RYAN[SM] TURNER SPECIALTY

Discussion on Network Security & Privacy Liability Exposures and Insurance

Presented By: Kevin Violette – Errors & Omissions Senior Broker,
R.T. Specialty, LLC

February, 25 2014
HFMA Washington-Alaska Chapter Annual Conference & Trade Fair

RYAN SM TURNER SPECIALTY

Irrefutable Laws of Information Security

1) Information wants to be free

- People want to talk, post, and share

2) Code wants to be wrong

- We will never have 100% error free software

3) Services want to be on

- Some background processes will need to be on

4) Users want to click

- If they are connected to the internet, people will click on things

5) Even a security feature can be used for harm

- Laws 2, 3, 4 even apply to security capabilities

Compromise is inevitable under any compute model. Managing the risk and surviving is the key

*Presented by the CIO at Intel – Malcom Harkins. Credit also to Phil Venables 2008, adapted from Scott Culp 2000, Pete Lindstrom 2008, and other sources

RYAN SM TURNER SPECIALTY

HHS/OCR Regulatory Fines

- Massachusetts Eye and Ear Infirmary (Sept. 2012): Entered into settlement with OCR that included a **$1.5 million** penalty after an OCR investigation into the 2010 theft of an **unencrypted laptop**.

- Hospice of Northern Idaho (December 2012): HONI agrees to pay $50K settlement for patient data breach. **This is the first settlement that involved fewer than 500 individuals**.

- WellPoint (July 2013): Entered into settlement to pay HHS $1.7 million for leaving customer information accessible over Internet. **No malicious intent.**

RYAN SM TURNER SPECIALTY

Recent Healthcare Breaches

- Horizon BCBS-New Jersey: Reported a breach in November involving two unencrypted desktop computers, potentially affecting 840,000 individuals.
- Stanford: Notified nearly 20,000 patients that their protected health information had been wrongfully posted to a student website, which resulted in a class action lawsuit filed for $20 million.
- AvMed: Agreed to pay $3 million in a data breach settlement. What sets this apart from other data breach settlements is Plaintiffs who have not suffered identity theft as a result of the breach may nevertheless collect from the Settlement Fund.
- Sutter Health: 4.24 million Sutter Health patients had their protected health information compromised after the theft of an unencrypted company desktop computer, making the breach one of the biggest HIPAA breaches in the United States. In its aftermath, Sutter Health is still facing up to $4.25 billion in class action lawsuits.

RYAN SM TURNER SPECIALTY

Recent Healthcare Breaches (con't)

- **Utah Department of Health (March 2012): [April 2013 Update]** Approximately 780,000 Medicaid patients and recipients of the Children's Health Insurance Plan in Utah had personal information stolen after a hacker from Eastern Europe accessed the Utah Department of Technology Service's server. The main risk for consumers stemmed from the ~280,000 Social Security numbers that were exposed. As of April 2013, the state has spent ~$9M on security audits, upgrades and credit monitoring for victims. A breakdown of some cost components:
  - • $467,000 to hire an ombudsman, staff a hotline, run ads and hold community meetings to notify victims.
  - • $1.9 million to provide two years of credit monitoring for those whose Social Security numbers were compromised.
  - • $741,000 on a legal consultant and forensic security audit.
  - • $300,000 to create an Office of Health Information and Data Security.

RYAN SM TURNER SPECIALTY

Final HIPAA/HITECH Rule – Business Associates

- Expands who is considered a business associate to subcontractors of business associates.
- Requires business associates to be in compliance with certain requirements of the HIPAA Privacy & Security Rules.
- Imposes direct liability on business associates for violations of the rule.

RYAN SM TURNER SPECIALTY

Final HIPAA/HITECH Rule – Breach Notification

- Modifies the Breach Notification rules to limit the discretion of regulated entities to decide whether or not a Breach must be reported.
- Removed the exception which stated that dates of birth and zip codes don't apply.
- **The risk of harm standard has be replaced by a four-factor analysis.**

RYAN℠ TURNER SPECIALTY

New Four-Factor Analysis

The organization must determine whether there is a low probability that information has been compromised using the following four factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

RYAN SM TURNER SPECIALTY

Confidentiality of Medical Information Act

The primary purpose of the CMIA is to protect an individual's health information, in either electronic or paper format, from unauthorized disclosures to third parties.

- Statutory damages of $1,000 per affected patient (without proof of actual damages) may apply, in addition to compensatory and punitive damages and attorney fees.

- Can apply in cases where it can be shown that the information has been viewed by a 3rd party without patient authorization.

RYAN SM TURNER SPECIALTY

Privacy Insurance Coverage Structure

Privacy/Security Liability

First Party	First Party	Third Party	Third Party
Other Business Costs	**Breach Notice Costs**	**Civil lawsuits**	**Regulatory Actions**
• Business interruption • Data repair /replacement • Cyber-extortion	• Notification/credit monitoring costs ($ or person sub-limits) • Crisis management/PR • Forensic Investigation	• Consumer class action • Corporate or financial institution suits • Credit card brands	• State AG investigations • FTC investigations • Health & Human Services • Foreign Privacy Entities

RYAN SM TURNER SPECIALTY

Insurable Losses/Costs

First Party Expense Costs (typically sub-limited, sometimes outside of the limit):

- Data Forensics Expenses
- Customer Notification Expenses
- Crisis Management Expenses
- Credit/Identity Monitoring Expenses
- Cyber extortion ransom payments and expenses
- E-Business Interruption due to network security event
- PCI Fines

Third Party Liability

- Defense costs and settlements for breaches of privacy and network security
- Regulatory Defense and Penalties

RYAN SM TURNER SPECIALTY

Two Approaches to Breach Response

Monetary sublimit approach:

- Dedicated sublimit for responding to breaches (sometimes outside of the limit)
- Carriers have preapproved vendors, but allow flexibility in choosing vendors
- Better for Insureds that have existing vendor relationships or more sophisticated in house privacy departments

Number of persons approach:

- Breach response coverage provided for a given number of affected individuals (not tied to the limit of liability)
- Insured must use vendors approved by the carrier
- Better for smaller Insureds that do not have existing vendor relationships, and want a streamlined approach to breach management.

RYAN SM TURNER SPECIALTY

What are the Key Coverage Considerations?

- Coverage for:
  - Breaches by rogue employees
  - Breaches by 3rd party vendors
  - Loss of corporate confidential information
  - Loss of data electronically and through written means
  - Breach response/mitigation services
  - Regulatory fines and penalties (not just defense)
  - Wrongful collection of data

RYAN SM TURNER SPECIALTY

How much limit should we buy?

- Exposure is tied directly to the number of individuals you have information on
- Types of protected information stored
- Location and segregation of sensitive data
- Industry specific considerations
- How much do my peers buy?

RYAN SM TURNER SPECIALTY

Choosing a Privacy Insurance Carrier

- Financial stability
- Coverage terms and conditions
- Appetite for clients in your industry
- Appetite for the size of your client's business
- Commitment to the product
- Claims paying reputation and infrastructure
- Industry expertise
- Relationships with expertise – attorneys, security firms, forensic specialists

RYAN SM TURNER SPECIALTY

Managing Privacy Risks

Contracts – Cloud providers and Data Holders

- Review Vendor Agreements – Insurance Requirements, Indemnify
- Limitations of Liability / Indemnifications

Privacy controls/procedures

- Access to electronic information only as needed for employees
- Information is encrypted whenever possible
- Review of physical security procedures used at various locations
- Privacy policy in place, monitored for compliance, updated
- Sharing of customer information with any 3rd parties
- International privacy rules for data transfers

Claims, legal matters, and insurance

- Broker Interaction – Let us help with the process
- Provide leverage and discussion about coverage intent with carrier - Use previous experience
- Work with coverage and outside counsel as necessary

RYAN SM TURNER SPECIALTY

Important Privacy Issues

- Assess what information is being collected - Think through the types of data you are collecting
- Determine what laws apply to your company based upon the information it collects, where it does business and the identity of its customers
- Reserve the right to modify your privacy policy
- Assess whether you have a responsibility to report a data security incident
- Consider what security systems you have in place and what security measures you are requiring third parties to have
- Determine if you are sending or receiving data to countries that have higher privacy and security standards
- Consider restrictions upon the use of removable media
- Make sure your privacy policy makes the necessary disclosures

RYAN SM TURNER SPECIALTY

How to prepare for a Privacy Event

- Know what types of data are stored and where
- Develop an ongoing plan to assess / monitor / evaluate privacy risk
- Create an ongoing compliance, education, and mitigation plan
- Develop a response plan for when a data event occurs (it will)

- Typical components of a response plan for a data breach:
  - Determine scope of breach
  - Internal remediation – Forensic expertise/repair, vendors involved?)
  - External party notifications (banks, credit bureaus, police, FBI)
  - Affected consumer disclosure (state requirements, timing, scope)
  - Do we own or license the data? (response requirements are different)
  - Notification (message, medium)
  - External remediation (credit monitoring)

RYAN[SM] TURNER SPECIALTY

RT ProExec

Setting new expectations.

for more information, please visit
www.rtspecialty.com