Data Breach: It Can Happen to You

TSTCI

2016 Spring
Managers' Conference

Carl R. Galant

June 9, 2016

Why Should You Care?

“I am convinced that there are only two types of companies: those that have been hacked and those that will be.”

“No company is immune, from the Fortune 500 corporation to the neighborhood ‘mom and pop’ business”

– Robert S. Mueller, Former FBI Director, March 1, 2012

“I do believe that in the future, the cyber threat will equal or even eclipse the terrorist threat.”

– Robert S. Mueller, August 8, 2013

Why Should You Care?

- Average cost of data breach in U.S. = $6.5M (up 11% from 2014)
  - $217 per record (new record high)
  - Breaches of less than 10,000 records = avg. cost of $4.7M
  - Breaches of more than 50,000 records = avg. cost of $11.9M

- Causes
  - 49% - malicious or criminal attack (also most costly)
  - 19% - negligent employees
  - 32% - system glitches that include IT and business

- Certain factors decrease costs
  - Incident response plan and team
  - Encryption
  - Employee training
  - Board-level involvement
  - Insurance protection

Source: *Ponemon Institute Research Report, 2015 Cost of Data Breach Study: United States*

Why Should You Care?

The costs are money, plus much more:

- Lost customer business
- Damage to reputation
- Investigations and forensics
- Legal services
- Audit and consulting services
- Notification costs
- Regulatory fines

Top 10 Data Most Often Stolen

- Real Names
- Birth Dates
- Social Security Numbers
- Home Addresses
- Medical Records
- Phone Numbers
- Financial Information
- Email Addresses
- Usernames and Passwords
- Insurance Policy Numbers

What are the different threats?

- Phishing
- Web App Attacks
- Point of Sale attacks
- Malware
- Denial of service
- Spamming

Why Should You Care?

- Fiduciary duty
  - Management and Board have fiduciary duty to safeguard company assets / customer data
    - Must be able to show:
      - complying with law
      - meeting industry standards

Numerous Laws at Play

- **Texas law – broad application**
- **Other states laws – if breach spans states lines**
- **Federal law – numerous proposed in Congress**
- **FCC – proposed rule on ISPs**
- **HIPAA**

Texas Law

What is a data breach?

- An incident that results in the confirmed disclosure of data to an unauthorized party.

  - Tex. Bus. & Com. Code § 521.053 – "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data."

  - Good faith acquisition of SPI by an employee for legitimate purpose is not a breach unless person uses or discloses SPI in an unauthorized manner. *Id*.

Texas Law is Very Broad

- Applies to every business that has sensitive personal information (SPI)
- If you discovery a breach, must disclose it to individual whose SPI was, or is reasonably believed to have been, acquired by an unauthorized person
  - Statute sets out when to send notice and how
  - Delay for law enforcement

Sensitive Personal Information

"Sensitive personal information" means:

(A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) social security number;

(ii) driver's license number or government-issued identification number; or

(iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(B) information that identifies an individual and relates to:

(i) the physical or mental health or condition of the individual;

(ii) the provision of health care to the individual; or

(iii) payment for the provision of health care to the individual.

Your Obligation Under Texas Law

A business shall implement and maintain *reasonable procedures*, including taking any appropriate corrective action, to protect from unlawful use or disclosure any SPI collected or maintained in the regular course of business.

REASONABLE PROCEDURES = INDUSTRY STANDARDS

Your Obligation Under Texas Law

- Evaluate and assess risks, periodically
  - Types of data you maintain
  - Electronic assets
  - How can data be accessed
- Prepare written policies and procedures
  - Explain how you ensure privacy and security
  - Physical and technical safeguards
  - Breach response plan
- Properly train employees
  - Written confirmation of training upon hire
  - Enforcement of penalties for violations
  - Periodic refresher training

Strategies for Your Policies

- **People**

  - Create hierarchy of responsibility
  - Train employees how to use, manage, and dispose of data
  - Provide regular training for employees
  - Regular and consistent messaging about privacy/security
  - Know who you'll call for help (internal and external)
    - Establish response team – small; high-level employees
    - Consider an outside team—forensic experts, privacy counsel and communications firms

Strategies for Your Policies

- **Process**

  - Know what data you are protecting and where stored
  - Understand assets: electronic devices, software, firewalls, etc.
  - Go through hypothetical breach scenarios with response team
  - Know which employees have access to which applications and learn what the reporting obligations may be in case of a breach
  - Limit collection of SPI or other personally identifiable information
  - Minimum necessary - limit disclosure to only those that need to know
  - Act immediately to remediate vulnerabilities
  - Document actions taken to evaluate risks, prepare procedures, and remedy risks or incidents

Strategies for Your Policies

- **Technology**
  - Review network logs
  - Monitor back-up servers
  - Destruction policies
  - Laptop encryption
  - Password policies: complexity, change frequency
  - Develop a remediation plan with technology enhancements
  - Use encryption, external media, USB and e-mail policies
  - Evaluate cloud and third-party technology providers' preparedness
  - Amend vendor contracts, as necessary, to require compliance with applicable data security regulations

Cyber Liability Insurance

1) Errors and Omissions

2) Media Liability

3) Network Security

4) Privacy

Cyber Liability Insurance

What's NOT Covered: key items typically NOT covered in network security/privacy liability policies:

- Reputational harm
- Loss of future revenue (e.g., if sales down due to customers staying away after data breach).
- Costs to improve internal technology systems
- Lost value of your own intellectual property

Cyber Liability Insurance

Insurers typically will require:

- An audit
- Industry standard technology
- Written policies & procedures
- Employee training

FCC Proposed Rule on ISPs

- **Privacy rules for Broadband Internet Access Service (BIAS) providers**
  - **Proposed Mar. 31, 2016**
  - **In addition to existing voice rules**
  - **Stems from 2015 Open Internet Order (applies Section 222 of Communications Act to ISPs)**
  - **FCC seeking comment on whether to “harmonize” rules with requirements for voice and cable/satellite providers**

FCC Proposed Rule on ISPs

- **Addresses customer proprietary information (PI)**

- **Customer proprietary network information (CPNI)**
  - **E.g., service plan info, geo-location, MAC addresses, IP addresses, traffic stats**

- **Personally identifiable information (PII)**
  - **Any information that is linked or linkable to an individual**
  - **30 data elements, from name to browsing history to religion**

FCC Proposed Rule on ISPs

- Requirements on ISPs
  - Must issue privacy policies that explain:
    - What PI the BIAS collects and why
    - What PI the BIAS shares
    - How can customers opt in or out of use and sharing

FCC Proposed Rule on ISPs

- Requirements on ISPs
  - Data Security
    - Adopt risk management practices
    - Institute personnel training practices
    - Adopt customer authentication requirements
    - Identify senior mgmt. responsible for security
    - Assume accountability for use and protection when shared

FCC Proposed Rule on ISPs

- Requirements on ISPs
  - Breach Notification
    - Notify affected customers no later than 10 days after discovery
    - Notify FCC no later than 7 days after discovery
    - Notify FBI and US Secret Service of breach reasonably believed to related to more than 5,000 customers no later than 7 days after discovery, and 3 days before notice to customers

FCC Case Study

- **2014 – two telecom carriers fined $10M for failing to protect personal information**
  - Subsidized telephone service to low income consumers
  - Collected SS#, driver's license, tax returns, etc.
  - Used 3d party to store; not protected; accessible on internet

- **Violation of Communications Act to:**
  - Fail to protect consumers "proprietary information" even when stored on a third party's server
  - Represent to consumers that you will take appropriate steps to protect data and not follow through
  - Fail to provide notice to all potentially affected by a breach

Video Privacy Protection Act

- **18 USC sec. 2710 - Prohibits sharing "personal information" about video viewing habits of consumers without consent**
  - **Passed 1988 - Robert Bork's video rental records appeared in papers**
  - **Evolution of online advertising and marketing creating new problems**
  - **Mobile apps and websites share technical information with third-party advertisers and marketers that uniquely ID consumer's devices**
- **Recent uptick in litigation: Plaintiffs allege violations of VPPA due to consumer interactions with media websites, audio/video players, and streaming content.**
  - **Statutory penalties for violations – attractive to plaintiffs**

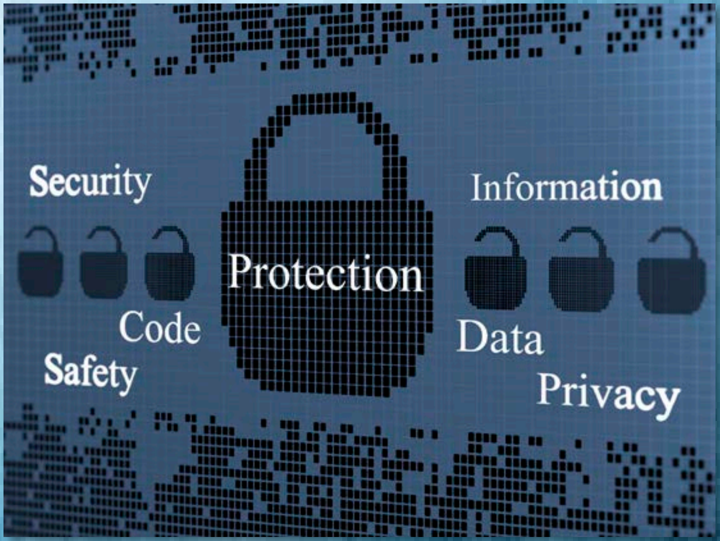
Video Privacy Protection Act

- **Unique identifiers**
  - **Shared behind the scenes**
  - **Enables third-party advertisers or marketers to personally identify end-users**
  - **They use this information to cater their marketing**
- **Examples from lawsuits:**
  - **Android ID**
  - **Device serial numbers for streaming video boxes**
  - **MAC address (hardware address for WiFi comms)**
  - **Unique IDs contained in browser cookies**

Video Privacy Protection Act

How to minimize risk:

- Identify which of your apps, websites, video/audio players, or other online services provides access to videos.
- Test video-related apps and websites to spot when unique identifiers are being shared and evaluate the nature of the unique identifier.
- Evaluate potential VPPA exposure: should certain technical things or info sharing be changed?



Contact Information

CARL R. GALANT

McGinnis Lochridge

600 Congress Avenue, Ste 2100
Austin, Texas 78701
(512) 495-6000 Main
(512) 495-6083 Direct

cgalant@mcginnislaw.com

Website: www.mcginnislaw.com