Big Data, Big Opportunities and Risks: What You Need to Know about Data Security

Melissa Krasnow, Dorsey & Whitney LLP

Bridget Sakach, AIG

This presentation was created by Dorsey & Whitney LLP, 50 South Sixth Street, Suite 1500, Minneapolis, MN 55402. This presentation is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances. An attorney-client relationship is not created or continued by sending and/or receiving this presentation. Members of Dorsey & Whitney will be pleased to provide further information regarding the matters discussed in this presentation.
“Though 83% of executives claim to dislike the term Big Data, or find it to be overstated, it must be admitted that Big Data has served as an effective rallying cry and focal point that has raised awareness of data as a corporate asset – love the term or hate it.”

Source: NewVantage Partners Big Data Executive Survey 2014.
Data security risks with Big Data

“Big Data creates potential targets of increased value.”


Big Data presents “heightened data security risks” and “....companies need to take reasonable steps to safeguard consumers’ personal information. The importance of implementing reasonable data security cannot be overstated.”

Cybersecurity laws and guidance and provisions in contracts and policies

• Federal Trade Commission’s Start with Security guidance (June 2015) and Staff Report on Internet of Things (January 2015)

• National Institute of Standards and Technology’s critical infrastructure cybersecurity framework (February 2014)

• Federal Financial Institutions Examination Council on Cybersecurity Awareness

• Interagency Guidelines Establishing Standards for Safeguarding Customer Information
Cybersecurity laws and guidance and provisions in contracts and policies (cont.)

• Massachusetts and certain other states (e.g., California) have security procedures laws

• California Attorney General, California Chamber of Commerce and Lookout: Cybersecurity in the Golden State (February 2014)

• Laws and guidance in other countries (e.g., Canada)

• Provisions in contracts and policies
State breach notification laws and SEC guidance

- 47 states, plus the District of Columbia, Guam, Puerto Rico and Virgin Islands, have breach notification laws that require notification of a breach to affected individuals (Alabama, New Mexico, and South Dakota do not have these laws)

- 23 state breach notification laws*, plus Puerto Rico law, also require notification of a breach to a state attorney general or regulator in addition to the affected individuals

*Includes Connecticut, Montana and Rhode Island law amendments

Federal and foreign breach notification laws and provisions in contracts and policies

- Federal HIPAA / HITECH Act breach notification for covered entities and business associates regarding protected health information
- Will there be a comprehensive federal breach notification law?
- Laws and guidance in other countries (e.g., Canada)
- Provisions in contracts and policies
Incident response plan guidance

- Department of Justice’s Best Practices for Victim Response and Reporting of Cyber Incidents (April 2015)
- National Institute of Technology’s Computer Security Incident Handling Guide (August 2012)
- California Attorney General, California Chamber of Commerce and Lookout: Cybersecurity in the Golden State (February 2014)
Enforcement, litigation and other consequences

- Federal regulators (e.g., Federal Trade Commission, financial institution regulators, Department of Health and Human Services, Securities and Exchange Commission, etc.)
- State regulators (e.g., California and Massachusetts state attorneys general)
- Foreign regulators
- Litigation
- Other consequences
Some steps organizations are taking to prepare

• Preparing, revising and testing incident response plans: tabletop exercises (TTXs)
• Preparing and revising company policies and programs, including training
• Procuring security and data breach services
• Oversight by board of directors / committee
• Governance
• Considering or reviewing cyber liability insurance
Cyber liability insurance

Main coverages in a traditional cyber liability insurance policy include:

- Security and privacy liability insurance that responds to third party liability
- Event management insurance that responds by paying costs for breach notification, public relations and other services to assist in managing a covered privacy or network security incident
- Cyber extortion insurance that pays to settle network security-related extortion demands made against the insured
- Network business interruption insurance that responds to an insured’s loss of income and operating expenses when business operations are interrupted or suspended due to a failure of network security
Resources – Big Data; Cybersecurity

Big Data

- Protecting Privacy in the Era of Big Data

- DRAFT NIST Big Data Interoperability Framework (Draft Version 1, April 6, 2015)
  http://bigdatawg.nist.gov/V1_output_docs.php

- Big Data Executive Survey 2014

Cybersecurity

- Written Information Security Programs

- Cybersecurity White Paper

- Start with Security
Resources – Cybersecurity (cont.)

- Staff Report on Internet of Things

- Framework for Improving Critical Infrastructure Cybersecurity

- Cybersecurity Awareness
  https://www.ffiec.gov/cybersecurity.htm

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information
  https://www.federalregister.gov/articles/2001/02/01/01-1114/interagency-guidelines-establishing-standards-for-safeguarding-customer-information-and-rescission

- Cybersecurity in the Golden State
  https://oag.ca.gov/cybersecurity
Resources – Breach Notification/Disclosure

- State Breach Notification Laws Continue to Change

- CF Disclosure Guidance: Topic No. 2

- Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
Resources – Incident Response Plans

• Guidance for Incident Response Plans

• Best Practices for Victim Response and Reporting of Cyber Incidents

• Computer Security Incident Handling Guide
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

• Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (see slide 14)

• Cybersecurity in the Golden State (see slide 13)
Resources – Boards of Directors and Corporate Governance

- Board Oversight of Cyberrisks: Directors and Officers Litigation

- Boards of Directors, Corporate Governance and CyberRisks: Sharpening the Focus

  [http://www.nacdonline.org/Cyber](http://www.nacdonline.org/Cyber)
Questions and Answers

Melissa Krasnow, Dorsey & Whitney LLP
(612) 492-6106
krasnow.melissa@dorsey.com

Bridget Sakach, AIG
(216) 479-8951
Bridget.Sakach@aig.com