



YOUR DELAWARE ADVANTAGE

Data Security and Data Breaches: Critical Legal and Business Risks

Presented to Greater Wilmington Cyber Security Group
Presented by William R. Denny and Alan R. Silverstein

February 6, 2013



Topics for Discussion

- Why do you need a response plan?
- What is a data security breach?
- State requirements and legislative update
- What should you be doing?



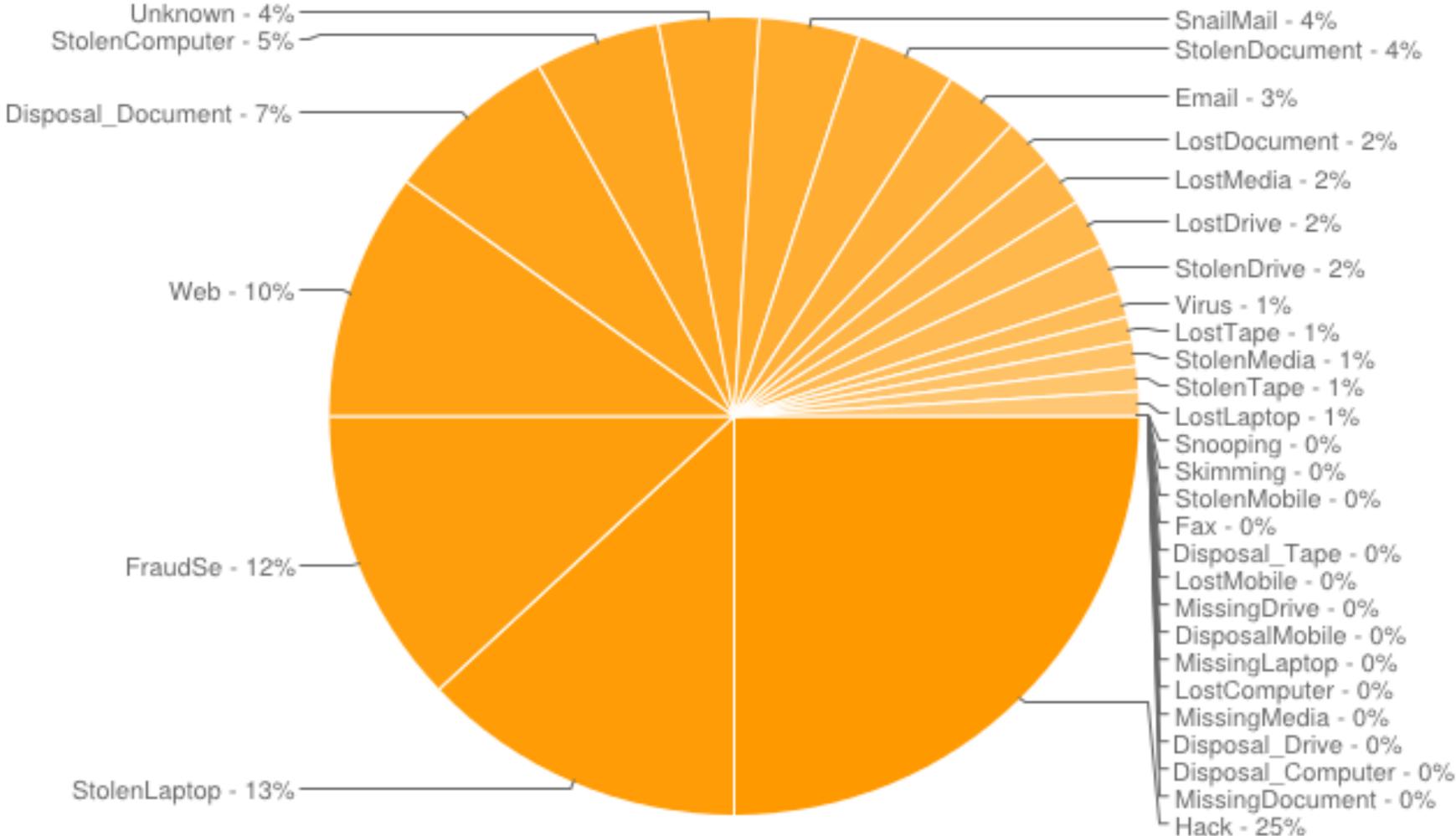
Why do You Need a Data Breach Response Plan?

- Numbers of Breaches are Growing
 - 2012 total: 1478 breaches (36% increase over 2011)
 - Source: Open Security Foundation / DataLossDB.org
 - 2011 total: 1086 breaches
 - 2010 total: 826 breaches
 - 2009 total: 727 breaches
- Average cost of data breach in 2010 was \$7.2 million, or \$214 per lost record
- FTC and State Attorneys General are prosecuting companies for failing to protect personal information (“PI”)
- Public relations nightmare!



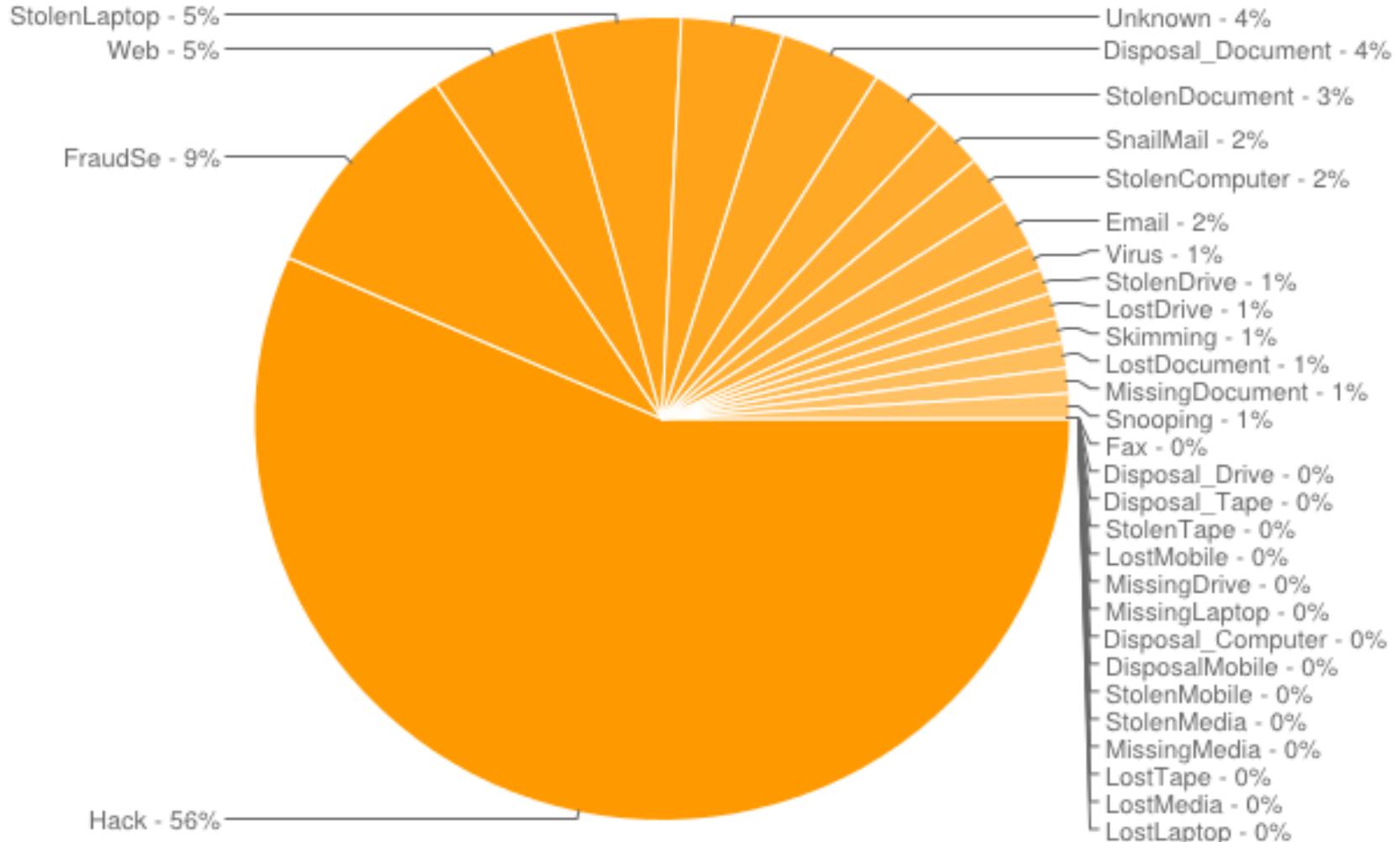
Incidents by Breach Type – All Time

Incidents by Breach Type - All Time



Incidents by Breach Type - 2012

Incidents by Breach Type - Last Year



The Evolving Threat

- Major Incidents of Data Breach in 2012 include:
 - Zappos – 24 million records, hacker
 - University of North Carolina – 350,000 records, exposed data
 - Global Payment Systems – 7 million records, hacker
 - South Carolina Health and Human Services – 228,435 records, insider
 - University of Nebraska – 654,000 records, stolen from database
 - LinkedIn – 6.5 million records, hacked
 - Nationwide Mutual – 1.1 million records



Benefits of a Data Breach Response Plan

1. Thoughtful and Prepared Reaction
2. Better Decision Making
3. Minimized Risk and Loss



What Is a Data Security Breach?

- A breach of the security of a system that involves unencrypted personal information (“PI”) that has been or is reasonably believed to have been acquired by an unauthorized person.
- PI = First name or initial and last name with one or more of the following: SSN, drivers license number, credit card number, financial account number with PIN, password or authorization code.
- Distinguish between data owner and service provider.



Privacy = Security = Privacy

- Data privacy and information security are linked
- Information security is a legal and technology issue
- It applies to all companies
- There are legal standards for security
- The law is a work in progress



What Type of Legal Duties?

- Duty to provide appropriate security
 - To prevent breaches
 - To detect breaches
 - To respond to breaches
- Duty to warn
 - Duty to disclose breaches to those who may be affected
- Duty to disclose state of security readiness
 - Transparency for investors, customers and others



State Requirements and Legislative Update

- State laws continue to evolve
- Breach disclosure statutes have been enacted in 46 states
 - Four states without such laws are Alabama, Kentucky, New Mexico and South Dakota
- Data disposal laws have been enacted in 29 states
- Data security laws in some states
- Massachusetts has enacted far-reaching rules establishing minimum standards for safeguarding personal information



Massachusetts Data Security Regulations

- Intended to establish *minimum standards*
- Applies to *any* entity that owns or licenses PI about a resident of Massachusetts
- Risk-based approach, taking into account size, scope and type of business, amount of resources available, amount and type of data collected, and need for security and confidentiality of PI in paper and electronic form



Massachusetts Data Security Regulations

- Companies must develop, implement and maintain a comprehensive written information security program (WISP)
 - Designate employees to maintain the WISP
 - Identify and assess reasonably foreseeable internal and external risks: data mapping
 - Develop security policies and training for employees
 - Oversee third party providers
 - Regular monitoring
 - Establish and maintain up-to-date computer security systems
 - Encryption
 - Backup tapes



Delaware Law

- Delaware Law: Computer Security Breaches (6 *Del. C.* §12B-101)
 - All companies possessing PI of Delaware residents
 - Obligation to investigate suspected breaches
 - Obligation to notify Delaware residents about unauthorized access to their PI
 - Encryption is a defense
 - Noncompliance can result in civil liability
- Level of encryption required may be defined by state laws



Concerns with State Law Approaches

- Potentially conflicting and cumulative burdens
- Geographical uncertainties regarding jurisdiction
- Common law theories cause courts to become rulemakers
- Enforcement issues
 - Standing to sue
 - Difficult to ascertain damages
 - State agency resources and expertise



Will We Get Federal Legislation?

- Obama's cyber security legislative proposal includes national data breach reporting system
- Several proposals in House and Senate
 - Data Security and Breach Notification Act of 2012 (S.3333)
- Existing Piecemeal Laws Dealing with Data Breach
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Health Information Technology for Economic and Clinical Health Act (HITECH Act)
 - Gramm-Leach-Bliley Act (GLBA)
 - OMB's "Breach Notification Policy" for Federal Agencies





What should you be doing?



Know Your Information

- Do you know what kind of information you have and what happens to it?
 - Evaluate any place that you collect, store and disclose sensitive data
 - Pay attention to employee data as well as customer data
 - Identify where and to whom this information is disclosed
 - Look at access controls for how your employees view information



Pay Attention to the Right Rules

- Marketing rules
- Collecting information from children
- Health care benefits program
- Disposal of sensitive information
- Employee monitoring



Have an Information Security Program

- Assign responsibility
- Keep proper documentation
- Program should include paper and electronic
- Train employees on basic information security
- Oversee vendors and key contract terms
- Stay on top of security developments
- Pay attention to problems faced by others



Who Should Be Involved?

- Not just an IT or public relations initiative
- Critical to involve C-level management

- Incident Response Team:
 - Information technology resources
 - Information security (physical security and access)
 - Compliance
 - Business heads (consumer information)
 - Human resources (employee information – medical, payroll, tax, retirement)
 - Legal counsel
 - Public relations / investor relations



Be Ready to Act

- Who is in charge when there is a data breach?
- Where do your employees report problems?
- Do you have a good program to identify and fix problems?
- Evaluate requirements for security breach mitigation and notification



Steps to Minimize Risks

- Collect the minimum amount of PI necessary to accomplish the business purposes
- Retain PI for the minimum time necessary
- Mandate encryption for all PI
- Limit the number of people with access to PI
- Regularly monitor and review who has access
- Create and enforce necessary policies



Elements of a Data Breach Notification Policy

- Procedure for internal notification of security incidents
- Procedure to notify data owner following detection of security incident
- Procedure to contact appropriate law enforcement
- Procedure to notify individuals whose unencrypted PI may have been accessed by unauthorized persons
 - Statutory time requirements may be as short as 30 days
- Procedure to document response actions taken
- Review compliance with all state data breach protection laws



Assign Tasks to Members of Response Team

- Establish a point person
- Identify key personnel for each task
- Prioritize and assign tasks
- Calculate timelines and set deadlines
- Communicate with management
- Establish attorney-client privilege for investigation and communications



Determine Nature and Scope of Breach

- Investigate facts
- Interview witnesses
- Determine type of information compromised
- Assess potential liability
- Identify individuals potentially at risk and state of residence



Understand Data Breach Notice Requirements

- State laws:
 - What constitutes PI?
 - When is a notice required?
 - Who must be notified?
 - Timing?
 - What information must be included in notice?
 - Method of delivering notice?
 - Other state-specific requirements?
- Industry-specific laws
- International laws



Determine Appropriate Notices

- Customers
- Employees
- Law enforcement (state/federal)
- Federal regulatory agencies
- State agencies
- Consumer reporting agencies
- Third party vendors
- Insurers
- Media



Prepare Notices

- Content of notices
 - General description of the incident
 - Type of information compromised
 - Steps to protect information from further unauthorized access
 - Contact information
 - Advice to affected individuals (credit reporting, review account activity)
- Delivery method
- Timing
- Tailor notices based on recipient



Summary of How to Plan for a Breach

- Plan for the worst – not “if” but “when”
- Have plans and procedures in place
- Appoint an Incident Response Team
 - Core team to manage a security breach
 - Clearing house for investigation, containment, compliance, law enforcement and the media
 - Empowered to take swift and decisive action
- Draft notices should be ready to go – and know who needs to be notified and when
- Practice, practice, practice



To reach us

William R. Denny

Direct dial: (302) 984-6039

wdenny@potteranderson.com

Alan R. Silverstein

Direct dial: (302) 984-6096

asilverstein@potteranderson.com

Potter Anderson & Corroon LLP

1313 North Market Street

P.O. Box 951

Wilmington, DE 19899-0951

www.potteranderson.com

