Cyber Liability Risks - What, How, Costs, Risk Mitigation

sponsored by

Insur Banc

A Division of Connecticut Community Bank, N.A.
# Recent Security Breaches

<table>
<thead>
<tr>
<th>Who</th>
<th>How</th>
<th>What</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Milford/Uxbridge School 2013</td>
<td>Laptop containing personal information was stolen from Multi-State Billing Services (Medicaid billing) employee vehicle.</td>
<td>3,000 Student Records</td>
<td>MSBS to reimburse for credit freezes for 3yr. Possible violations of MA privacy laws: laptop sensitive data must be encrypted. Fines can be $5000 per person or record</td>
</tr>
<tr>
<td>Legal Seafood 2014</td>
<td>Unauthorized person accessed a server containing information from online customer transactions. Hacker breached the identity of individuals in 8 colleges and administrations.</td>
<td>4,000 Credit Cards</td>
<td>Still Open / TBD</td>
</tr>
<tr>
<td>Harvard University July, 2015</td>
<td>Identity thieves hacked into patient information database, to steal private data.</td>
<td>151,626 Patient Records</td>
<td>Harvard has suggested individuals to change their usernames and passwords. Advantage is offering credit monitoring and call center support through Experian</td>
</tr>
<tr>
<td>Advantage Dental 2015</td>
<td>Unencrypted thumb drive containing protected health information (ePHI) stolen from staff member’s vehicle.</td>
<td>350,000 Customer Records</td>
<td>$150,000 settlement for potential HIPAA/HHS violations. Must implement actions to correct deficiencies in its HIPAA program</td>
</tr>
<tr>
<td>Adult &amp; Pediatric Dermatology Practice 2014</td>
<td>An employee stole customer information on 350,000 clients including account numbers. Files for as many as 900 clients ended up on a website.</td>
<td>2,000 Patients</td>
<td>• The employee has been fired and • MS bank is notifying all of the individuals affected • The FBI is currently investigating the incidence</td>
</tr>
<tr>
<td>Morgan Stanley 2015</td>
<td>Unencrypted thumb drive containing protected health information (ePHI) stolen from staff member’s vehicle.</td>
<td>350,000 Customer Records</td>
<td>• The employee has been fired and • MS bank is notifying all of the individuals affected • The FBI is currently investigating the incidence</td>
</tr>
</tbody>
</table>
## Largest Incidents by Record Volume*

<table>
<thead>
<tr>
<th>Records</th>
<th>Date</th>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>220,000,000</td>
<td>08/22/2014</td>
<td>Unknown Organization</td>
</tr>
<tr>
<td>200,000,000</td>
<td>10/19/2013</td>
<td>Experian</td>
</tr>
<tr>
<td>152,000,000</td>
<td>10/03/2013</td>
<td>Adobe Systems, Inc.</td>
</tr>
<tr>
<td>150,000,000</td>
<td>03/17/2012</td>
<td>Shanghai Roadway D&amp;B Marketing Services Co.</td>
</tr>
<tr>
<td>145,000,000</td>
<td>05/21/2014</td>
<td>eBay</td>
</tr>
<tr>
<td>140,000,000</td>
<td>06/08/2013</td>
<td>Unknown Organization</td>
</tr>
<tr>
<td>130,000,000</td>
<td>01/20/2009</td>
<td>Heartland Payment Systems &amp; Banks</td>
</tr>
<tr>
<td>110,000,000</td>
<td>12/18/2013</td>
<td>Target Brands, Inc. / Fazio Mechanical Services</td>
</tr>
<tr>
<td>109,000,000</td>
<td>09/02/2014</td>
<td>Home Depot, Unknown Organization</td>
</tr>
<tr>
<td>104,000,000</td>
<td>01/20/2014</td>
<td>Korea Credit Bureau</td>
</tr>
</tbody>
</table>

*Source: DataLossDB Open Security Foundation Website, 2015

---

![LOST DATA = LOST PROFITS](image)
**Top 5 Types of Security & Privacy Risks**

- **Physical Loss or Theft**: Lost or stolen laptop, physical file security
- **Employee Mistakes**: IT departments and vendors cannot prevent these types of losses
- **Network Security**: Malware, Trojan Horses, Virus, SQL injection, etc.
- **Cyber Extortion**: Gaining access to confidential/sensitive data and threatening to release it
- **Denial of Service Attack**: A targeted attack with the purpose to slow down or stop a network

*Source: Travelers Cyber Liability Presentation May 2015*

---

**History of Breaches Over Time**

*Source: DataLossDB Open Security Foundation Website. 2015*
How Do Breaches Occur (Frequency)?

- Payment Card Skimmers, 0.1%
- POS Intrusions, 0.7%
- Cyber-Espionage, 0.8%
- Denial of Service, 3.9%
- Web App Attacks, 4.1%
- Miscellaneous Errors, 29.4%
- Crime Ware, 25.1%
- Physical Theft/Loss, 15.3%
- Insider Misuse, 20.6%

*Source: Verizon "2015 Data Breach Investigations Report"

How Do Breaches Occur (cont)-Confirmed Data Breaches?

- Denial of Service, 0.1%
- Payment Card Skimmers, 3.1%
- Physical Theft/Loss, 3.3%
- Miscellaneous Errors, 8.1%
- Web Attacks, 9.4%
- POS Intrusions, 28.5%
- Crime Ware, 18.8%
- Cyber-Espionage, 18.0%
- Insider Misuse, 10.6%

*Source: Verizon "2015 Data Breach Investigations Report"
**Definitions-Personally Identifiable Information**

**Personally Identifiable Information (PII)** - as used in information security and data privacy laws, refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. The types of information normally associated with PII include: (at least three of the following combined)

a) Name and Address (NAA)
b) Date of Birth (DOB)
c) Social Security Number (SSN)
d) Credit Card Number
e) Account Number/PIN or other Financial Account Information
f) Zip Codes? New precedent set by Song-Beverly Act
g) Emails

*Source: Identity Theft Resource Center Data Breach Report 2009*

---

**Definitions-Protected Health Information**

**Protected Health Information (PHI)** - HIPAA regulations define health information as "any information, whether oral or recorded in any form or medium" that:

a) "is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse" and

b) "relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual."

*Source: Identity Theft Resource Center Data Breach Report 2009*
Definitions – Confidential Business Customer Data

1. Trade secret information
2. Confidential financial data
3. Other non-public confidential data of business customers
   i. employee personal data
   ii. payroll data
   iii. billing information
4. Any customer confidential business data subject to a signed Non-Disclosure Agreement (NDA)

Who’s & What’s

Who Has Unauthorized Access
• Hackers
• Anonymous
• Foreign states - China, Ukraine, Russia
• CryptoLocker
• CryptoWall
• WikiLeaks
• Employees, Faculty, Students
• Out-sourced and 3rd Party Vendors
• The Cloud

What Are They Accessing
• Laptops
• Computer Networks / Wireless Networks
• PDAs / Cellphones
• Paper files
• Websites
• Dumpster Diving
• War Driving
• WiFi Networks
• POS
2015 Findings and Implications for Organizations

The cost of data breach increased.
- Average cost of a data breach for an organization represented in the study increased from $5.9 million to $6.5 million.
- The cost per record increased from $201 to $217.

More customers terminated their relationship with the company that had a data breach.
- Companies are losing more customers following a data breach.
- Certain industries, especially financial services and retailers, are more prone to high churn in the aftermath of a data breach.

Malicious / criminal attacks rather than negligence or system issues were the main causes of data breach.
- 47% say the main cause of data breaches were malicious or criminal attack.
- 25% say employee negligence were the main cause of data breaches.
- 29% say system glitches were the main cause of data breaches.

Time to identify and contain data breach affects cost
- Malicious attacks can take an average of 256 days to identify.
- Data breaches caused by human error take an average of 158 days.

The cost of lost business increased from $1.33 million to $1.57 million.
- Costs include: abnormal turnover of customers, increased customers acquisition activities, reputation losses & diminished goodwill.
- The highest cost for lost business was $4.59 million in 2009.
- Average number of records per breach in the U.S. was 28,070.

Certain organizational factors reduced the overall cost.
- Board involvement and purchase of insurance can reduce the cost per record by $5.50 and $4.40 per record, respectively.

Business continuity management reduced the cost of a breach.
- For the first time research reveals having a business continuity management team involved in the remediation of a breach can reduce the cost by an average of $7.10 per compromised record.

*Source: Ponemon Institute, LLC – "2015 Cost of Data Breach Study: Global Analysis"
Additional Findings

- RAM scraping malware was present in some of the high-profile retail breaches
- In 60% of cases attackers able to compromise an organization within minutes
- 23% of recipients now open "phishing" messages and 11% click on the attachment
- 50% open emails and click on "phishing link" within the first hour
- For more than two years, more than two-thirds of incidents involving Cyber-Espionage patterns have featured "phishing"
- Mobile devices are not a preferred vector in data breaches-Android devices more secure than iOS devices
- 70%-90% of malware events are unique to an organization
- Information sharing, compliance and regulatory standards imposed on industry level may not be the best approach-one size does not fit all

*Source: Verizon "2015 Data Breach Investigations Report"

Average Cost of a Data Breach Over Ten Years

*Source: Ponemon Institute, LLC – "2015 Cost of Data Breach Study: Global Analysis"*
Direct & Indirect Per Capita Data Breach Cost Over Ten Years

<table>
<thead>
<tr>
<th>Year</th>
<th>Cost per Record</th>
<th>Indirect Cost</th>
<th>Direct Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>$138</td>
<td>$88</td>
<td>$50</td>
</tr>
<tr>
<td>2007</td>
<td>$182</td>
<td>$128</td>
<td>$54</td>
</tr>
<tr>
<td>2008</td>
<td>$197</td>
<td>$145</td>
<td>$52</td>
</tr>
<tr>
<td>2009</td>
<td>$202</td>
<td>$152</td>
<td>$50</td>
</tr>
<tr>
<td>2010</td>
<td>$204</td>
<td>$144</td>
<td>$60</td>
</tr>
<tr>
<td>2011</td>
<td>$214</td>
<td>$141</td>
<td>$73</td>
</tr>
<tr>
<td>2012</td>
<td>$194</td>
<td>$135</td>
<td>$59</td>
</tr>
<tr>
<td>2013</td>
<td>$188</td>
<td>$128</td>
<td>$60</td>
</tr>
<tr>
<td>2014</td>
<td>$201</td>
<td>$134</td>
<td>$67</td>
</tr>
<tr>
<td>2015</td>
<td>$217</td>
<td>$143</td>
<td>$74</td>
</tr>
</tbody>
</table>

*Source: Ponemon Institute, LLC – “2015 Cost of Data Breach Study: Global Analysis”

Factors Affecting Per Capita Cost of Data Breach

<table>
<thead>
<tr>
<th>Decrease Cost Per Record</th>
<th>Increase Cost Per Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident response team</td>
<td>Consultants engaged</td>
</tr>
<tr>
<td>Extensive use of encryption</td>
<td>Rush to notify</td>
</tr>
<tr>
<td>Employee training</td>
<td>Lost or stolen devices</td>
</tr>
<tr>
<td>BCM involvement (Business Continuity Management)</td>
<td>Third party involvement</td>
</tr>
<tr>
<td>CISO appointed</td>
<td></td>
</tr>
<tr>
<td>Board-level involvement</td>
<td></td>
</tr>
<tr>
<td>Insurance protection</td>
<td></td>
</tr>
<tr>
<td>$12.60 per record</td>
<td>$4.50 per record</td>
</tr>
<tr>
<td>$12.00 per record</td>
<td>$8.90 per record</td>
</tr>
<tr>
<td>$8.00 per record</td>
<td>$9.00 per record</td>
</tr>
<tr>
<td>$7.10 per record</td>
<td>$16.00 per record</td>
</tr>
<tr>
<td>$5.50 per record</td>
<td></td>
</tr>
<tr>
<td>$5.60 per record</td>
<td></td>
</tr>
<tr>
<td>$4.40 per record</td>
<td></td>
</tr>
</tbody>
</table>

*Source: Ponemon Institute, LLC – “2015 Cost of Data Breach Study: Global Analysis”
FTC’s 10 Lessons to Identify Vulnerabilities

1. Start with security
2. Control access to data sensibly
3. Reduce secure passwords and authentication
4. Store sensitive personal information securely and protect it during transmission
5. Segment your network and monitor who’s trying to get in and out
6. Secure remote access to your network
7. Apply sound security practices when developing new products
8. Make sure your service providers implement reasonable security measures
9. Put procedures in place to keep your security current and address vulnerabilities that may arise
10. Secure paper, physical media and devices

*Source: Nixon Peabody Data Privacy Blog, July 22, 2015

If You Do Nothing Else… Take Care of These Things!

1. Have a vulnerability assessment performed to find internal and external gaps
2. Have a written and tested Breach Incident Response Plan
3. Employ anti-virus software on ALL devices/update daily
4. Employ intrusion protection and detection software-update and test regularly
5. Have a tested Disaster Recovery Plan in place
6. Encrypt ALL hard drives, servers, back-up tapes and portable devices
7. Have scans and filters for ALL email attachments
8. Limit remote access to your systems
9. Employ two-factor authentication
10. Employ and enforce continuous employee training for those who collect, use, transmit and dispose of confidential data

*Source: Nixon Peabody Data Privacy Blog, July 22, 2015
Privacy Related Laws

- Personal Data Privacy & Security Act of 2007
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Gramm-Leach-Bliley Act of 1999 (GLBA)
- Fair Credit Reporting Act
- Fair & Accurate Credit Transactions Act of 2003
- Electronic Communications Privacy Act of 1986
- Family Educational Rights & Privacy Act (FERPA)
- State Specific Data Breach Notification Laws*
- High Tech Act (enacted with Jan 2009 Federal Stimulus Package)
- MA GL, 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth of Massachusetts

*Currently 47 states, in addition to the District of Columbia and Puerto Rico, have security breach notification laws.

47 State Now Have Breach Notification Requirement

- Alaska (ALASKA STAT. § 45.48.010 at seq.)
- Arizona (ARI. REV. STAT. ANN. § 44-7201 et seq.)
- Arkansas (ARK. CODE ANN. § 50-1-101 et seq.)
- California (CAL. CIV. CODE § 1798.82)
- Colorado (COLO. REV. STAT. § 6-1-716)
- Connecticut (CONN. GEN. STAT. § 46a-50c)
- Delaware (DELA. CODE ANN. § 29-264.1)
- District of Columbia (DC. CODE § 8-103 et seq.)
- Florida (FLA. STAT. § 630.0715)
- Georgia (GA. CODE ANN. § 16-3-121)
- Hawaii (HAWAII STAT. ANN. § 98-960 et seq.)
- Idaho (IDAHO CODE ANN. § 42-2630 et seq.)
- Illinois (ILL. STAT. ANN. § 5/10-7501)
- Indiana (IND. CODE ANN. § 24-4.9)
- Iowa (IA. CODE ANN. § 13.031)
- Kansas (KAN. STAT. ANN. § 60-447 et seq.)
- Kentucky (KENT. STAT. ANN. § 50-78-101)
- Louisiana (LA. REV. STAT. ANN. § 23:2222)
- Maine (ME. STAT. ANN. § 80-A-301)
- Maryland (MD. STAT. ANN. § 12-405)
- Massachusetts (MASS. GEN. L. ANN. § 450B.1001)
- Michigan (MICH. STAT. ANN. § 445.27)
- Minnesota (MINN. STAT. ANN. § 135E.01)
- Mississippi (MISS. CODE ANN. § 75-20-1)
- Missouri (MISS. CODE ANN. § 75-20-1)
- Montana (MONT. CODE ANN. § 30-14-1704)
- Nebraska (NEB. REV. STAT. ANN. § 37-501 et seq.)
- Nevada (NEV. REV. STAT. ANN. § 230A.010 et seq.)
- New Hampshire (NH. REV. STAT. ANN. § 375-A:19 et seq.)
- New Jersey (N.J. STAT. ANN. § 56A:24-23)
- New Mexico (NM. STAT. ANN. § 74-44-1 et seq.)
- New York (NY. REV. STAT. ANN. § 23-A:1701 et seq.)
- North Carolina (NC. STAT. ANN. § 57-60 et seq.)
- North Dakota (ND. CODE ANN. § 54-05-01 et seq.)
- Ohio (OH. REV. STAT. ANN. § 2931.45)
- Oklahoma (OKLA. STAT. ANN. § 159.37)
- Oregon (OR. STAT. ANN. § 603A.010 et seq.)
- Pennsylvania (PA. REV. STAT. ANN. § 1750.1 et seq.)
- Puerto Rico (PR. CODE. ANN. § 24-527)
- Rhode Island (RI. GEN. LAWS ANN. § 59-11-22 et seq.)
- South Carolina (SC. CODE ANN. § 30-4-170)
- Tennessee (TN. CODE ANN. § 47-18-1 et seq.)
- Texas (TEX. REV. STAT. ANN. § 157.003 et seq.)
- Utah (UT. CODE ANN. § 78B-3-102 et seq.)
- Vermont (VT. STAT. ANN. § 95-207)
- Virginia (VA. STAT. ANN. § 18.2-188.2 et seq.)
- West Virginia (W.VA. STAT. ANN. § 55-2-102)
- Wisconsin (WI. STAT. ANN. § 196.507)
- Wyoming (WYO. STAT. ANN. § 21-1-201 et seq.)

*Currently 47 states, in addition to the District of Columbia and Puerto Rico, have security breach notification laws.
Important Legislation

Hi-Tech Act – part of the 2009 American Recovery and Reinvestment Act, otherwise known as the Stimulus package, the HITECH Act provides incentives for physicians who implement “meaningful use” of an Electronic Health Record system. The “Notification in the Case of a Breach” section contains new requirements, such as:

• Requires notification within 60 days for a privacy breach involving HIPAA covered PHI
• Requires notification to U.S. Dept. of Health & Human Services and media outlets for privacy breaches impacting 500 or more individuals
• Breaches less than 500 must be logged & provided to HHS annually
• Authorizes state attorney generals to bring suit for HIPAA violations

Other Important Legislation

MA GL 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth of MA. Effective March 1, 2010. Consistent with FTC Red Flags Rule, all companies that own, license, store or maintain personal information regarding a MA resident (whether or not the business has a location in MA) must implement an identity theft prevention. This new piece of legislation requires new data protection standards, such as:

• Development & implementation, for all records that contain PII of a MA resident, a “comprehensive written information security program”. (W.I.S.P)
• Utilization of encryption of Personal Information for computer systems, including Laptops, wireless networks & PDA’s.
• Protection of paper documents containing PII using “lock & key” procedures & document retention & destruction procedures.
• Employee training to educate employees on the law and protecting PII
• Failure to comply with the law could cost violators up to $5,000 civil penalty for each violation. What a “violation” constitutes has yet to be defined.
New Developments In Cyber, Security & Privacy

- Data in the Cloud – Data Warehousing, Cloud Applications, Cloud Data Storage
- Mobile App Security – Privacy Issues related to mobile apps and customer data
- Bring Your Own Device (BYOD) – Employees use of personal computing devices (Smart Phones, Tablets, etc.) for business usage
- Geo-Location and Smart Phones – Smart Phones and Tablets with ability to track individuals location via GPS
- SEC Guidelines for Public Companies – Public Companies now have to disclose their Cyber Security Risk Management and Exposure in their public filings
- Cyber Security Executive Order – Increased Government scrutiny of companies for notification of cyber threats and to mitigate cyber security threats
- Song-Beverly Act (CA) and other state laws pertaining to Zip Codes – recent developments have changed the definition of PII to include Zip Codes. Will the definition of PII continue to change?
- "Internet of Things" – network connected consumer products in the household.
- Cyber Terrorism (CryptoLocker & CryptoWall) – small businesses extorted for their data
- Evolution of PII – Changes in what information is considered "personal" (Biometrics, etc.)

Traditional Insurance – How does it respond?

Property and Crime Insurance Policies generally:
- Respond only to loss of or damage to tangible property
- Exclude Indirect or Consequential Loss
- Exclude personal property in the care, custody or control of the insured

General Liability Insurance Policies generally:
- Respond only to loss from Bodily Injury or Property Damage
- Does not apply to 3rd party data liability exposure
- Respond to unambiguous physical injuries to the body (i.e. mental anguish-gray area)
- Respond to personal injury (invasion of privacy) only when it is the direct result of a "publication"
Potential Coverage Overlaps

- Errors & Omissions (E&O) Insurance may have some overlap or grey areas of coverage for specific professional firms, such as, tech companies, law firms & accountants. In many cases, there is an implied duty to protect customer information. However, E&O policies are not designed to specifically cover Cyber & Privacy exposures. Stand-Alone Cyber & Privacy coverage is needed to pick up key First Party & Third Party coverages not available in E&O policies.

- Directors & Officers Liability (D&O) policies may provide protection for specific exposures, such as, suits by investors against D’s & O’s for failing to disclose cyber security risks or failing to disclose the nature and scope of the costs of a data breach. However, D&O policies are not designed to cover specific Cyber & Privacy Coverage grants.

- Commercial Crime – Most Cyber & Privacy policies do not cover fraudulent transfer or wire transfer of funds or actual theft of funds. Crime policies can include Wire Transfer Fraud and Computer Systems Coverage.

- Coordination of Coverage – A comprehensive review of all policies in an Insured’s Insurance Portfolio should be reviewed to properly assess where coverage may be available.

Insurance Carriers

1. ACE USA
2. AIG/Chartis
3. Admiral
4. Allied World (AWAC)
5. Arch
6. Argo Pro/Colony
7. Aspen
8. AXIS
9. Beazley USA
10. Brit Syndicate
11. Capitol Insurance
12. CHUBB
13. C.N.A
14. Crum & Forster
15. Digital Risk Managers
16. Endurance Specialty
17. E-Risk Services
18. Euclid
19. Evanston Insurance
20. Freedom Specialty
21. Great American / ThinkRisk
22. Hartford Ins.
23. Hiscox
24. IronShore
25. Kiln Syndicate
26. Liberty
27. LLOYDS (various syndicates)
28. NAS/Lloyd's
29. Navigators Insurance
30. One Breach
31. Philadelphia Ins.
32. QBE Specialty
33. RLI Insurance
34. RSUI Group
35. SafeOnline
36. Starr Indemnity
37. Travelers
38. Torus Specialty
39. XL Professional
40. Zurich American
FBinsure’s Cyber Practice Leader

Ed McGuire  
Director of Specialty Insurance  
Main: 508-824-8666  
Direct: 508-659-8185  
Mobile: 978-844-7720  
Email: emcguire@fbinsure.com  
Web: www.fbinsure.com