Emerging cyber risks

September 17th, 2015
1. Introductions
2. Exposure Overview & Current Trends
3. Insurance Landscape
4. Claims & Coverage Issues
5. Future of Cyber Liability
6. Q & A
INTRODUCTIONS

Section one
INTRODUCTIONS

• Moderator:
  • Robert Barberi, Vice President, Willis Cyber Security & Privacy

Panelists:
• Andy Obuchowski, Jr., Practice Leader, McGladrey Security & Privacy
• Cynthia Larose, Member, Mintz, Levin, Cohn, Ferris, Glovsky & Popeo
• Stephen Pannucci, Vice President, Zurich North America
EXPOSURE OVERVIEW & CURRENT TRENDS

Section two
Data and privacy violations are on the rise

- In 2014, there were more than 1,868 significant privacy breaches reported in the US – roughly 5 per day. Preventable breaches (unencrypted devices) continue to decrease, while breaches involving hackers/organized crime and rogue employees continue to increase. As a result, claims severity has spiked dramatically. Especially in the retail and managed care sectors.
  - 761 unique cyber breaches led to theft or compromise of 83,176,279 individual records. Health care providers, service providers and retailers accounted for most of the breaches

Eleven of the top 15 largest breaches of all time occurred in 2014

- Neiman Marcus; PF Changs; Community Health Systems; UPS; Home Depot; Jimmy John’s; PF Changs; Sony; Staples; JP Morgan Chase; New York; Michaels
- Other Large Breaches: Anthem; Premera; CareFirst; Target
## Regulatory Landscape

| Applies to: | A health plan, health care clearinghouse and health care provider who transmits any health information in electronic form in connection with a covered transaction. |
| Who Must Be Notified: | The patient or their personal representative, the Department of Health and Human Services Office for Civil Rights (HHS) and the media if more than 500 residents of a state or jurisdiction are affected. |
| Notification Timeframe: | Without unreasonable delay and in no case later than sixty (60) calendar days after the breach is discovered. |
| Preemption: | Preempts state law to the extent it is more strict |

## HIPAA Privacy Regulations - Covered Entity

- **Applies to:**
  - A health plan, health care clearinghouse and health care provider who transmits any health information in electronic form in connection with a covered transaction.

- **Who Must Be Notified:**
  - The patient or their personal representative, the Department of Health and Human Services Office for Civil Rights (HHS) and the media if more than 500 residents of a state or jurisdiction are affected.

- **Notification Timeframe:**
  - Without unreasonable delay and in no case later than sixty (60) calendar days after the breach is discovered.

- **Preemption:**
  - Preempts state law to the extent it is more strict

## What do Regulators Expect?

- **Transparency**
- **Prompt and thorough investigation**
- **Good attitude and cooperation**
  - Commitment to compliance and safeguarding PII
- **Appropriate and prompt notification**
- **Corrective action**
  - Know the root cause and address it
  - Staff training
  - Awareness program
  - Technical safeguards
  - New policies/procedures/physical safeguards
- **Remediation and mitigation**
<table>
<thead>
<tr>
<th>State</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vermont</td>
<td>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).</td>
</tr>
<tr>
<td>Kentucky</td>
<td>Became 47th state with breach notification law in April 2014.</td>
</tr>
<tr>
<td>Florida</td>
<td>Notice to affected within 30 days. Email address and PW = PII.</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>“Written information security plan” for businesses storing MA resident personal information.</td>
</tr>
<tr>
<td>New Jersey</td>
<td>Username/email address and PW = PII (pending). Encryption requirements for Health Insures (effective August 1, 2015).</td>
</tr>
<tr>
<td>Indiana</td>
<td>Notice “without unreasonable delay” interpreted by AG as 30 days. Enforcement action (assurance of voluntary compliance).</td>
</tr>
<tr>
<td>California</td>
<td>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 15 business days of learning of breach if entity licensed by CDPH.</td>
</tr>
<tr>
<td>Connecticut</td>
<td>AG practice of requesting 2 years of credit monitoring following SSN exposure, though not in statute.</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>AG requests notice if incident affects PA residents, though no statutory requirement.</td>
</tr>
<tr>
<td>Nevada</td>
<td>Driver authorization card numbers = PII. User names, unique identifiers, email addresses in combination with passwords, access codes or security questions = PII.</td>
</tr>
</tbody>
</table>
SOURCES OF A DATA BREACH

- Growing incentive for insiders to abuse access to sensitive data for financial gain
- Disgruntled current and former employees exploit back-doors
- Theft of Intellectual Property
- Security compromise – loss of sensitive client data
- Infrastructure downtime may lead to Dependent Business Interruption claim

- Intent is to disrupt and/or embarrass a target
- Motivations are fickle and unpredictable
- Massive DDoS attack

- Access controls and behavior monitoring insufficient to detect insider threats
- Users who fail to embrace “culture of security” will find ways to circumvent ‘inconvenient’ security controls
- Patience is a virtue. Tactics have evolved from “hit and run” to “infiltrate and stay.”
- Industrialization - Black markets exist for all types of personal information
- Proliferation of mobile platforms and BYOD policies creates new vectors
Most incidents emanate from outside the organization;
• The human employee element continues to be the area where a large part of unforeseen data breaches whether they are malicious, accidental or completely unknown;
• The last vector most likely refers to third parties;
• Trend of hacking for fun is over, breaches are a business and perpetrators are treating it as such;
• Significant gap between how long it takes an attacker to compromise a system versus how long it takes a company to discover the compromise;
• The divide & cost realities between the defenders versus the perpetrators.

Source: Risk Based Analytics

Source: Verizon
THE STATISTICS: IDENTIFYING & CONTAINING A BREACH

Mean Time to Identify and Contain a Data Breach (in days)

MTTI: “Mean Time to Identify”
MTTC: “Mean Time to Contain”

Relationship Between Mean Time to Identify with Total Average Cost

Source: Ponemon Institute
What data is collected/ stored/ transacted?

- Personally Identifiable Info. (PII)/Protected Health Info. (PHI)
- Credit Card Numbers
- Confidential 3rd party information
- Merger/Acquisition target/plans
- Financial Account Information

Where is it?

- Vendor Access/Capabilities/Storage/Process/ Mobile Devices (Applications) / Portable Devices (i.e. thumb drives)

Dependent Businesses

- What information can be accessed via or by dependent business partners?

How well is it protected? / How long is it kept?

What is a breach?

- Unauthorized disclosure / Unauthorized acquisition
- Data compromised

Describe any privacy/breach related contractual stipulations?
INSURANCE LANDSCAPE

Section three
A range of limit, retention and privacy breach response cost sub-limit options are available. All options have certain trade offs, which must be identified and weighed:

- **Third Party only**
- **First and Third Party**
- **Costs coverage options**
  - Full limits
  - Per Person Coverage
  - Notification coverage inside or outside the Policy Aggregate Limit
  - Quota Share

When considering the types of coverage that is appropriate, the organization should consider the following:

- **Internet & Network Business Interruption.** What is the impact of an interruption on the organizations network or web-site service? What percentage of sales/customer offerings are being offered online or are network dependent?

- **Loss of Data through an IT security Event or Theft.** What is the value of your data or programs? What would the expense of recovering your data cost your operations? What customer lists, customer preference information, supplier information, pricing information and other vital competitive information may be at risk for theft by a thief or hacker?

- **Liability for loss or disclosure of confidential information.** What confidential information does the organization hold and what is the potential loss if a class action were to be commenced? What would be the cost of notifying and providing credit monitoring for those customers? What are the costs of defending an investigation by regulators and how much might fines be if they are imposed?

- **Liability of loss as a result of the acts of a third-party.** What activities are third party vendors doing on your behalf? What important commercial or confidential data do they hold and what would be the loss or liability if it were to be corrupted or released?

- **Media Exposure.** What is your exposure to potential trademark infringement from domain name, slogan or advertising message, product names, etc.; copyright violations for content on websites, brochures or elsewhere; accusations of false advertising and unfair competition; infringement of trade secrets
TRADITIONAL INSURANCE GAPS

Most traditional insurance policies have gaps in the coverage relative to these risks

- **Property:** Usually requires physical damage to a tangible asset to trigger coverage. Data is not considered tangible property in most policies. Also, computer viruses and hacker attacks seldom damage your systems “physically.” Also, most property policies include computer virus exclusions, or provide for small sub-limits of network business interruption coverage.

- **General Liability:** Physical damage or bodily injury trigger is not activated in a network security breach. Advertising Injury and Personal Injury coverage can be difficult to trigger as a result of intentional and/or criminal acts, like breach of confidential data due to a hacker or computer virus. Also, Property Damage definition advises that “Tangible property does not include data.”

- **Commercial Crime:** Covers theft of money and securities, but does not cover the theft of data, information, and account numbers (including credit card data) and may also require intent.

- **Professional Liability/ E&O:** Intentional acts are usually excluded. Often, an event such as a security breach can not only harm your client, but also your client’s customers. Most E&O policies do not respond to these types of security breach/disclosure of sensitive data events. Some healthcare E&O policies may provide coverage for breach of protected health information, but may not extend to financial and employee information.
What’s best addressed elsewhere. Certain exposures are best addressed, transferred and evaluated in other insurance policies and as a result are typically excluded from cyber/privacy policies they include:

• Bodily Injury/Property Damage- Best addressed under a Commercial General Liability Policy;
• Act of God, Pollution – Best addressed under a Traditional Property and/or Environmental Policy;
• SEC- Best addressed under a Directors & Officers policy;
• EPLI- Best addressed under an Employment Practices Liability Policy;
• Theft of the value of money and securities – Best addressed under a crime or fidelity Policy;

Your Business Risks- the costs of doing business:

• Contractual Liability Exclusions- If you decide not to do something. Just because, that is not necessarily insurable;
• Collection Exclusions- Your collect information of others without letting them know and use it for other means;
• Patent – Are always completely excluded;
• Known Prior Acts- Not designed to insure a burning building;

Knowingly Dishonest Acts:

• The policy will exclude and make severable the acts of bad actors from the entity. Ensuring that the entity is protected against the bad acts of rogue employees
Underwriting exposure analysis driven by PII/PHI records, security controls and revenue

<table>
<thead>
<tr>
<th>Organizational Risk Culture</th>
<th>Access to Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>n  How does the organization encourage, and cascade, tone from the top in relation to information security?</td>
<td>n  How do you set and monitor access controls?</td>
</tr>
<tr>
<td>n  Enforcement of information security policies</td>
<td>n  Does the organization offer two factor authentication?</td>
</tr>
<tr>
<td>n  Privacy and security budget</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Security Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>n  Are you “compromise ready” (i.e., incident response plan)?</td>
</tr>
<tr>
<td>n  Does the organization have a Chief Security Officer?</td>
</tr>
<tr>
<td>n  Does the organization have a Chief Information Officer?</td>
</tr>
<tr>
<td>n  Does the organization have an information security response Team?</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Databases</th>
</tr>
</thead>
<tbody>
<tr>
<td>n  Encryption of personal and confidential information stored on databases</td>
</tr>
<tr>
<td>n  Key retention policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>n  Unencrypted or encrypted</td>
</tr>
<tr>
<td>n  Limit access of personal devices to critical systems</td>
</tr>
<tr>
<td>n  Mobile technology policy implementation/assessment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employee Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>n  Training on policies and procedures</td>
</tr>
<tr>
<td>n  Phishing training seminars</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vendor Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>n  Undertaking vendor due diligence and contract analysis</td>
</tr>
</tbody>
</table>
In 2014, there were more than 1,868 significant privacy breaches reported in the US – roughly 5 per day. Preventable breaches (unencrypted devices) continue to decrease, while breaches involving hackers/organized crime and rogue employees continue to increase. As a result, claims severity has spiked dramatically. Especially in the retail and managed care sectors with the examples of Target, Neiman Marcus, P.F. Changs, Goodwill Industries, Michael Stores, Living Social, Staples, SuperValu, Home Depot, Anthem and Premera.

Consequently, the markets have tightened their underwriting standards, pricing and retention guidelines (including separate class action retentions).

Many clients in the retail or managed care industries have experienced extremely challenging renewals. Some of our largest clients have struggled to obtain the excess capacity necessary to complete their existing limit structure. In some instances, the pricing on the higher excess layers exceeded the pricing on the lower excess layers, as they struggled to find markets to participate on the program.
CLAIMS ISSUES & COVERAGE CONSIDERATIONS

Section four
CLAIMS MANAGEMENT

Professional Liability Underwriting Society

Transition
- Detailed timeline for transition managed by Transition Officer
- Bespoke approach for handling of legacy claims
- Identification of barriers to coverage in order to develop new strategy for resolution

Policy Negotiation

Process Review and Training
- Review reporting structures, policies and procedures and provide feedback and guidance
- Create and implement mock claims analysis to demonstrate
- Provide on-site multidisciplinary coverage seminar to enhance our client’s knowledge of claims management process and how policies respond

Claims Notified

Ongoing Claims Process
- Proactive management of claims process
- Initiation and leadership of interaction between Insurers, lawyers and advisers
- Progress reports
- Negotiation with Insurers
- Ensure compliance with all policy obligations

Claims Management

Coverage Dispute

Claims Processing
- Preparation of relevant documentation
- Efficient claims handling
- Funds handling
- Recoveries

Pre-Claim Policy Construction
- In-depth policy review and drafting
- Ensure excess policies follow form on all material issues
- Focus on issues that impact efficient claims handling (Arbitration/Choice of Counsel/Notice/Definition of Claim)
- Minimize client obligations (claims/M&A)
- Provide current market and legal trends and their potential implications

Loss Reporting and Management
- Ensuring compliant claim notification
- Consent to counsel
- Consistent and frequent dialogue with our client’s lawyers and advisers
- Review of reports and opinions
- Expert coverage advice
- File handling
- Bordereau monitoring

Claims Championship
- Willis’ leverage
- Negotiation with insurers
- Creative solutions to claim disputes

Claims Resolution
Examples

- Breaches or disruptions in the cloud
- Acts of rogue employees
- Portable devices and encryption exclusions
- Credit Monitoring
- Terrorism
- Limited 1st Party Coverage
Section five

FUTURE OF CYBER LIABILITY
• 7th Circuit Reinstate Neiman Marcus Consumer Data Breach Class Action (July 22nd, 2015)

• Target Settles Visa Card Issuer Claims for $67M (August 18th, 2015)

• Target Settles Class Action Lawsuit brought Customers for $10M (March 19th, 2015)

• Byrne v. Avery Center for Obstetrics & Gynecology, P.C. (November, 11th, 2014)

• Walgreen Co v. Hinchy (November 14th, 2014)
Columbia Casualty Company v. Cottage Health System.

• Columbia Casualty (CNA), seeks to avoid coverage under a cyber insurance policy for the defense and settlement of a data breach class action lawsuit.

• Arises out of a data breach incident that resulted in the release of private electronic healthcare patient information stored on network servers owned, maintained, or used by the insured, Cottage Health System (Cottage). 32,000 patients impacted.

• The lawsuit sought damages for alleged violation of California’s Confidentiality of Medical Information Act.

• Settled in April 2015 for $4.125 million. Cottage’s cyber insurer, CNA, funded the settlement pursuant to a reservation of rights.

• CNA filed coverage litigation based on exclusions for “Failure to follow minimum required practices” and “material misrepresentations in the application” related to the insured’s cyber security program.

Takeaways:

• Review exclusionary language in both the policy and application carefully. Limit scope and negotiate severability language if possible.