




Cyber Liability - Where are We and Where are We Headed? Legislation, Litigation and Crisis Management

PLAN Regional Meeting:
New York '14
Wednesday, June 18, 2014

Data Breaches by the Numbers

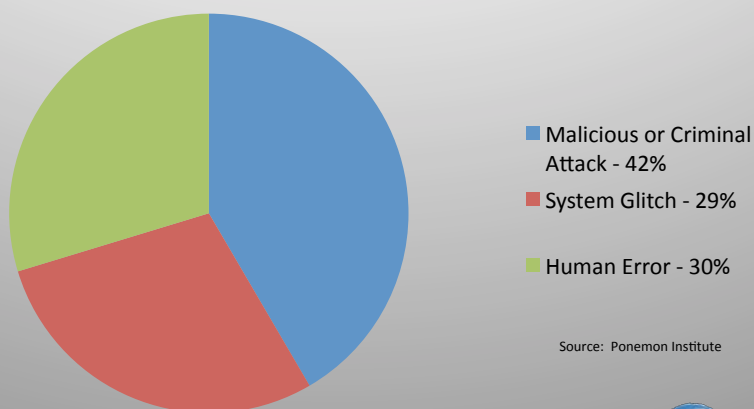
- Average number of records involved– 29,087
- Average organizational cost - \$5.85 Million
- Average detection and escalation costs - \$417,700
- Average notification costs - \$509,237
- Average post breach costs - \$1,599,996
- Average lost business costs - \$3,324,959

Source: Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis



Data Breach Causes

Root Causes



Source: Ponemon Institute



Cyber Insurance by the Numbers

- Total Cyberinsurance premiums paid in 2013 - \$1.3 Billion

Source: Nicole Perloth and Elizabeth A. Harris, "Cyberattack Insurance a Challenge for Business," New York Times (June 8, 2014)

- 2014 Cost of Data Breach Study
 - Only 32% of participants have data breach protection or cyber insurance policy
 - 54% of those with policy are satisfied with coverage



Data Security Breach Class Action Litigation and the Standing Defense



Standing

- Article III – “case” or “controversy”
- Actual identity theft, fraudulent charges (*AvMed*)
- Vast majority of potential plaintiffs will not have this, try to create standing through other alleged injuries:
 - Increased risk of identity theft
 - Time and effort to mitigate potential identity theft
 - Credit monitoring expenses
 - Emotional distress
 - Deprivation in the value of personal information



***Clapper v. Amnesty Int'l USA,* 133 S. Ct. 1138 (Feb. 26, 2013)**

- Amendments to FISA; Plaintiffs alleged communications being chilled, increased travel expenses
- Supreme Court: No standing, injury not “certainly impending”
- “[W]e have repeatedly reiterated that threatened injury must be certainly impending to constitute injury in fact, and that allegations of possible future injury are not sufficient.” The Court held plaintiffs also cannot “manufacture standing” by incurring expenses to mitigate against non-imminent harm.



The issue now: Did *Clapper* change the analysis?

Maybe: *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588, at *3-6 (N.D. Ill. Sept. 3, 2013)

- Facts: Skimmers potentially stole customer credit and debit information by tampering with PIN pad devices
- Posture: Motion to dismiss for lack of standing
- Standard: Plaintiff must have injury in fact that is fairly traceable to the action of the defendant that will likely be redressed with a favorable decision – injury that is certainly impending may satisfy this standard, but possible future injury will not.
- Result: Dismissed - Allegations of untimely notification, breach of statute, improper disclosure of PII, and loss of privacy did not satisfy standing because these harms do not equate to disclosure; allegations of expenses incurred to mitigate risk of identity theft did not satisfy standing because those expenses were not alleged with specificity and because those expenses could merely be manufactured injury; allegations of emotional distress and diminished value of products and services could not be proven.



The issue now: Did *Clapper* change the analysis?

Tabata v. Charleston Area Med. Center, 2014 WL 2439961 (W. Va. App., May 28, 2014)

- *Facts: Plaintiff alleged Defendant was responsible for placing personal medical information on a database accessible to the public*
- *Posture: Appeal from order denying class certification and finding no standing because named Plaintiff sustained no actual injury or economic loss*
- *Result: Order reversed because Plaintiff has a legal interest in having their medical information kept confidential. When a medical provider violates this interest, it is an invasion of that interest sufficient to satisfy standing. Class certification order reversed because all of the class members were in exactly the same position, and, because no injury (other than invasion of privacy interest) was alleged, there are no varying injury allegations outside of the common injury to the class' privacy interest.*



The issue now: Did *Clapper* change the analysis?

Regents of the Univ. of California v. Superior Court (Platter) (2013) 220 Cal.App.4th 549, *as modified on denial of reh'g* (Nov. 13, 2013)

- *Facts: Plaintiff alleged theft of a computer hard drive from a hospital.*
- *Posture: On appeal from dismissal/demurrer*
- *Result: Reversed and case dismissed without leave to amend because CMIA section 56.36 allows a private right of action for negligent maintenance only when such negligence results in unauthorized or wrongful access to the information.*



The issue now: Did *Clapper* change the analysis?

Eisenhower Med. Center v. Superior Court, 2014 WL 2115216 (Cal. App. 4 Dist., May 21, 2014)

- Facts: Plaintiff alleged computer stolen from EMC containing names, medical record numbers, age, date of birth, and last four digits of SSNs.
- Posture: Appeal from denial of summary adjudication for hospital.
- Result: Dismissal upheld because patient identifying information stolen from hospital was not “medical information” covered by CMIA.



Policies and Coverage



Data Privacy and Network Security: A Multi-Threat Environment

Technology

- Viruses, SQL Injections, DDoS attacks, etc.
- Structural vulnerability
- Social Media/Networking
- Phishing

External

- Business Associates
- Vendors/Suppliers (contractors, outside counsel, cloud providers)
- Foreign and domestic organized crime
- Hackers/Hacktivists

Internal

- Rogue employees
- Careless staff
- BYOD



Old School

- Laptop theft
- Dumpster diving
- Photocopier

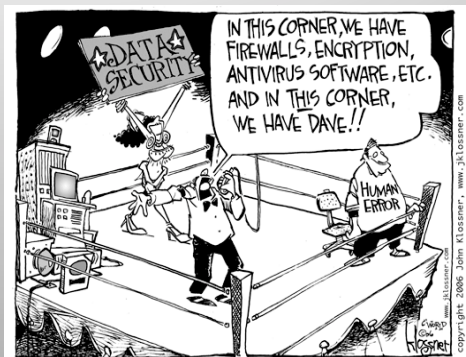
Regulatory

- HHS, HIPAA & HIPAA HITECH
- Identify Red Flags
- SEC, FTC, state attorney generals
- 48 State breach notification laws (NM proposed)
- PCI Compliance



The Weakest Link

- ✓ **Unintended disclosure** was responsible for 29% of incidents reported by agencies over the last three years (Most common type of breach)
- ✓ **Loss or theft of portable devices** exposed more than 80 million records, **86% of that total. number of records exposed**





Sample Insurance Gap Analysis







■ Not Covered
 ■ Covered
 ■ Dependent upon specifics of claims, may not be covered

Privacy & Cyber Perils	Property	General Liability	Traditional Fidelity Bond	Computer Crime	E&O	Special Risk	Broad Privacy & Cyber Policy
Destruction, corruption or theft of your electronic information assets/data due to failure of computer or network	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Theft of your computer systems resources	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Business Interruption due to a material interruption in an element of your computer system due to failure of computer or network security (including extra expense and forensic expenses)	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Business interruption due to your service provider suffering an outage as a result of a failure of its computer or network security	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Indemnification of your notification costs, including credit monitoring services	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Defense of regulatory action due to a breach of privacy regulation	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Coverage for Fines and Penalties due to a breach of privacy regulation	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Threats or extortion relating to release of confidential information or breach of computer security	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Liability resulting from disclosure of electronic information & electronic information assets	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Liability from disclosure confidential commercial &/or personal information (i.e. breach of privacy)	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered
Liability for economic harmed suffered by others from a failure of your computer or network security (including written policies & procedures designed to prevent such occurrences)	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Not Covered	Covered

Note: All insurance coverage is subject to the terms, conditions, and exclusions in the applicable individual policies.



Available Cyber Coverage

-  **Network Security Liability:** 3rd party liability resulting from a failure of your network security to protect against destruction, deletion or corruption of a 3rd party's electronic data, denial of service attacks against Internet sites or computers; or transmission of viruses to third party computers and systems.
-  **Privacy Liability:** Liability to a 3rd party as a result of your failure to properly handle, manage, store or otherwise control personally identifiable information, corporate information identified as confidential and protected under a nondisclosure agreement and unintentional violation of privacy regulations.
-  **Crisis Management & Identity Theft Response Fund:** Expenses to comply with privacy regulations, such as communication to and credit monitoring services for affected customers. This also includes expenses incurred in retaining a crisis management firm for the purpose of protecting/restoring your reputation as a result of the actual or alleged violation of privacy regulations.
-  **Cyber Extortion:** ransom or investigative expenses associated a threat directed at you to release, divulge, disseminate, destroy, steal, or use the confidential information taken from the Insured, introduce malicious code into the your computer system; corrupt, damage or destroy your computer system, or restrict or hinder access to your computer system.
-  **Network Business Interruption:** reimbursement of your own loss of income &/or extra expense resulting from an interruption or suspension of its systems due to a failure of network security to prevent a security breach.
-  **Data Asset Protection:** recovery of your costs and expenses incurred to restore, recreate or regain access to any software or electronic data from back-ups or from originals or to gather, assemble and recreate such software or electronic data from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction, deletion or damage.



What Are the Gaps in Traditional Policies?

Traditional insurance does not respond to all cyber liability.

- **Errors and Omissions (E&O):** Even broadly worded E&O policies remain tied to “professional services” and often further tied to a requirement that there be an act of negligence
- **Commercial General Liability (CGL):** CGL covers only bodily and tangible property—Advertising Injury / Personal Injury (AI/PI) section has potential exclusions/limitations in the area of web advertising
- **Property:** Courts have consistently held that data isn't “property”— “direct physical loss” requirement not satisfied
- **Crime:** Requires intent and only covers money, securities, and tangible property
- **Kidnap and Ransom (K&R):** no coverage without amendment for “cyber-extortion”



Information Risk Insurance Marketplace

- Robust market with \$350MM of market capacity for liability (third party)
- \$200MM for Business Interruption (first party)
- Recent Innovations
 - Turnkey breach management approach
 - Pre-loss control services



Data Breach Response



Agenda

2013 & 2014 Attacks Disrupt Breach Response Plans

What should a good breach response plan include?

Questions to Ask Your Clients



2013 & 2014 Attacks Disrupt Breach Response Plans

Breach response planning should no longer assume that:

1. Antivirus will catch most if not all attacks.
2. Breaches may not occur because vendors must follow your client's information security plan.
3. Outdated software may cause a breach since it can not be upgraded or patched to prevent attacks.
4. Distributed Denial of Service (DDOS) attacks upon your brochure website is only a nuisance.



What should a good breach response plan include?

Breach response plans must adapt to the last 2 years of successful and highly publicized attacks:

Assume that virtually any client you underwrite or represent can and will be breached.

A viable breach response plan would include the ability to:

- Detect, stop and contain attacks using access you provide to your vendors.
- Pinpoint and replace outdated software intruders utilize to break in.
- Allow you to re-direct and manage traffic away from websites that are subjected to DDOS.



Questions to Ask Your Clients

When was your breach response plan last updated?

Does the plan address working with critical vendors who play a role in providing critical services?

Does the vendor have a breach response plan?

Does the vendor have access to your client's network?

Do you have in place a process to locate and remove software that is no longer supported or can not be patched?

Does the plan address working with web content providers and any parties who manage web traffic?



Summary

Successful intrusions and attacks over the past 2 years have changed the information security landscape.

Prior assumptions about antivirus software can no longer be relied upon as a factor in preventing attacks.

Insurers and legal professionals should inquire to determine if breach response plans have been updated for:

- Identification and replacement of outdated software.
- Drive by attacks
- DDOS attacks on website
- Attacks on vendors who are allowed in your network.



New York and New Jersey Notification and Disposal Statutes





Notification

- General Business Law: Ch 20, Art. 39-F §899-aa
- Applies to a very narrow set of *computerized* data
 - Unauthorized person **acquired** “personal information”
 - Information that can identify a person like:
 - Name,
 - Number, or
 - Other identifier.
 - **PLUS** “private information”
 - Which includes one or more of the following:
 - Social Security Number;
 - Driver’s License Number or Non-Driver ID Number;
 - Account Number, Credit/Debit Card Number **PLUS**
 - » Related Passwords or PINs



Notification

- Once unauthorized person gets the information:
 - **First** contact the **State Police**
 - They will tell you to notify the victims or to wait
 - **Next** contact **Attorney General** and **Department of State**
 - **Then**, once the police say it’s okay, **notify the victims** by:
 - Written Notice;
 - Telephone Notice; or
 - Electronic Notice *if the victim has previously okayed e-notice.*
- If you’ve lost **more than 500,000 records**, or
 - It will cost **more than \$250,000** to notify victims, or
 - You don’t have **sufficient contact information** then
 - You can use substituted notice.





Notification

- If you've lost more than 5,000 records
 - **Notify the consumer reporting agencies**
 - Attorney General will have a list
- Limited Protection
 - No **regulatory guidance**.
 - **PII** must be **acquired** not just **accessed**.
 - **Biometric data** not covered.
 - **Health records** not covered.
 - **Zip codes** and **email** not covered.
 - **Physical records** not covered.



Disposal & Trends

- General Business Law: Ch 20, Art. 39-F §399-h
Disposal of Records
 - **Physical records** or **backup tapes/disks** with PII
 - **Shredded** before disposal; or
 - PII contained in record **destroyed**; or
 - Modifies record to make PII **unreadable**; or
 - Takes "**commonly accepted industry practices**" to ensure no unauthorized access to PII.
 - No guidance on **electronically stored PII**
- Legislative, regulatory and judicial trends moving towards **greater protection**.





Trends

- Business that acquires “highly sensitive information” undertakes a covenant to safeguard it. **Business breaches a fiduciary duty if it fails.**
 - *Daly v. Metropolitan Life Ins. Co.*, 782 N.Y.S.2d 530, 535 (Sup.Ct.N.Y.Cty.2004)

- **Releasing confidential information** to third parties **without safeguards** is a breach of fiduciary duty.
 - *U.S. v. District Council of NYC*, 90 Civ. 5722, 2013 WL 2451737 *6 (S.D.N.Y. June 5, 2013)



Notification

- **N.J.S.A. 56:8-163** Disclosure of Security Breach
- Applies to even narrower set of *computerized* data
 - Unauthorized **access to** “personal information”
 - **First Name** or Initial and **Last Name**
 - **PLUS** one or more of the following:
 - Social Security Number;
 - Driver’s License Number or State Identification Number;
 - Account Number, Credit/Debit Card Number **PLUS**
 - » Related Passwords or PINs
 - Note **absence** of New York’s “other number” element.





Notification

- After **discovery** or **notification** of unauthorized access:
 - **First** determine if disclosure is necessary
 - Misuse of the information is not reasonably possible
 - Keep written record of determination for 5 years.
 - *If you have to disclose, then* contact the **State Police**
 - They will tell you to notify the victims or to wait
 - **Then**, once the police say it's okay, **notify the victims** by:
 - Written Notice; or
 - Electronic Notice *that is consistent with Electronic Signatures in Global and National Commerce Act" (15 U.S.C. s.7001)* .



Notification

- If you've lost **more than 500,000 records**, or
 - It will cost **more than \$250,000** to notify victims, or
 - You don't have **sufficient contact information** then
 - You can use substituted notice.
- If you've lost more than 1,000 records
 - **Notify the consumer reporting agencies**
 - As defined by subsection (p) of section 603 of the federal "Fair Credit Reporting Act" (15 U.S.C. s. 1681a)





Notification

- Limited Protection
 - No **regulatory guidance** – **defeated in 2009**
 - **Identification numbers** not covered.
 - Passport
 - Medicare / Medicaide ID
 - Federal / Military ID
 - Prisoner Number
 - **Biometric data** not covered.
 - **Health records** not covered.
 - **Zip codes** and **email** not covered.
 - **Physical records** not covered.



Disposal

- N.J.S.A. 56:8-162 **Disposal of Records**
 - **Any material, regardless of physical form**, that has personal information **recorded** or **preserved shall be destroyed** by:
 - **shredding**; or
 - **erasing**; or
 - Otherwise modifying the personal information to make it **unreadable, undecipherable** or **nonreconstructable**.
- **Covers** electronically stored personal information.





Trends

- No cases interpreting this statute



Questions and Answers

