



PROTECT. MANAGE. GROW.

## Cyber and Privacy Liability

### *An Overview*

*Thomas Ciano*

[Tom.ciano@usi.biz](mailto:Tom.ciano@usi.biz)

*(781) 376-2710*



## *What is Cyber Liability?*

- The liability associated with e-business, the Internet, networks and use of computer technology
- The liability associated with privacy issues, virus transmission or other 'means' of compromised data that is passed to a third party

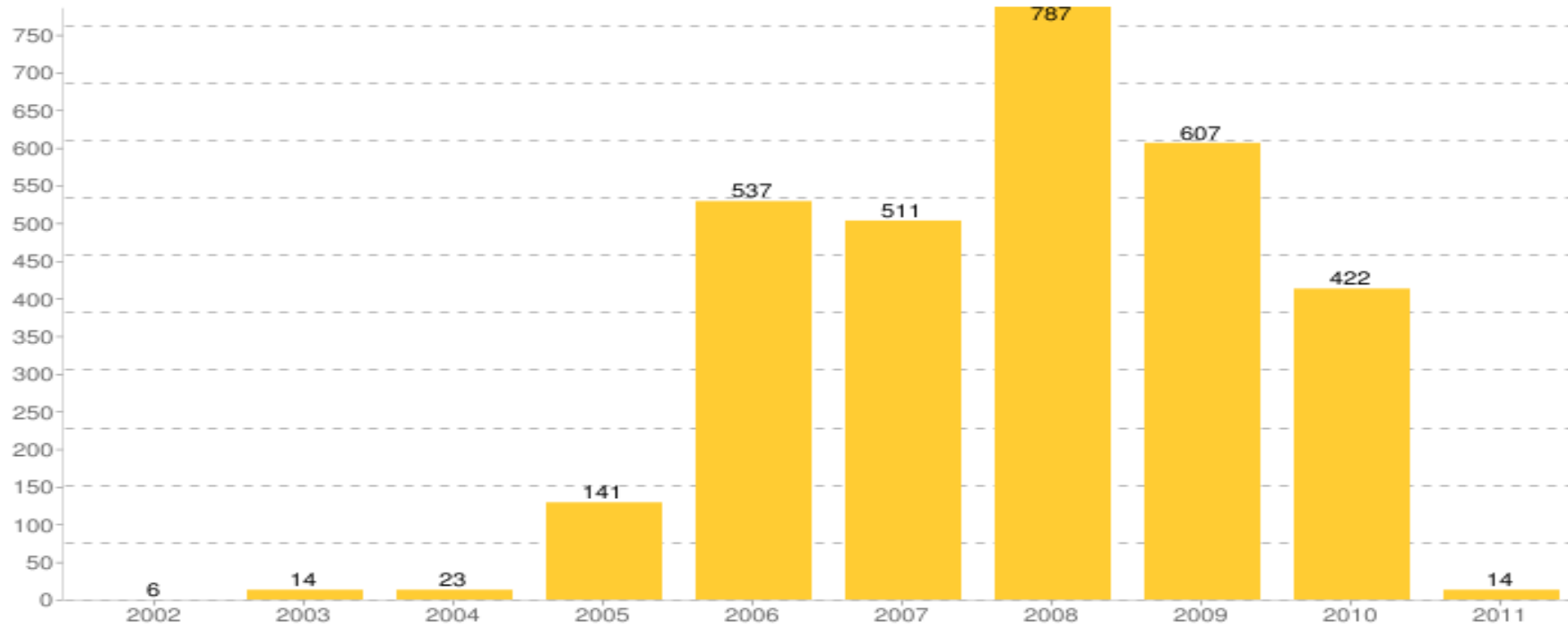


PROTECT. MANAGE. GROW.



## Historical Data Loss Incidents (as of February 2011)

DataLossDB.org Incidents Over Time



Datalossdb.org is operated by the Open Security Foundation, a non-profit organization dedicated to tracking and reporting security vulnerabilities and breaches of personal information. Source: <http://datalossdb.org>

3/28/2011

Content © 2009 USI.

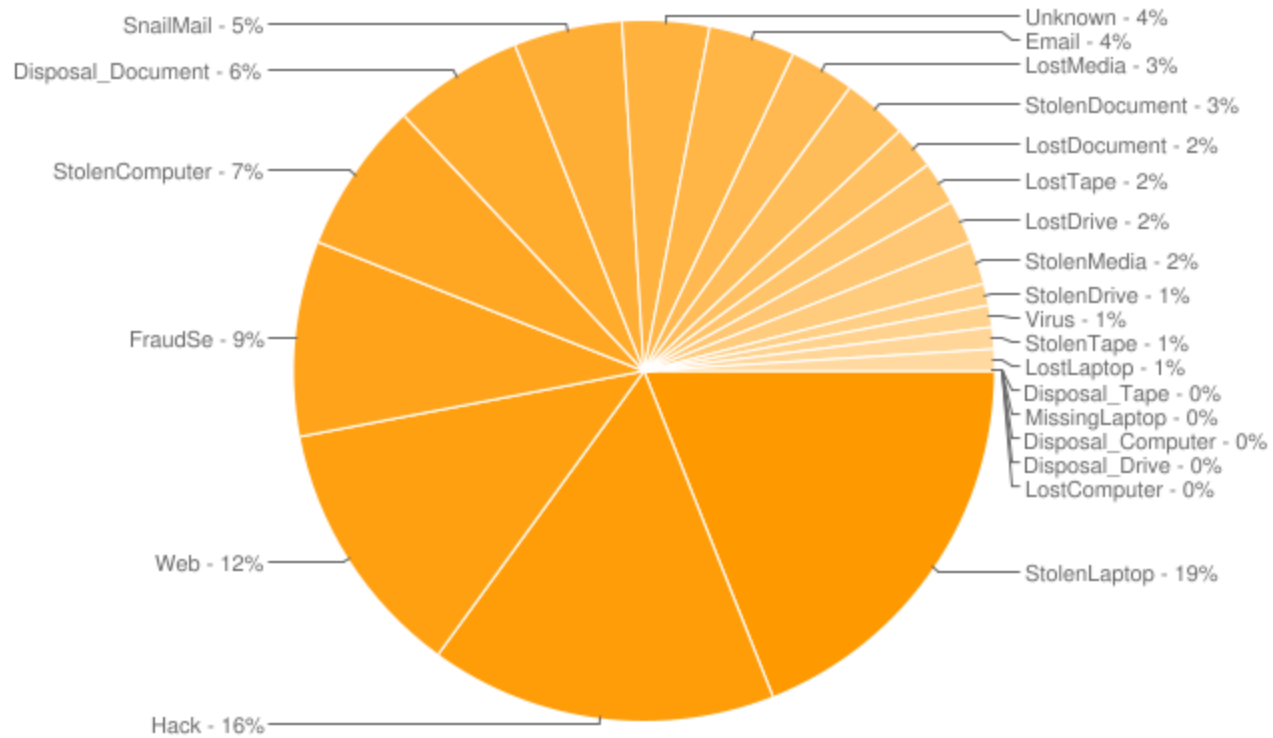


PROTECT. MANAGE. GROW. 3



## Types of Incidents (as of February 2011)

Incidents by Breach Type - All Time



Source: <http://datalossdb.org>

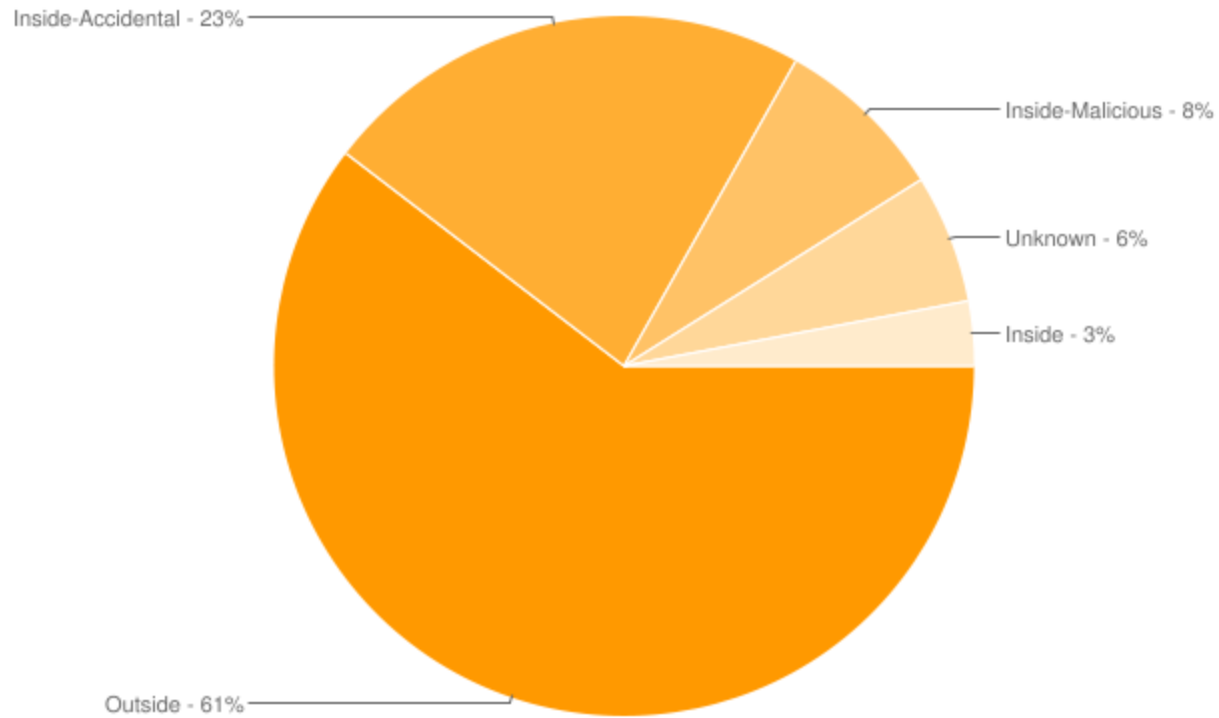


PROTECT. MANAGE. GROW.



## Incidents By Vector (as of February 2011)

Incidents by Vector - All Time



Source: <http://datalossdb.org>



PROTECT. MANAGE. GROW.



## *Recent Healthcare Breach Examples*

<b>Date Reported</b>	<b>Company</b>	<b>Summary</b>	<b>Estimated Cost*</b>
2/4/2011	Medi-Cal	2,400 Beneficiaries' names, Social Security numbers and other identifying information emailed to personal computer, two attorneys and two union representatives	\$144,000
1/19/2011	Hull and East Yorkshire Hospitals NHS Trust	1,147 Records exposed including health info, names. Addresses on lost laptop	\$68,820
1/13/2011	St. Vincent Hospital	1,800 patient names, dates of service and certain clinical information exposed due to email breach	\$108,000
1/6/2011	Grant Medical Center	Unsecured patient information on computers stolen by employee and sold to computer store	Unknown
1/4/2011	Pinnacle Health System	1,086 patients' names, dates of birth, Social Security Numbers, medications, and medical notes exposed on web for over two years	\$65,160
1/4/2011	Gary C. Spinks, DMD, PC	1,000 patient names, addresses, health and dental insurance member numbers, Social Security Numbers, dated of birth, dental care records, and dental x-rays may have been access by hacker	\$60,000



## Recent Healthcare Breach Examples (continued)

Date Reported	Company	Summary	Estimated Cost*
12/27/2010	Geisinger Wyoming Valley Medical Center	2,928 patient names, medical record numbers and medical procedure notes sent via unencrypted emailed to physician home email account	\$175,680
12/23/2010	Mankato clinic	3,159 patient's full name, date of birth, medical record number, healthcare provider's name, encounter date, and diagnosis information stolen from laptop parked in car	\$189,540
7/19/2010	South Shore Hospital	Backup tape lost by vendor exposes 800,000 patients medical details	\$48,000,000
2/8/2010	AvMed Health Plans	Stolen laptop exposes 1.2M names, addresses, Social Security numbers and health details	\$72,000,000

\*Note that these estimates are based on the Ponemon Institute's 2009 direct costs figures from their [2009 Annual Study: Cost of a Data Breach](#). We multiply \$60.00 by the number of records to obtain this figure. Keep in mind that depending on the breach, the direct costs are not always suffered by the breached organizations. In the case of credit card number breaches, the direct costs can often be suffered by banks and card issuers. Also note that this is only an estimate.



PROTECT. MANAGE. GROW.



## *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
- **State Breach Laws** (CA CB 1386 – landmark act in 2003)
- **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** – Signed into law Dec 2010, requires financial institutions and creditors to have a written Identity Theft Prevention program designed to detect ID theft warning signs
- **Federal Trade Commission (FTC)** – this is the most active enforcer and brought enforcement actions resulting from security breaches for BJ's Wholesale Club, CardSystems, ChoicePoint & DSW.



## *MA Data Protection Regulation – 201 CMR 17.00*

- Applies to **ALL** organizations that have personal information of MA residents in **either paper or electronic** form.
- Requires:
  - Written information security program (WISP)
  - Identification of all paper records and electronic storage media containing personal information
  - Restricting access to all such records or media
  - Encryption of all personal information
    - stored on laptops or other mobile devices
    - to be transmitted wirelessly and,
    - to the extent technically feasible, that will travel across public networks
  - System monitoring
  - Employee training
  - Taking reasonable steps to select third party service providers that are able to comply with the regulations.
  - Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information

See <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>



PROTECT. MANAGE. GROW.



## *Who is Exposed?*

- Companies holding personally identifiable information
- Companies managing a network
- Companies who would suffer from lost revenue if attacked
- All companies in business



PROTECT. MANAGE. GROW.



## *Review: Potential Data Breach Sources*

- Lost or stolen laptop, computer or other storage device
- Backup tapes lost in transit
- Hackers
- Employee theft / human error
- Internal security failure
- Viruses, malware, computer security loopholes
- Improper disposal of information



PROTECT. MANAGE. GROW.



## *What is at Stake?*

- Bad press / reputation
- State notification costs
- Dissatisfied customers / employees
- Legal / defense Costs
- Indemnity & settlements
- Regulatory investigation / assessed fees
- Financial strength
- Unbudgeted expenses



PROTECT. MANAGE. GROW.



## *Statistics on Data Breach/Identity Theft*

- 500 million records have been breached since 2005<sup>1</sup>
- 70% resulted from external sources<sup>2</sup>
- 60% were discovered by a third party<sup>2</sup>
- The average cost per record compromised is now \$204 based on the 2008 sample<sup>3</sup>
- Insider negligence remains present in majority of actual cases<sup>3</sup>
- Average total per incident cost in 2009 was \$6.75 million<sup>3</sup>

1- Privacy Rights Clearinghouse

2 - Verizon Business 2009 Data Breach Investigations Report

3 - Ponemon Institute January 2010 Fifth Annual US Cost of Data Breach Study





## *The Insurance Gap*

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



PROTECT. MANAGE. GROW.



## *The Insurance Gap (continued)*

- **Miscellaneous E&O**
  - Typically excludes a security breach
  - Designed to provide errors & omissions coverage for non-tech based operations
- **EDP Rider**
  - Typically excludes employee dishonestly and errors in programming
- **Property**
  - Coverage is specific to physical loss or damage to tangible property
  - Named physical perils
  - Errors in processing, programming, electronic data, electronic vandalism typically excluded





## *Reasons to consider Cyber & Privacy Liability Coverage*

### ■ Laws & Regulation

- Legal Cost - a cyber crime attorney may cost up to \$700 per hour
- Keeping quiet is not an option
- Notification Costs can average from \$2 to \$12 per person
- Court ordered credit monitoring can average from \$10-\$30 per year / per person
- Regulatory/Governmental Fees

### ■ Technology

- Millions of records can be contained on one key size USB drive

### ■ Outsourcing

- Information is being moved further out of our physical control with outsourcing of network services, utilization of off-site hosting and 3<sup>rd</sup> party system updates



PROTECT. MANAGE. GROW.



## *Key Coverage Areas in Cyber Liability*

### *3<sup>rd</sup> 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





## *Key Coverage Areas in Cyber Liability (continued)*

### *3<sup>rd</sup> Party Cyber Liability Coverage*

- Media or Content
  - Responds to advertising injury for losses arising from the display of material online
- Intellectual Property
  - Responds to loss arising from infringement of trademark, copyright and other protected sources



PROTECT. MANAGE. GROW.



## *Key Coverage Aspects in Cyber Liability (continued)*

### *1<sup>st</sup> Party Cyber Liability Coverage*

- **Data Asset/Data Restore**
  - Covers data restoration expenses after a covered data breach
- **Business 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



PROTECT. MANAGE. GROW.



## *Key Coverage Aspects in Cyber Liability (continued)*

### *1<sup>st</sup> Party Cyber Liability Coverage*

- Notification (*Coverage may be included under privacy coverage as 3<sup>rd</sup> 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
- Cyber Extortion
  - Covers cost to investigate, negotiate and settle if credibly threatened or if an extortion demand is received



PROTECT. MANAGE. GROW.



*Questions?*



PROTECT. MANAGE. GROW.



## *Resources*

- [www.ncsl.org](http://www.ncsl.org)
- [www.pcisecuritystandards.com](http://www.pcisecuritystandards.com)
- [www.ftc.gov](http://www.ftc.gov)
- <http://datalossdb.org>
- [www.privacyrights.org](http://www.privacyrights.org)



PROTECT. MANAGE. GROW.