Arnall Golden Gregory LLP

Attorneys at Law

How Cybersecurity Initiatives May Impact Operators

Ross A. Buntrock, Partner
ross.buntrock@agg.com
202.669.0495

Agenda

- Rise in Data Breaches
- Effects of Increase in Cybersecurity Threats
- Cybersecurity Framework
- Obama Administration's Agenda and Efforts
- Congressional Responses: Hearings and Legislation

Agenda

- Big Data: White House Report
- Cyber Threat Information Sharing: CTIIC and Executive Order
- White House Summit
- Consumer Privacy Bill of Rights Act of 2015
- Questions

U.S. Data Breaches on the Rise…

- Data breaches hit a record high in 2014
  - 783 incidents according to a recent report
  - 27 percent over the number of breaches reported in 2013
  - 18.3 percent over the previous high of 662 breaches tracked in 2010
- So far in 2015:
  - As of April 21, 2015, 256 data breaches exposing 102,374,010 records

Report by Identity Theft Resource Center (ITRC)

U.S. Data Breaches on the Rise…

- Data breaches hit a record high in 2014

As of April 21, 2015:
256 data breaches exposing 102,374,010 records

Source: Identity Theft Resource Center (ITRC)

Effect of Increasing Cybersecurity Threats

Regulatory Changes?

- The Obama Administration has announced an aggressive cybersecurity and data security agenda.

- Congress has held a number of hearings and proposed new legislation in an attempt to address the issue.

Effect of Increasing Cybersecurity Threats

Regulatory Changes?

- Some of these new privacy, data security, and cybersecurity proposals may come to bear on operators in the coming years, adding to their already substantial regulatory burden.

Obama's Administration

Cybersecurity Framework

- First announced in President's 2013 State of the Union Address
- Released on February 12, 2013
- Intended to encourage companies to adopt best practices for critical infrastructure
  - including global digital infrastructure, such as undersea communications cables that land in the U.S.

Obama's Administration

Cybersecurity Framework

Current Status:

- Remains entirely voluntary
- Lacks key incentives sought by industry stakeholders
- But…it is too soon to handicap the success of the initiative

Obama's Administration

Cybersecurity Agenda

- On January 13th, President Obama delivered remarks on cybersecurity initiatives at the Department of Homeland Security's (DHS) National Cybersecurity Communications Integration Center (NCCIC)
- Proposed cybersecurity legislation
  - incentivizing the private sector to share cyber threat information with DHS
  - providing "liability protections for companies that share information on cyber threats"

Obama's Administration

Cybersecurity Agenda

- Obama also highlighted an initiative to "update the authorities of law enforcement" to better combat cyber crime"

- Given the rise of cyber crime, including recent announcement regarding IRS hack, the item will move higher up in priority

Obama's Administration

Privacy and Data Security Efforts

- On January 20th, in the State of the Union Address, President Obama urged lawmakers to pass comprehensive cybersecurity legislation
- White House Report- Big Data: Seizing Opportunities, Preserving Values
- Executive Order - Cyber Threat Information Sharing
- Consumer Privacy Bill of Rights

Congressional Response

Hearings on Privacy and Data Security

January 21

The U.S. Senate Commerce, Science, and Transportation Committee's hearing entitled, "Protecting the Internet and Consumers Through Congressional Action"

January 27

The U.S. House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade's hearing entitled, "What Are the Elements of Sound Data Breach Legislation?"

The House Science, Space, and Technology Committee's Subcommittee on Research and Technology's hearing entitled, "The Expanding Cyber Threat"

March 18

The U.S. House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade's hearing entitled, "Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015"

Congressional Response
Cybersecurity Legislation

H.R. 1560 - *Protecting the Cyber Networks Act*

- improve cybersecurity…through enhanced sharing of information about cybersecurity threats
- permit companies to voluntarily share cyberthreat information with the government and receive protection from liability
- require companies to omit individual personal information not related to a cybersecurity threat before submitting information to the government

HR 1731 - *National Cybersecurity Protection Advancement Act of 2015*

- amend the Homeland Security Act of 2002
- enhance multi-directional sharing of information and strengthen privacy and civil liberties protections
- designate NCCIC as lead civilian "portal" for voluntary cyber threat information sharing
- require double "scrubbing" of personal information unrelated to cybersecurity risk by companies and NCCIC
- enhance voluntary information sharing

White House Report

- On February 5th, the White House published an interim report entitled, "***Big Data: Seizing Opportunities, Preserving Values***"
  - calls for utilization of big data, for law enforcement activities, among other things
  - details the impact that big data has on the economy, government, and society, as well as the privacy concerns raised in its collection

Big Data

White House Report

- concludes that individual privacy is “far from perfect” and “technology alone cannot protect privacy absent strong social norms and a responsive policy and legal framework”

Big Data

Policy Recommendations

- The Report makes policy recommendations for the President and Congress to consider, including:
  - Advancing the Consumer Privacy Bill of Rights
  - Passing national data breach legislation
  - Extending privacy protections to non-U.S. persons
  - Amending the Electronic Communications Privacy Act

Big Data
Policy Recommendations

- The Report specifically examines how big data may be used to strengthen the nation's local, state, and federal law enforcement communities.

Creation of CTIIC

- On February 10th, the White House announced the creation of the **Cyber Threat and Intelligence Integration Center (CTIIC)**
  - aims to enhance cyber threat information sharing across government agencies

Creation of CTIIC

- CTIIC will operate under the Office of the Director of National Intelligence
  - collect and analyze cyber threat information to efficiently distribute to government agencies
  - enable the government to quickly analyze and assess fast-moving cyber threats or cyberattacks
  - enable existing government cyber units to do their jobs more effectively

Cyber Threat Information Sharing

Executive Order

- On February 12th, President Obama issued an Executive Order:
  - with the goal of "promoting private sector cybersecurity information sharing"
  - discussing the importance of cybersecurity information sharing across government agencies, as well as between the government and the private sector.

Cyber Threat Information Sharing

Executive Order

- According to the Order, “[r]apid information sharing is an essential element of effective cybersecurity, because it enables U.S. companies to work together to respond to threats, rather than operating alone.”

Cyber Threat Information Sharing

Executive Order

- Framework to Enhance Information Sharing
  - Developing a common set of voluntary standards for information sharing organizations
  - Clarifying the Department of Homeland Security's authority to enter into agreements with information sharing organizations
  - Streamlining private sector companies' ability to access classified cybersecurity threat information

White House Summit

Cybersecurity and Consumer Protection

- On February 13th, President Obama delivered prepared remarks which outlined **four principles** for private entities and government agencies to consider:

  1. Share cybersecurity information with each other

  2. Recognize when the government may be able to assist or provide information related to cybersecurity

White House Summit

Cybersecurity and Consumer Protection

3. Evolve the company's or agency's cybersecurity practices

4. Focus on protecting the privacy and civil liberty of the American people

Consumer Privacy Bill of Rights Act of 2015

- On February 27th, the White House released a draft
- Requires companies to:
  - provide conspicuous notice of how they use consumer data,
  - ensure that data is being used for its intended purpose, and
  - provide consumers with a method of having their data deleted

Consumer Privacy Bill of Rights Act of 2015

- Permits industries to develop codes of conduct that would have to be approved by the Federal Trade Commission

- Empowers the FTC and state attorneys general to enforce the privacy and data security policies and practices outlined in the proposal through civil penalties

Consumer Privacy Bill of Rights

Baseline Protections for Consumers

Individual Control

Transparency

Respect for Control

Security

Access and Accuracy

Focused Collection

Accountability

Baseline Protections for Consumers

- **Individual Control**: Right to exercise control over what personal data organizations collect from them and how they use it.
- **Transparency**: Right to easily understandable information about privacy and security practices.
- **Respect for Context:** Right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.

Baseline Protections for Consumers

- **Security**: Right to secure and responsible handling of personal data.
- **Access and Accuracy**: Right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate.

Baseline Protections for Consumers

- **Focused Collection**: Right to reasonable limits on the personal data that companies collect and retain.
- **Accountability**: Right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

Recent Developments

- **Acquisition**: Telstra finalized its acquisition of Pacnet Limited last month.
  - Telstra is the largest telecommunications and media company in Australia.
  - Pacnet provides connectivity and data center services to carriers, multinational corporations and governments in the Asia-Pacific region.

Recent Developments

- **Data Breach**: Shortly have the acquisition, it was revealed that Pacnet's corporate system had been accessed by an unauthorized third party through an SQL vulnerability that enabled malicious software to be uploaded to the network and ultimately led to the theft of admin and user credentials.

Recent Developments

- Telstra immediately addressed the vulnerability and has continued to monitor the network through its incident response capabilities.
- There is no evidence that any activity extended to Telstra's networks—the Pacnet corporate IT network remains isolated.
- Pacnet customers and staff have been informed of the incident, Australian Federal Police have been notified as well.
- Currently, there is no evidence that information was stolen from Pacnet's Network.

Questions?

Arnall Golden Gregory LLP

Attorneys at Law

For more information:

Ross Buntrock

ross.buntrock@agg.com

202.669.0495

This presentation is intended to provide general information on various regulatory and legal issues. It is NOT intended to serve as legal advice or counsel on any particular situation or circumstance.