Cybersecurity and Data Breach: Mitigating Risk and How Government Policymakers Approach These Critical Issues

Todd Bertoson
Principal
todd.bertoson@dentons.com
+1 202 408 5395

Daniel Gibb
Senior Managing Associate
daniel.gibb@dentons.com
+1 202 408 3938

Erin Sheppard
Counsel
erin.sheppard@dentons.com
+1 202 496 7533

Legislative activity on cybersecurity: Will Congress pass information sharing legislation?

- Legislation enacted over the past two Congresses has been largely noncontroversial.
- More than 20 bills have been introduced this Congress to address a number of cybersecurity issues.
- Information-sharing legislation is seen by industry and many security experts as the most important tool to improve cybersecurity.
- The House passed information sharing legislation, H.R. 1560 and H.R. 1731, in April 2015. However, the companion legislation in the Senate, S. 754, remains stalled.
  - These bills provide for incentives for companies to share threat information with each other and the federal government.
  - Provisions granting antitrust exemptions and liability protections for companies remain controversial.
  - Privacy protections are not adequate for many civil liberty advocates.

Administration activity to enhance cybersecurity practices

- Cybersecurity Executive Order 13636 (February 12, 2013)
  - Tasked the National Institute of Standards and Technology with developing a voluntary cybersecurity framework for critical infrastructure.
  - Required sector-specific agencies and the Department of Homeland Security (DHS) to identify critical infrastructure.
  - Required regulatory agencies to determine the adequacy of current requirements and their authority to new establish requirements to address the risks.
- Cybersecurity Executive Order 13691 (February 12, 2015)
  - Calls for establishing new "information sharing and analysis organizations to serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and government."
- Presidential Memorandum - Establishment of the Cyber Threat Intelligence Integration Center (CTIIC) (February 25, 2015)
  - The CTIIC is a national intelligence center focused on "connecting the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting US national interests, and on providing all-source analysis of threats to US policymakers.

Legislative activity on data breach: Will Congress pass federal data breach legislation?

Will 2015 be the year for a federal data security bill?

- More than 50 federal data security bills have been introduced since 2005, and not one has made it to the Rose Garden, leaving a patchwork of state laws in effect.
- On April 15, the House Energy and Commerce Committee passed a comprehensive data security bill—the Data Security and Breach Notification Act of 2015—on a party-line vote.
  - Sponsored by Rep. Blackburn (R-TN) and co-sponsored by Reps. Welch (D- VT), Burgess (R-TX) and Loebsack (R-IA)
  - During the mark-up, Rep. Welch ultimately voted against the bill, exposing ongoing party tensions
- The bill requires entities that collect and maintain personal information of individuals to secure that information and provide notice to the individual should a breach of security occur.
- Key elements of the bill include:
  - Requires companies to use “reasonable security measures” to protect an individual’s personal information.
  - Defines "personal information" to include:
    - An individual's first and last name, or first initial and last name and a government-issued ID number
    - An individual’s first and last name, or first initial and last name and any two of the following: home address or telephone number; mother’s maiden name; or date of birth
    - Financial account number or debit card number, a full Social Security number, and another unique account identifiers

Will 2015 be the year for a federal data security bill? (cont.)

- Key elements of the bill include:
  - Requires companies to notify affected individuals within 30 days, unless there is no reasonable risk that breach has resulted in, or will result in, identity theft, economic harm or financial fraud
  - Provides for enforcement by the Federal Trade Commission (FTC) and state attorneys general, and subject to civil penalties
  - Preempts state data security and breach notification laws
- Main sticking point: Does the bill exempt a company from liability under state common law?
- Senate Commerce Committee Ranking Member Nelson (D-FL) introduced S.177 in January 2015, which also requires companies to implement security policies for the treatment and protection of personal information and establishes procedures to be followed in the event of a breach.
- Senate Commerce Committee Chairman Thune (R-SD) is prepping his own draft data breach notification and data security bill but the path forward remains unclear.

Administrative action on data breach: FTC on the beat

FTC on the beat

- Since 2001, the FTC has taken enforcement action in more than 50 data security cases.
- Section 5 prohibition against "unfair or deceptive practices" may apply where a business has made false or misleading claims about its data security procedures, or failed to employ reasonable security measures and, as a result, causes or is likely to cause substantial consumer injury.
- Other federal statutes include the FTC's Safeguards Rule, the Fair Credit Reporting Act and the Children's Online Privacy Protection Act.
- *FTC v. Wyndham Worldwide Corp. et al.*

Cybersecurity requirements applicable to federal contractors

- Absent comprehensive cybersecurity legislation, there remains a patchwork of obligations applicable to government contractors.
  - Federal Information Security Management Act (FISMA) (44 U.S.C. § 3551-58)
  - HIPAA (42 U.S.C. § 1320d-2(d))
  - Privacy Act (5 U.S.C. § 552a)
  - Agency-specific security laws (e.g., NDAA § 941)

- Individual agencies have also enacted their own cybersecurity and/or information security regulatory requirements.
  - DOD, GSA, DHS, NASA
  - Each vary in terms of what standards they reference and what requirements they impose (e.g., NIST vs. internal policy; security controls; audits; incident response plans; training requirements)

Cybersecurity requirements applicable to federal contractors

- Cybersecurity Executive Order 13636 (Feb. 19, 2013)
  - Required GSA and DOD to craft a report on feasibility, benefits and merits of incorporating security standards into acquisitions.
  - Report was to address steps for harmonization and consistency in cybersecurity procurement requirements.

- So far in 2015 we have seen a trend toward greater uniformity in required controls and reporting obligations across procuring agencies, yet there has been no government wide rule-making.
  - NIST SP 800-171
  - OMB guidance

Cybersecurity requirements applicable to federal contractors

- Defense Federal Acquisition Supplement Interim Rule: Network Penetration Reporting and Contracting for Cloud Services, issued August 26, 2015, dramatically expands the scope of covered information.
  - Previous rule was limited to "unclassified controlled technical information"
  - Now covers a much broader scope of information:
    - Controlled technical information, critical operations security information, export control information, <u>and</u> "*Any information marked or otherwise identified in the contract that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information)*"
  - Requires covered contractors to implement SP 800-171 protections
  - Requires rapid reporting of *any* incident "that affects a covered contractor information system or the covered defense information residing therein."
- Applies to <u>all</u> DOD contractors and subcontractors, regardless of tier and regardless of contract type

Introduction to state attorney general data breach investigations

Introduction to state attorney general data breach investigations

Overview of the AG investigative process

- Data breach notification responsibility
- AG inquiry letter
- AG press releases
- Ensuring confidentiality of document productions
- Tolling agreement
- Resolution

State attorney general data breach investigations

Consumer breach notification analysis

- Varied definitions of personal information
- Notification timeframe
- Risk of harm analysis

Unfair and deceptive trade practices jurisdiction

- "Reasonable" security practices
- Deceptive policies and privacy statements

State legislative initiatives

- California: Personal information expanded to include a username or email address, in combination with a password or security question and answer that would permit access to an online account (2013)
- Florida: Requires production of forensics reports (2014)
- New York: Legislation allowing safe harbor for companies adopting heightened data security standards (2015)
- Illinois: Expanded definition of PII (2015)

Preemption: How will federal legislation impact state AG enforcement?

State Attorney General Data Breach Investigations

Important factors in regulator analysis

- Potential for consumer injury (identity theft, credit cards, etc.)
- Consumer notification timeline
- Reasonableness of security practices
- Facts surrounding breach detection (self-detected, response time, etc.)
- Cooperation with law enforcement
- Ongoing process of assessing security enhancements

Case examples: Choicepoint, TJX, TD Bank

Contacts

Todd Bertoson
Principal
Washington, DC
D +1 202 408 5395
todd.bertoson@dentons.com

Erin Sheppard
Counsel
Washington, DC
D +1 202 496 7533
erin.sheppard@dentons.com

Daniel Gibb
Senior Managing Associate
Washington, DC
D +1 202 408 3938
daniel.gibb@dentons.com

Thank you

Dentons US LLP
1301 K Street, NW
Suite 600, East Tower
Washington, DC 20005-3364
United States