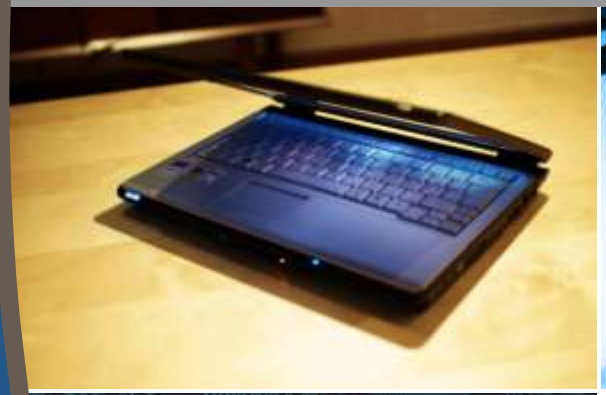
Cindi Heffernan, CPCU
Alliant Insurance Services, Inc.

Cyber Liability Overview
April 18, 2012



Alliant

PEOPLE | PRODUCTS | PROCESSES

Agenda

- Cyber Background
  - Types of Data Maintained
  - Breach Defined
  - How does a Breach Happen?
  - The Numbers
  - Costs Associated with a Breach
- Claims
- Coverage
  - Cyber Liability
  - Privacy & Security Liability

Types of Data Maintained

- Personally Identifiable Information (PII)
  - Name, Date of Birth. Address, Social Security Numbers
- Protected Health Information (PHI)
  - Medical Records
- Credit Card Numbers
- Confidential Business Information
  - Technical Data
  - Hard copy

Breach Defined

- In general:
  - The unauthorized acquisition, access, use or disclosure of protected information, which compromises the security or privacy of the information
  - The breach in turn, poses a significant risk of financial, reputational, or other harm to the individual

Seconds to Breach

How Does A Breach Happen?

- Lost or stolen laptops often containing protected information for numerous individuals
- Theft – internal & external
- Inadequate destruction of data
- Lost back up storage devices
- Stolen computer servers
- Hacking/Phishing
- Denial of Service
- Cyber Extortion
- Cloud Computing

The Numbers

- Data indicates that in less than two years unsecured protected information data breach has impacted 11 million people.
- Estimates of the costs associated with breach response following a stolen laptop can be as high as $258 per record.
- $32 billion loss to consumers
- $130.1 billion cost to businesses
- 40 new malicious programs per minute
- 14 victims worldwide every second

Costs Associated With A Breach

- Third party liabilities from suits by individuals impacted by the breach
- Estimates in excess of $250 to notify each individual
- Loss of reputations and public confidence
- Taxing of internal resources in information technology, legal, public relations and other support departments

Recent Public Entity Breaches

www. privacyrights.org

- March 21, 2012 **City of Providence, Providence, Rhode Island**

  The city of Providence **accidentally** provided the Social Security numbers of almost **3,000** former employees when releasing information for a **public records request**. The city's legal team responded to the request by emailing a .pdf file with retiree names, dates of retirement, dates for cost-of-living-adjustments, and monthly pension received each month. Social security numbers and employee identification numbers were displayed as redacted in the document, but could easily be read when the .pdf file was expanded or when the highlight color of the document was changed to a light color.

- February 28, 2012 **City of Springfield, Springfield, Missouri**

  Two **hackers claimed responsibility** for hacking the website of the city of Springfield, Missouri. The breach occurred on February 17, and the databases on the server contained over 300,000 entries. **Hackers** claimed to have acquired 6,071 entries related to the date of birth, weight, height, race, hair color, skin tone, phone number, address, and Social Security number of people listed in online police reports. The hackers posted a significant amount of information, but voluntarily removed any sensitive information that could cause problems for consumers.

Recent Public Entity Breaches, Cont

- November 4, 2011 **Washington South Supervisory Union, Northfield, Vermont**

  Supervisory Union notified all employees that a **serious security breach** on its financial computer system was discovered and that their financial information may have been compromised. The breach was not described in detail, but employees were informed that payroll would be temporarily using paychecks. Supervisory Union contacted all banking institutions that were involved in **direct deposit** and informed them that client data may have been compromised. Employees were also encouraged to contact all banking institutions to review their financial accounts, contact their banks, change their email passwords, and avoid clicking on suspicious emails.

- March 17, 2012 **Kennedy Space Center, Orlando, Florida**

  The theft of **a company-issued laptop** from an employee's car resulted in the exposure of sensitive information. The laptop was stolen from the employee's car while it was at home and contained the names, Social Security numbers, races, national origins, genders, dates of birth, contact information, college affiliations, grade-point averages, and other information of employees. The hard drive was not encrypted. The Kennedy Space Center had planned to have all hard drives encrypted by September 2012 prior to the breach.

What are the Costs?

- Attorney Fees
  - Breach Guidance
  - Investigation
  - Notification
  - E-discovery
  - Litigation Preparation
  - Contractual Review
  - Defense
- Plaintiff Demands
  - Fraud Reimbursement
  - Credit Card Replacement
  - Credit Monitoring/Repair/Insurance
  - Civil Fines/Penalties
  - Time
- Breach Costs
  - Forensics Vendor
  - Notification Vendor
  - Call Centers
  - PR Vendor
  - ID Theft Insurance
  - Credit Monitoring
  - ID Restoration
  - Attorney Oversight

Cyber – Coverage Elements

- Information Security & Privacy Liability
- Privacy Notification Costs
- Regulatory Defense and Penalties
- Website Media Content Liability
- System damage & restoration; business interruption from hacking or virus

Cyber – Coverage Highlights

- Limits of Liability
  - $1,000,000 Aggregate Limit each insured/member
  - $10,000,000 Aggregate Limit all insureds/members
  - $250,000 Aggregate Limit – Notification Costs
  - $25,000 BI hourly sublimit & Forensic Expense sublimit
- Retentions
  - $50,000 – TIVs under $500MM
  - $100,000 – TIVs $500MM and over

Current Cyber Policy
Additional Technology Assistance

- Experienced claims team and expert service providers provide an immediate and appropriate data breach response
- Legal experts regularly handle data breaches and can walk you through the complex minefield while also understanding the sensitivities of the situation which can affect your reputation

Privacy & Security Liability Coverage

- Coverage designed for Entities with lower exposure
- Coverage includes:
  - Notification
  - Credit Monitoring
  - Extra Expense
  - Fines & Penalties
  - Public Relations
  - Loss Control
- Can be added to a Public Officials Liability policy
- Lower premiums – based on revenue and class of buisness
- $1,000,000 max. limits

Questions??

Cindi Heffernan, CPCU

Alliant Insurance Services, Inc.