TRENDS IN CYBER LIABILITY

Presented by Chris DiIenno
Data Privacy and Network Security Group
Lewis Brisbois Bisgaard & Smith

Types of Data at Stake

Residents, constituents, employees…

- **PII – Personally Identifiable Information**
  - i.e., Social Security number, driver's license number, bank account information, credit card information, online/financial account username and password, medical information, health insurance information, and recently, email address and password in CA, FL and PR.
- **PHI – Protected Health Information**
  - Information relating to provision of healthcare, mental/physical condition, payment for provision of healthcare that identifies or can be used to identify individual
- **PCI – Payment Card Industry Information**
  - Cardholder data

What Threats?

- **Malicious attack**
  - Hackers in network, Malware and viruses, Phishing scams, Physical theft of hardware and paper
  - Rogue employees
- **Employees**
  - Negligence related to use and storage of data, failure to follow or learn policies and procedures, loss of portable devices, mis-mailing of paper, unencrypted emails to the wrong recipients
- **Vendors and Sub-contractors**
  - Any of the above can occur to a business partner with whom data is shared

Regulatory Exposures

State level breach notice: 47 states (plus Puerto Rico, Wash. D.C., Virgin Islands) require notice to customers after unauthorized access to PII/PHI.

- Require firms that conduct business in state to **notify resident consumers** of security breaches of unencrypted computerized personal information
- Many require **notification of state attorney general**, state consumer protection agencies, and credit monitoring agencies
- Notice due "without unreasonable delay"
- Some states allow private right of action for violations

Evolving Exposures

VERMONT

- Notice to affected **individuals** within **45** days of breach discovery
- Notice to VT **AG** within **14** days of breach discovery or affected individual notice (whichever is sooner)

KENTUCKY

- Became 47th state with breach notification law in April 2014

FLORIDA

- Notice to affected within **30** days
- Email address and PW = PII

MASSACHUSETTS

- "Written information security plan" for businesses storing MA resident personal information

CALIFORNIA

- Email address and PW = PII
- Amendment effective 2015 requires entity providing notice to offer appropriate identity theft prevention and mitigation services if the entity was source of breach.
- ***Strict health information protection***
  - Notice to DPH and affected individuals within 5 business days of learning of breach (amendment in effect 2015 changes this to 15 days)

South Carolina's Notice Law

- Breach: unauthorized access to and acquisition of computerized data; when there is material risk of harm to a resident.
- Personal Information is name plus: Social Security number; driver's license or state ID number; financial account number PLUS account access code/password; other numbers allowing access to financial accounts.
- Notice: written notice; without unreasonable delay; to Department of Consumer Affairs if over 1,000 affected.

Payment Card Industry (PCI)

- Payment Card Industry Security Standards Council (Visa, Mastercard, AmEx, Discover, JCB International)
- Requires merchants and service providers to abide by certain protocols to protect customers' credit card information
- Imposes "fines" and "penalties" on offending merchants and service providers (can be millions)
- Impact on standard of care – industry investigations, outside lawsuits
- Small minority of states have incorporated PCI-DSS requirements into data protection laws

Regulatory Actions

- State Level
  - Massachusetts: Women & Infants Hospital of Rhode Island (WIH) (2014)
    - WIH discovered 19 unencrypted backup tapes containing PII of 12,000 Mass. residents were missing in April 2012 after they were supposedly shipped in the summer of 2011; no notice to consumers and regulators until the fall of 2012.
    - **$150,000 settlement.**
- HHS/OCR
  - Presbyterian Hospital & Columbia University (2014)
    - ePHI accessible through internet search engines related to 6,800 individuals.
    - OCR investigation found: hospital made no effort to assure the server was secure or contained appropriate software protections; no thorough risk analysis or risk management plan; failed to implement appropriate policies or to enforce those it did have in place.
    - **$4.8 million settlement.**
- FTC
  - Wyndham Worldwide Corporation (2014)
    - Alleged repeated security failures (3 incidents over 2 years) resulting in the exposure of credit card information for over 600,000 people.
    - U.S. District Court for the District of N.J. denied Wyndham's attempts to dismiss the complaint.
    - **Court found that the FTC had authority to bring an unfairness claim in data security context.**
    - Court warned "this decision does *not* give the FTC a blank check to sustain a lawsuit against every business that has been hacked."
    - Third Circuit Court of Appeals currently considering whether FTC had this authority.

Anatomy of a Breach Response

BREACH DISCOVERY

EXPERTS
- Breach coach
- Forensics
- Public relations

INVESTIGATION—internal/forensic/criminal
- How did it happen
- When did it happen
- Is it still happening
- Who did it happen to
- What was accessed/acquired (**What wasn't**)
- Encrypted/protected

NOTICE OBLIGATIONS
- State
- Federal
- Other (i.e. PCI)

NOTICE METHODS
- Written
- Electronic
- Substitute
- Media

DEADLINES
- Can be from 48 hours to "without unreasonable delay"

INQUIRIES
- State regulators (i.e. AG, PD)
- Federal regulators (i.e. OCR)
- Federal agencies (i.e. SEC, FTC)
- Consumer reporting agencies
- Plaintiffs

LITIGATION
- Government Entities
- Class action
- Indemnification
- Subrogation

Regulator/Compliance Cost

BREACH COSTS

- Attorney oversight
- Forensics
- Notification
- Call centers
- PR
- ID Insurance
- Credit/ID monitoring
- ID restoration

PLANNING AND DATA MANAGEMENT

- Breach planning (Mass.)
- ID Theft monitoring (red flags)
- PCI DSS (Nevada and merchants)
- HIPAA
- IRPs

Litigation Trends

SINGLE PLAINTIFF

- Identity theft
- Privacy

GOVERNMENT ACTION

- Attorney General
- FTC (Wyndam)
- HHS

SUBRO/INDEMNITY

- Contractual Issues

BANKS

- Cost of replacing credit cards
- Reimbursement of fraudulent charges
- Business interruption

CLASS ACTION

- Failure to protect data
- Failure to properly notify
- Failure to mitigate
- Unjust enrichment
- Violations of consumer protection
- Statutory
- Time

Defense Eroding

Stollenwerk v. Tri West – assert **actual** identity theft

Krottner v. Starbucks Corp. – increased risk of **identity theft** constitutes an **injury-in-fact**

Anderson v. Hannaford – alleged fraud in population and **money spent** in mitigation efforts sufficient (instead of time/effort)

Resnick v. AvMed – 11th Cir. – Similar to ***Anderson*****;** also held **unjust enrichment claims viable for failure to keep promise to protect information**

In re Hannaford Bros. Data Security Breach Litigation – **does time equal money? No. But fraud plus purchase of credit monitoring may equal standing.**

ChoicePoint Data Breach Settlement – FTC paid for **"time they may have spent monitoring their credit or taking other steps in response"**

Target Class Action – Judge denies Target's motion for dismissal, holding that Banks established plausible allegation that ***failure to detect intrusion caused the financial institutions harm***

Costs

LITIGATION

- Investigation
- e-discovery
- Litigation prep
- Contractual review
- Defense (MDL?)

PLAINTIFF DEMANDS

- Fraud reimbursement
- Credit card replacement
- Credit monitoring/ repair/ insurance
- Civil fines/ penalties
- Statutory damages (CMIA)
- Time

Gaps in Traditional Insurance Products

- *Errors and Omissions (E&O)*: even a broadly worded E&O policy is still tied to "professional services" and often further tied to a requirement that there be an act of negligence
- *Commercial General Liability (CGL)*: covers only bodily and tangible property—Advertising Injury / Personal Injury (AI/PI) section has potential exclusions/limitations in the area of web advertising
- *Property*: courts have consistently held that data isn't "property"—"direct physical loss" requirement not satisfied
- *Crime*: requires intent and only covers money, securities, and tangible property
- *Kidnap and Ransom (K&R)*: no coverage without amendment for "cyber-extortion"

What Can Be Done? Before and After a Cyber Claim

Before:

- Assess
- Recognize data is at risk and have a plan in place
- Insure

After:

- First need to know you had or have a breach (internal reporting)
  - Report of lost laptop (because human error is an element in most breaches)
  - Log files show unauthorized access

  OR
  - As is the case with the vast majority of breaches it is discovered/reported by a third party

The Real After:

- Companies fall into three groups:
  - Overreact and make public statements without facts
  - Underreact and wait days/weeks to act
  - Those with a plan

Best Practices

- Identify all potentially private information
- Define internal written policies
  - Network usage
  - Social networking
  - Data handling
- Computer network sophistication and security
  - Backup, backup, backup
  - Encryption
  - Competent IT Professionals
  - Firewalls/IDS
  - Assess/Insure

Best Practices

Vendor compliance
- Non-disclosure agreements ("NDA")
- Cyber
- Certificates of Insurance (Cyber)

Employee training
- Awareness, training
- Enforcement

Incident-response planning
- First response
- Business continuity
- Disaster recovery
- Lessons learned
- Policies and procedures updated, trained, enforced

What Else Can Be Done?

PROACTIVE RISK MANAGER STEPS

- **Empowered Senior Executive**
- Talk to your IT Security folks. Gain an appreciation of the many challenges
- Not many Firms can say: how many records they have; what type of data is being collected, stored, shared, protected; where does all this data reside; when is it purged?
- **Assess** & test your own staff and operations
- Document your due care measures (training and enforcement)
- **Insurance**
- Red Flags, data security and breach response plans – affirmative duties
- Service level agreements
- Repeat

Thank You!