Cyber/Information Security Insurance

Pros / Cons and Facts to Consider
Presenters

Calvin Rhodes, Georgia Chief Information Officer
Ron Baldwin, Montana Chief Information Officer
Ted Kobus, Partner - BakerHostetler
Steve Emanuel, New Jersey Chief Information Officer (Facilitator)
Background

– Most Organizations realize Data Breach is not a matter “IF” but “WHEN”

– Questions on the Minds of Most CIO’s
  • Am I / How well are we Prepared?
  • Do I know WHAT to Do?
  • What are my Options?
Getting Prepared

– Do I Want to Pursue Cyber Insurance and if so, How Much?
– What Type of Coverage can be Provided?
– What are the Triggers for a Policy
– What is Excluded from Coverage
Getting Prepared

– What types / how much Data is Covered
– What Other Costs and Services are Covered
– What Do I need to Know to Make the Choice - “Do I” or “Don’t I”
Recent Cyber Statistics

Main Reasons for Not Buying

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premiums are too expensive</td>
<td>52%</td>
</tr>
<tr>
<td>Too many exclusions, restrictions and uninsurable risks</td>
<td>44%</td>
</tr>
<tr>
<td>Property and casualty policies are sufficient</td>
<td>38%</td>
</tr>
<tr>
<td>Unable to get insurance underwritten because of current risk profile</td>
<td>26%</td>
</tr>
<tr>
<td>Coverage is inadequate based on our exposure</td>
<td>26%</td>
</tr>
<tr>
<td>Risk does not warrant insurance</td>
<td>9%</td>
</tr>
<tr>
<td>Executive management does not see the value of this insurance</td>
<td>5%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
</tr>
</tbody>
</table>

Customer Satisfaction Recommendations

<table>
<thead>
<tr>
<th>Rating Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3%</td>
</tr>
<tr>
<td>1 to 2</td>
<td>6%</td>
</tr>
<tr>
<td>3 to 4</td>
<td>11%</td>
</tr>
<tr>
<td>5 to 6</td>
<td>13%</td>
</tr>
<tr>
<td>7 to 8</td>
<td>23%</td>
</tr>
<tr>
<td>9 to 10</td>
<td>44%</td>
</tr>
</tbody>
</table>

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC
Publication Date: August 2013
State of Georgia
Cyber Insurance: An Overview

Calvin Rhodes, Chief Information Officer
Cyber Insurance by Definition

Protection against losses related to information security breaches, such as data theft/loss, business interruption caused by a computer malfunction or virus, and fines or lost income because of system downtime and/or network intrusion.
Investigating Cyber Insurance

- Risk Management is the responsibility of our Department of Administrative Services
- State CIO participating on review process to insure at the enterprise level
- Georgia Board of Regents has already insured the university system
A Broadening Frontier

- Growing interest fueled by high-profile cyber events
  - 24% of companies have already purchased cyber insurance
  - 33% plan to buy within next 12 months
  - 17% are exploring cyber insurance

Source: Gartner, 2015
A Nascent, Immature Market

– Little actuarial data
  • Risks are hard to quantify
– No standard policies
  • Underwriting is case-by-case
– Federated models
  • Not well understood by carriers
– Cloud coverage murky
  • Carriers reluctant, fear large-scale events
– Contract Agreements
  • Still main avenue for mitigation for companies
Help When You Need It

– Policies offer one-stop access to core services:
  • Customer notification
  • Credit monitoring
  • Crisis communication
  • Forensic investigation
  • Data restoration
  • Potential cyber extortion
  • Related third-party liability
No Substitute for Security

– Cyber insurance does not cover all information security risks
– Weak security may make coverage too expensive or impossible to obtain
– Coverage could be disincentive to strengthening security if considered a safety net
Read the Fine Print

- Carrier’s underwriting relies on information provided by potential insured
  - Must accurately represent security posture
- Post-event audits
  - Clauses may limit/void policy if discrepancies identified
- Slow Payouts
  - Anecdotal reports suggest a lengthy process
Challenges for States

– Limited data about public sector use
– Federated models
  • Underwriting complicated by incongruent security postures and exposures across agencies
– Varying statutes
  • 47 states have breach laws
  • Georgia requires higher standard of response for breaches of less than 50K records than for larger ones
Challenges for States

- Role of sovereign immunity
- Premiums, deductibles may be cost-prohibitive
- Self insurance by states
State of Montana
Cyber/Information Security Insurance

Ron Baldwin, Chief Information Officer
Montana’s Overview

- Data Breach vs. Cyber Incident
- Montana Cyber/Information Security Insurance
- Cyber Incident Response Process
- DPHHS Incident
What is a Data Breach?

• “Data breach” is a term of art and the precise definition depends on the applicable state and federal law(s).

• Data breach notification laws exist in 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands. Trigger is based on individual’s state of residence.

• Federal sector-specific laws (e.g., HIPAA/HITECH for healthcare and FERPA for student records) may also present separate breach reporting obligations, and apply to types of personal information not explicitly covered by the Montana statute.

• In Montana, a “breach” is the unauthorized acquisition of personal information that is reasonably believed to have caused loss or injury.
Personal Information Under Montana Law

First name or first initial and last name of an individual in combination with any one or more of the following data elements when the name and the data elements are not encrypted:

- Social security number or tax identification number;
- Driver’s license number, state identification number or similar identification number issued by an state, district or territory;
- An account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a person’s financial account.

Personal information does not include public information lawfully made available from federal, state, local, or tribal government records.
When an “Incident” Becomes a Data Breach in Montana

• Under Montana law, “data breach” means the:

  ➢ Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by a state agency or by a third party on behalf of a state agency and causes or is reasonably believed to cause loss or injury to a person. Mont. Code Anno., § 2-6-501(1).

  ➢ Risk of Harm reporting threshold: What “materially compromises the security, confidentiality, or integrity of personal information” is open to interpretation. AG guidance in other states.
Montana’s Cyber/Information Security Insurance

- Montana participates in a national cyber/information security insurance program underwritten by Certain Underwriters at Lloyd’s, Syndicators 623 and 2623 (“Beazley”).
- $2,000,000 Policy Aggregate Limit for Privacy Notification Costs (subject to a $100,000 per incident Retention); $1,000,000 Policy Aggregate Limit for Beazley Nominated Service Providers.
- Insurance doesn’t cover everything. $100,000 deductible, 10% state co-insurance for credit monitoring.
- Coverage is nice, but breach prevention should be the collective focus.
Montana’s Cyber/Information Security Insurance

The state’s commercial insurance policy provides coverage for:

• Data breach response costs including, but not limited to, forensic investigations, mail notification, and credit monitoring (one year).
• Fines/penalties assessed by regulatory authorities.
• Revenue streams lost as a result of a breach.
• Personal injuries and property damage for negligent acts or omissions of the state.
• Website content and media.
• Cyber ransoms and fines.
• Public relations firm consultation
Cyber Incident Response Process
Step One: Notify Response Team

• Use the term “incident” instead of “breach” as a point of reference in all communications.
• Notify your agency’s internal incident response team (i.e. agency head, IT manager, risk manager, attorney, etc.).
• Notify the cyber insurance brokerage firm and cyber insurance carrier.
• Follow the instructions found at the Risk Management & Tort Defense Division’s (RMTD) website at http://rmtd.mt.gov/claims/agenciesreportclaims.mcpx
  ➢ Call us within 24 hours at (406) 444-2421
  ➢ Have the immediate supervisor complete the “Report of Incident” and send it to us within two days.
  ➢ Do not contact individuals whose information may have been released. Do not contact law enforcement or regulatory authorities (that will be done by the insurance carrier attorneys).
Cyber Incident Response Process

Step Two: Escalate as Necessary

• Internal investigation and reporting of incident to the State’s cyber liability insurance carrier;
• Privacy counsel (attorney-client privilege and work product protections);
• Computer forensics expert;
• Public relations and crisis management consultant;
• Mailing/notification vendor (is your agency equipped to print and mail 5,000 notification letters? How about 50,000? 500,000?);
• **Timing is everything:** Notification (to the affected individuals) must be made **without unreasonable delay**, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. Mont. Code Anno., § 2-6-504(1)(b)
• Fixed deadlines in other states
DPHHS 2014 Cyber Incident Timeline

- May 15<sup>th</sup> - Initial discovery
- May 22<sup>nd</sup> - Forensic confirmation
- May 29<sup>th</sup> - Initial public communication
- June 23<sup>rd</sup> - File sent to mail processing center (1.3M)
- June 24<sup>th</sup> - Follow-up public communication
- July 3<sup>rd</sup> - Began mailing - 200K notices/day
On complex security issues, the key timeframe of notification is the 60-day HIPPA requirement, which begins with initial discovery.

- Performed scope analysis of incident
- Created notification list
- Documented potential HIPAA exposure for Office of Civil Rights
Regrettably, a DPHHS server was hacked. We apologize that this happened and want to provide you with more information and the steps we are taking to protect our clients and staff who had information on the affected server.

What happened? On May 22, 2014, outside forensic experts confirmed that hackers gained entry to a Department of Public Health and Human Services (DPHHS) computer server, though there is no evidence that information on the server was used inappropriately or even accessed. DPHHS took immediate action on May 15 when it first detected suspicious activity by shutting down the server, contacting law enforcement and bringing in outside experts to help investigate. Based on our investigation, we believe the hackers first gained entry in July of 2013. The information on the server may have included names, addresses, dates of birth, Social Security numbers and limited clinical information. This incident should not impact MT DPHHS services as none of the information contained on the server was lost and we have a complete back-up of the information.

When did it happen? On May 22, 2014 outside forensic experts confirmed that a DPHHS server had been hacked. DPHHS took immediate action on May 15 when it first detected suspicious activity by shutting down the server, contacting law enforcement and bringing in outside experts to help investigate.
DPHHS Message to Public/Press (cont.)

• **How did this happen?** Unknown computer hackers used malware to gain entry to a DPHHS server containing client and agency employee personal information.

• **Have those affected clients been notified?** At this time, DPHHS is in the process of notifying all those people with information on the server.

• **What type of security is in place on the server?** We are continuously working to improve security of our computer networks and are committed to protecting client information. We deeply regret any inconvenience to you as a result of this incident. To help prevent something like this from happening in the future, we have taken the affected server offline and a new server containing backup files is being scanned and safely brought online. DPHHS has purchased additional security software to better protect sensitive information on existing servers, and as part of an internal investigation, DPHHS is reviewing existing policies and procedures to determine how to prevent this from happening again in the future.

• **Will this affect the services I receive?** This incident should not impact DPHHS services as none of the information contained on the server was lost and we have a complete back-up of the information.
BakerHostetler
Cyber/Information Security
Insurance - Provider Perspective

Ted Kobus, Partner
A Simplified View of a Data Breach

Discovery of a Data Breach
- Theft, loss, or Unauthorized Disclosure of PHI, PII, PCI

Evaluation of the Data Breach
- Forensics and Legal Review

Managing the Short-Term Crisis
- Notification and Credit Monitoring
- Public Relations

Handling the Long-Term Consequences
- Class-Action Lawsuits
- Reg. Fines, Penalties, and Consumer Redress
- Reputational Damage
- Income Loss
What Will You Encounter?

- Forensic investigation
- Operational challenges
- Breach notification law analysis
- Decisions on public statements
- Media and client inquiries
- Regulatory inquiries
What Will You Encounter?

- Law enforcement
- Class actions
- System remediation and revalidation
- Reporting of impact
- Regaining public trust
What Will Forensic Firms Ask You

1. How did you detect the intrusion?
2. Do you have a WISP or breach response plan?
3. Describe the data that you process or store.
4. Describe the logs that you maintain.
5. Are you preserving the environment?
6. Do you have a network diagram?
7. Describe your network environment.
8. What IT resources do you have?
9. Are there critical third party vendors?
10. What have you done so far?
Who Needs to be Notified?

- Affected Individuals
- Government Agencies
- Attorneys General
- Law Enforcement
- Credit Reporting Agencies (CRAs)
Offer of Credit Monitoring?

**Why**
- To mitigate harm
- Affected individuals’ expectations
- Regulators’ expectations

**Why Not**
- Does not prevent fraudulent charges on payment cards
- May impact litigation position
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
Costs of Breach Response

- Forensics
- Notification costs
- Credit monitoring
- Call center
- Remediation
- Legal fees
- Defense costs/settlement expenses
- Assessments & regulatory fines
Cyber Insurance Myths

1. *Cyber risk is too low to justify costs*
2. *IT has it under control*
3. *Existing insurance already covers cyber liability*
4. *Cyber attackers only target big companies*
Cyber Insurance Coverage: Breach Response

- Forensic investigators
- Legal counsel (including analysis for notification obligations and regulatory compliance)
- Notification vendors (including, printing and call center)
- Credit monitoring vendors
- Identity-theft related fraud resolution services
- Loss prevention services
- Crisis management services for public relations
Cyber Insurance Coverage Types

- **Remediation Coverage**: covers forensics, notification, credit monitoring, call center, legal, and public relations costs
- **Regulatory Coverage**: covers costs of response to administrative, government, or regulatory investigations, fines and penalties
- **Information Assets Coverage**: covers costs of recreating, restoring, or repairing damaged data and computer systems
- **Network Interruption Coverage**: covers lost revenue due to network interruptions or disruptions due to denial of service attacks, malicious code, etc.
- **Extortion Coverage**: covers costs of responding to ransom or extortion demands to prevent a threatened cyberattack
Cyber Insurance Considerations

1. Make sure policy limits and sub-limits are adequate for existing needs
2. Request retroactive coverage for prior unknown breaches
3. Be cautious of panel and prior consent provisions
4. Consider coverage for claims resulting from data vendors’ errors
5. Consider coverage for “loss” of data, not just data “theft”
6. Combine cyber insurance with data vendor indemnities to maximize protection
7. Request a subrogation waiver from insurer
8. Harmonize cyber coverage with other insurance
9. Negotiate favorable defense provisions
ANY QUESTIONS?