Managing Public Sector Cyber Risk

CT PRIMA Risk Management Day

September 16, 2016

Christopher Wardrop, CIC, CRM, SVP
Phone: 203-634-5764
Email: Christopher.Wardrop@usi.com
What is Cyber Risk?

- **Internet Liability Exposures** – Third party liability, personal injury and intellectual property associated with a website that can include a domain name or trade name infringement, copyright, defamation, etc.

- **Privacy Liability** - Associated with privacy issues, including the theft of personally identifiable data in hardcopy, electronic, or other format, including virus transmission or other ‘means’ of compromised data that is passed to a third party.

- **Network Security Liability** – Associated with a virus, hacker or denial of service attack originating internally, through email, or through the internet.

- **First Party** Exposures – Credit monitoring and disclosure costs, fines/penalties, public relations and crisis management expenses, forensic services, data reconstruction, etc.

- The downtime and other “indirect costs” associated with any or all of the above.
Regulatory Enforcement Actions/Acts


- **Health Insurance Portability and Accountability Act (HIPAA)** – applies to not only health care businesses but any employer that provides health care benefits

- **Gramm-Leach-Bliley Act (GLBA)** – Those affected must adhere to strict policies when handling non-public personal information – fines up to $1 million and 10 years in jail

- **Payment Card Industry Data Security Standard (PCI DSS)** – a worldwide security standard created to prevent credit card fraud

- **Sarbanes Oxley Act (SOX)** – Effective in 2002, sets standards for publically traded companies board, management and their accounting firms

- **Fair and Accurate Credit Transactions Act (FACTA)** – Disposal Rule – passed in 2003, created standards to help reduce identity theft and allows consumers to obtain a free annual credit report

- **Red Flag Rules** (FACTA Section 114).

- **Federal Trade Commission (FTC)** – this is the most active enforcer and brought enforcement actions resulting from security breaches for Target, BJ’s Wholesale Club, CardSystems, ChoicePoint & DSW)
Who is Exposed?

- Any organization holding personally identifiable information
- Organizations managing a computer network
- Organizations who would suffer from lost revenue if attacked
- All companies in business (ie your vendors/suppliers)

...So basically every organization!
All Industries Are Exposed. Critical Industries Include:

- Public Entities
- Financial institutions
- Healthcare
- Retail
- Service Providers
- Lawyers
- Technology
- Manufacturing
- Auditors
- Hospitality
- Medical Billing
- Schools
- Travel Agents
- Advertising
- Food and Beverage
- Pharmaceuticals
What “they” want: PII (personally identifiable information)

- Credit Card Information
- Personal Financial Information
- Social Security Numbers
- Drivers License Numbers
- Banking Information
- Employment Information
- Insurance Information
- Personal Health Information
- Business Information of others
- Trade Secrets
PII (personally identifiable information) – where does it hide in a public entity?

- Town or City Hall
  - Finance Department
  - Town Clerk
  - Social Services
- Park/Recreation Departments
- Board of Education
  - Cafeteria student accounts
  - Student activity accounts
  - Hard copy student records
  - Guidance/student advisors
- Senior Center
- Law Enforcement
- Utility Customer Service Center
Potential Data Breach Threats – Inside and Outside Your Organization

- Lost or stolen laptop, computer, tablet, smart phone or other storage device
- Backup media lost in transit
- Hacking by outside individuals or organizations
- Posting confidential personal information on your website
- Employee theft / human error
- Internal security failure
- Viruses, malware, computer security loopholes
- Improper disposal of information
What is at Stake to Your Organization?

- Legal / defense Costs
- Indemnity and settlements
- State notification costs
- Regulatory investigation / assessed fees
- Bad press / reputation
- Dissatisfied residents/employees
- Financial strength ratings
- Unbudgeted expenses & potential mill rate increases
Statistics on Data Breach/Identity Theft

- Organizational cost “per lost/stolen record” is $90-300 – direct and “soft” costs.
- Malicious or criminal attacks rather than negligence or system glitches are the main causes of data breach.
- 285 million records were breached in 2011 and have gone up each year since
- 69% were discovered by a third party
- Insider negligence is present in the majority of actual cases
The Insurance Gap

- **General Liability**
  - Excludes damage to and corruption of electronic data
  - Covers only “tangible” property
  - Personal and advertising liability does not cover violations or misuse of private information
  - Limited to bodily injury and property damage

- **Crime**
  - Covers loss due to employee theft of money, security or other property
  - Must be tangible and have intrinsic value
  - No coverage for loss of confidential information
The Insurance Gap (cont.)

- **Public Officials Liability Insurance**
  - Typically excludes a security breach
  - May not meet the definition of “Wrongful Act”
  - Limited Coverage with late trigger or report

- **Computer/Electronic Data Processing (EDP) Rider**
  - Typically excludes employee dishonesty and errors in programming

- **Property**
  - Coverage is specific to physical loss or damage to tangible property
  - Computer viruses are excluded
  - Errors in processing, programming, electronic data, electronic vandalism typically excluded
Key Coverage Aspects of Cyber Coverage

1st Party Cyber Liability Coverage

- Data Asset/Data Restore
  - Covers data restoration expenses after a covered data breach
  - Includes coverage for hiring forensic expert to determine source of breach

- Business and Operation Interruption
  - Covers costs and expenses resulting from a shut down of operations due to a covered data breach. (not always included).

- Reward Expense
  - May cover cost associated with information that leads to an arrest or conviction

- Crisis Management
  - Covers cost to hire a public relations firm to protect brand image and reputation
Key Coverage Aspects of Cyber Coverage (cont.)

1st Party Cyber Liability Coverage

- Notification (*Coverage may be included under privacy coverage as 3rd party*)
  - Includes costs for mailing state notification to each individual breached (postage), cost for credit monitoring if required, changing of account numbers or security codes, call center investigative costs
  - Expenses related to forensics, call center creation, I.D. theft insurance, PR vendors and attorney oversight

- Cyber Extortion
  - Covers cost to investigate, negotiate and settle if credibly threatened or if an extortion demand is received
  - Includes coverage for Ransomware claims (subject to deductible)
  - Case Study: Durham, NH Police Department

- Social Engineering
  - Phishing to get employees to transfer money
  - Phishing to get employees to transfer information
Key Coverage Aspects of Cyber Coverage (cont.)

3rd Party Cyber Liability Coverage

- Network Security
  - Responds to your liability when hackers use your systems to inflict damage on others. Covers unauthorized access, unauthorized use and denial of service attacks. Includes defense and settlement costs.

- Privacy
  - Responds to your liability when private information is disclosed. This can include a breach from a computer network or from a paper file. Covers failure to protect private or confidential information. Includes defense and settlement costs. The following can also be added:
    - Notification Expenses
    - Credit Monitoring
    - Credit Repair Services
    - Event Crisis Management
    - Regulatory Defense and Expenses
Some areas to focus when negotiating with your carrier(s):

- **Breach Response Costs Coverage:**
  - Offered at full policy limit or sub-limited?
  - Inclusive of overall limit or “Outside” the limit?
  - Dollar amount or on a “per record” basis?

- **Other things to consider:**
  - Regulatory coverage (seek full limit and defense/penalties)
  - Seek full “unknown” prior acts coverage
  - Avoid “Unencrypted portable device” exclusions
  - Data restoration/business interruption coverage – waiting period?
  - Cyber extortion/ransomware coverage?
  - Social Engineering sub-limit offered?
The Current Cyber Insurance Marketplace

- **Major municipal programs**
  - CIRMA
  - Trident
  - Travelers
  - Others

- **The Open Marketplace**
  - Ability to customize limits, retentions, manuscript forms
  - ACE
  - Beazley
  - AIG
  - Many others
  - Proprietary programs (USI’s “PrivaSafe” program)

- Forms and coverage language changing weekly
- Carrier appetites adjust based on claims trends in certain industry segments
How Do We Protect Ourselves? Risk Management Recommendations

- Know Your Organization’s Network and Cyber Security Risks
  - Use a self-assessment tool
  - Utilize law enforcement or outside consultants/experts
  - Review your basic security controls (ex. Encryption, passwords)
  - Review internal and external threats with your peers
  - Review or create a data breach response plan – who would you turn to?
  - Communicate security policy and procedures with all employees, in writing
  - Manage what hard copy and electronic data is kept.
  - Keep security software up to date
  - Consider sensitive information including in Freedom of Information request responses

- Know the Rules
  - Privacy regulations
  - Notification laws
  - Federal/State/Local regulations
Know Your Employees
- Communicate security policy and procedures with all employees, in writing.
- Manage what hard copy and electronic data is kept.
- Review employee access to data – including on tablets and smart phones

Know Your Business Partners
- Review contract language including indemnification provisions
- Broaden insurance requirements to cover loss of data and other expenses not related to bodily injury or tangible property damage
- Verify your business partner/vendor has their own data breach plan.
- Case Study #1 – Fire/EMS Software Vendor
- Case Study #2 – School/Google relationship

Consider Cyber Insurance
- Fills gaps in “traditional” property/casualty insurance
- Acts as a financial backstop to protect your budget
- Responds to resident & taxpayer questions about how you are protecting your organization and budget from new and emerging risks.
Now go out there and get ‘em!

Questions/Comments?

Christopher Wardrop, CIC, CRM, SVP
Phone: 203-634-5764
Email: Christopher.Wardrop@usi.com

Thank you from USI Insurance Services’
Public Entity Team!