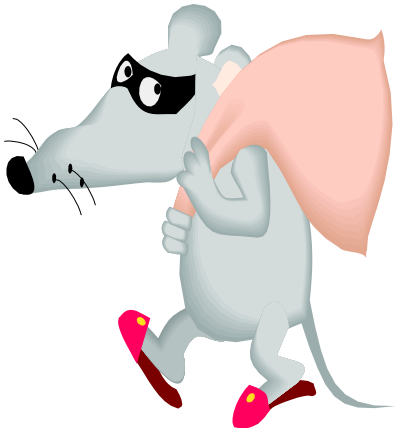
State Laws and Enforcement

- Massachusetts
- Nevada
- Texas
- California

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

State Data Breach Notification Laws

- ChoicePoint (2005)
- 46 States
- Electronic Information
- Risk of Harm analysis
- Reporting to individual and regulators



© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Regulatory fines

- BCBST paid over $1.5 million for data breach stemming from a loss of 57 back up tapes. That was in addition to the over $19M spent on remediation and mitigation efforts.

- South Shore Hospital in Weymouth, Mass., agreed to a $750,000 settlement with the state Office of Attorney General following a breach of protected health information that affected about 800,000 patients in 2010.

- Lucile Salter Packard Children's Hospital- CDPH imposed the maximum $250,000 fine for failing to report within 5 days a breach involving 532 patients. The breach resulted from an employee of LSPCH stealing a laptop. Breach was reported within 2 weeks.

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Class Action Theories

- Negligence, negligence per se,
- Breach of contract, breach of implied contract,
- Breach of implied covenant of good faith and fair dealing,
- Breach of fiduciary duty, and
- Unjust enrichment

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Class Action Cases

Resnick v AvMed, Inc. 693 F.3rd 1317 (11th Circuit), 2012) – Held the plaintiff's allegations of injury and causation were sufficient to withstand the motion to dismiss where they suffered identity theft due to a data breach.

Remanded to US District Court for S. District of Florida

Trial scheduled December 2013.

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Nationwide Insurance

Hancox et al. v. Nationwide Mutual Insurance Co., Case No. 13-cv-02047, filed in Federal Court in Kansas

Department of Insurance:

"While Nationwide has briefed my department and agreed to update us with the findings of its internal investigation, I've instructed staff to conduct a follow-up review of the breach to ensure the company has taken the necessary steps to guard against a future system failure."

"In a global economy, driven by electronic commerce, it is essential that all necessary steps are taken to ensure consumers are protected from an unintentional release or criminal theft of their personal data."

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

And more to follow . . .

- *In re Hannaford Brothers Company Data Security Breach Litigation*
- Sutter- 11 suits rolled into one- fight to get and keep in complex case using in Sacramento
- And coming soon . . . this weeks breach . . .

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Breach Incident Response

- Identification of Team
- Identification of Vendors
- Understanding of State and Federal laws and DEADLINES
- Understanding of Steps to take
- Regulators to contact
- Prepared with Credit Monitoring

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Moving to compliance . . .

- Due Diligence (M&A and contracting)
- Vendor Assessment
- Privacy Compliance
- Security Assessment & Documentation

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Vulnerabilities

- Data Loss – Laptops and especially PDAs
- Hackers
- Disaster Recovery & Business Continuity Plans

and of course. . . there is always

- Stupidity

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Outsourcing IT functions

- Hosting versus Cloud- Virtually every company today outsources some component of their IT system to third parties.

- Data “owner” still liability for privacy or security breaches

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Insurance

- Business interruption as a result of network or web site outage
- Costs from comprised digital assets
- Cyber extortion – threats to post/sell security vulnerabilities and/or confidential data
- Theft or destruction of Trade Secrets
- Breach notification and mitigation
- Reputational loss

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Insurance

- Enterprise wide data privacy wrongful acts whether from internal or external “hacker”
- Use of your network to launch at attack or “leapfrog” into third party web sites and/or networks (which may or may not be your clients)
- Unsolicited electronic communications
- Intellectual property infringement
- Economic harm to your customers for inability to meet contractual obligations
- Reputational loss

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

Questions?

Alisa Chestler

Baker, Donelson, Bearman, Caldwell & Berkowitz
920 Massachusetts Avenue, NW
Washington, DC 20001
202.508.3475

achestler@bakerdonelson.com

Twitter: @alchestler

© 2013 Baker, Donelson, Bearman, Caldwell & Berkowitz, PC