Data Privacy & Protection

March 10, 2016

Data Breach Notification and Cybersecurity Developments in 2016

Melissa J. Krasnow, Dorsey & Whitney LLP, and Certified Information Privacy Professional/US

Cyber risk

“There is, however, one clear, present and enduring danger to Berkshire against which Charlie and I are powerless. That threat to Berkshire is also the major threat or citizenry faces: a “successful” (as defined by the aggressor) cyber, biological, nuclear or chemical attack on the United States. That is a risk Berkshire shares with all of American business....

There is no way for American corporations or their investors to shed this risk. If an event occurs in the U.S. that leads to mass devastation, the value of all equity investments will almost certainly be decimated.”

Source: Warren Buffet’s Letter to the Shareholders of Berkshire Hathaway Inc. (February 27, 2016) at http://www.berkshirehathaway.com/letters/2015ltr.pdf

State breach notification laws

- **47 states, plus the District of Columbia, Guam, Puerto Rico and Virgin Islands, have breach notification laws (Alabama, New Mexico, and South Dakota do not have these laws)**
- **These laws require notification of a breach to affected individuals**
- **These laws cover breaches involving personal information in electronic format**

State data breach notification requirements

- **23* state laws, plus Puerto Rico law, also require notification of a breach to a state attorney general or regulator in addition to the affected individuals**
- **8 state laws cover breaches involving personal information in both electronic and paper formats**
- **4* state laws cover identity theft prevention and mitigation services**

***Rhode Island's amendment to its law becomes effective June 26, 2016**

Breach notification in federal and foreign 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 in other countries**
- **Provisions in contracts and policies**

Cybersecurity laws and guidance and provisions in contracts and policies

- **State security procedures laws**
- **California Data Breach Report (February 2016)**
- **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)**
- **Provisions in contracts and policies**

Enforcement, litigation and other consequences

- **Federal Trade Commission**
- **Department of Health and Human Services**
- **State attorneys general and regulators**
- **Foreign regulators**
- **Litigation**
- **Other consequences**

Steps organizations are taking to prepare

- **Preparing, revising and testing incident response plans: tabletop exercises (TTXs)**
- **Preparing and revising company policies and programs**
- **Training and awareness**
- **Security and data breach services**
- **Oversight by board of directors / committee**
- **Governance**
- **Considering or reviewing cyber liability insurance**

Incident response plans

- **Does the organization have an incident response plan and / or business continuity / disaster recovery plan?**
- **When was the last time each was tested or updated?**
- **How frequently is each tested or updated?**
- **What was the situation that was the subject of the testing?**
- **What are the results of and insights from testing or updating?**
- **Who are the members of the incident response team?**
- **Who are external team members, including service providers?**
- **What are incident response team member responsibilities?**

Incident response plans (continued)

- **Is there contact information for incident response team members?**
- **What are the lines of communication?**
- **What communications/disclosures/notifications are anticipated (e.g., internal and external)?**
- **Is the organization prepared to work with law enforcement, regulators, industry contacts and business partners?**
- **Is any cybersecurity or related training or awareness provided for employees, etc.?**

Resources

- **Breach notification**
  - **State Breach Notification Laws Continue to Change**
    https://www.irmi.com/articles/expert-commentary/state-breach-notification-laws-continue-to-change
- **Cybersecurity**
  - **California Data Breach Report**
  - **Written Information Security Programs**
    http://files.dorsey.com/files/upload/Krasnow-MA-Data-Security-Regulation-mar-2015.pdf
  - **Start with Security**

Resources (continued)

- **Cybersecurity**
  - **Staff Report on Internet of Things**
  - **Framework for Improving Critical Infrastructure Cybersecurity**
  - **Cybersecurity in the Golden State**

Resources (continued)

- **Incident response plans**
  - **Guidance for Incident Response Plans**
    http://www.irmi.com/articles/expert-commentary/guidance-for-incident-response-plans
  - **Best Practices for Victim Response and Reporting of Cyber Incidents**
  - **Computer Security Incident Handling Guide**

Resources (continued)

- **Boards of directors and corporate governance**
  - **Director Cybersecurity Risk Oversight and Actions** file:///C:/Users/Owner/Downloads/Krasnow_Cybersecurity_risk_for_Directors_011116.pdf
  - **National Association of Corporate Directors 2014 Cyber Risk Oversight Handbook**

Questions and answers

Melissa Krasnow
krasnow.melissa@dorsey.com
(612) 492-6106 (t)
(312) 350-1082 (m)