

CYBER RISK INSURANCE: Quantifying the Exposure

Eduard Goodman, J.D., LL.M., CIPP-US/C/E
Chief Privacy Officer



Protecting Identities. *Enhancing Reputations.*

A cyber event can take an organization that looks like this:



And leave it looking like this:



Cyber threat risk management



Key issues to hone in on for insurers looking to measure and look at policyholder 'cyber' risks they may or may not have considered:

- Data Breach Exposure Risks (or '9 ways to lose data')
- Vendor Risks
- Franchise Risks
- Payment Card System/Point of Sale equipment and management
- Data Ransom
- Wire Transfer /EFT Fraud
- Social Engineering

What is a data breach? (Generally)

A data breach is any exposure of private or confidential information held by an entity (business, government entity, etc.). This exposure could be through loss, theft or other method of exposure. This data can include:










- Confidential Company Data such as:
 - Business plans
 - Client lists

- Private Personal information such as:
 - Personally Identifiable Information
 - Protected Health Information
 - Account Information

What is a data breach? (Private Personal)

YOUR PII CHART™

LEGEND

-  **SOCIAL SECURITY NUMBER**
-  **CONTACT INFORMATION**
(email address, physical address, telephone and mobile numbers)
-  **GOVERNMENT-ISSUED IDENTIFICATION**
(driver's license, passport, birth certificate, library card)
-  **BIRTH DATE, BIRTH PLACE**
- WWW**  **ONLINE INFORMATION**
(Facebook, social media, passwords, PINs)
-  **GEOLOCATION**
(smartphone, GPS, camera)
-  **VERIFICATION DATA**
(mother's maiden name, pets' and kids' names, high school, passwords)
-  **MEDICAL RECORDS INFORMATION**
(prescriptions, medical records, exams, images)
-  **ACCOUNT NUMBERS**
(bank, insurance, investments, credit cards)

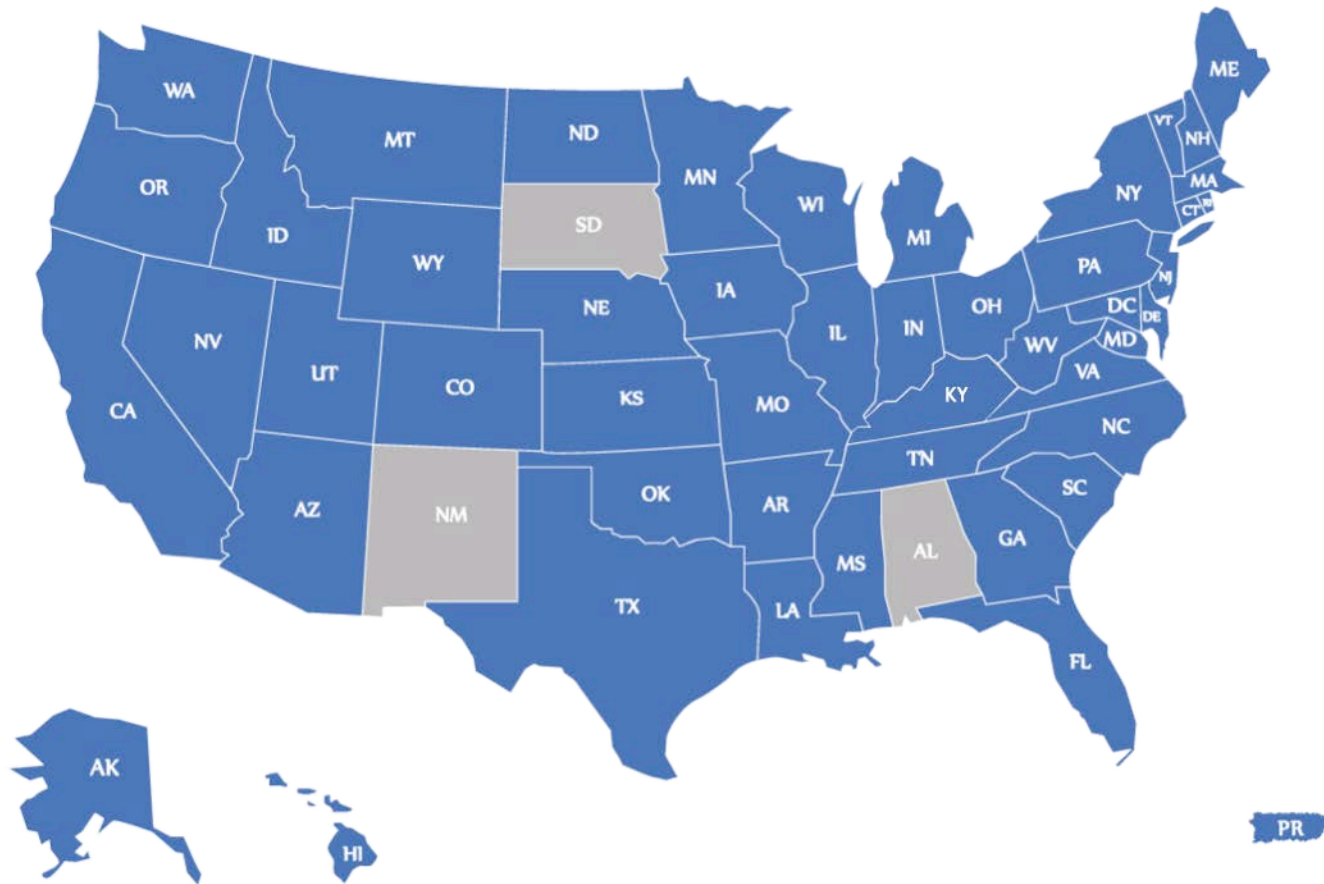




Under state breach notification laws, businesses must notify consumers if there has been a breach that exposes their unencrypted Personally Identifiable Information (PII).

What is a data breach?

47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands require notification of security breaches involving PII



Compromised System or Network (Hacking)

Situation: Policyholder reports that a computer or network housing PII has been compromised

Possible Scenarios

- Computer system has a virus, spyware, “bot” or Trojan horse
- Company Wi-Fi (wireless) network improperly secured or left open
- System has been hacked or accessed

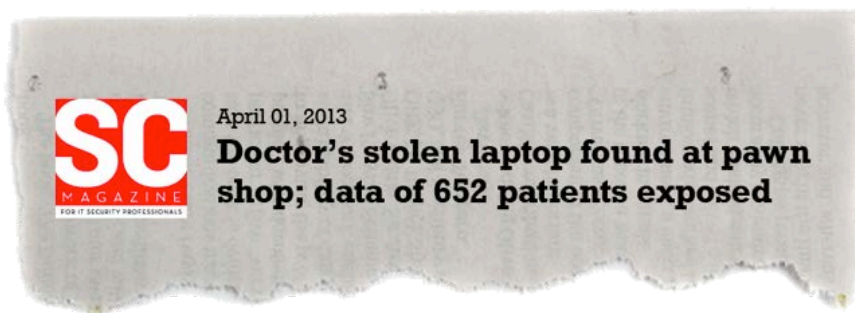


Missing or Stolen Laptop/Storage Device

Situation: Policyholder reports a missing computer device storing Personally Identifiable Information (PII), such as a laptop, USB flash drive or portable hard drive

Possible Scenarios

- Laptop stolen from a parked vehicle at the mall
- Luggage containing a laptop or portable storage device fails to arrive at destination
- Laptop or portable storage device stolen from a place of business or a home office

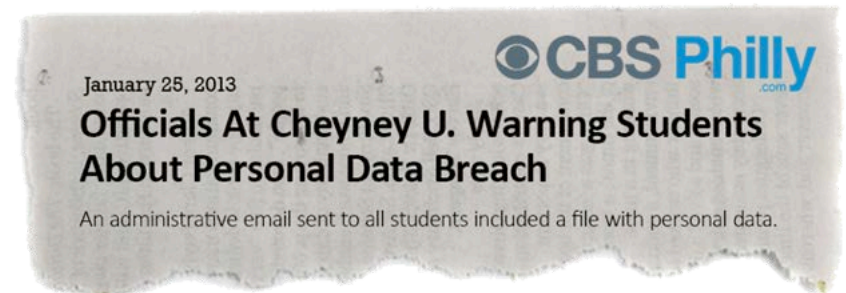


Mis-mailing

Situation: Policyholder reports that documents with one person's PII were mistakenly sent to someone else

Possible Scenarios

- Documents faxed to the wrong number
- Bill, statement of benefits, or other documents sent to wrong person or address
- Attachments containing PII emailed to incorrect recipient

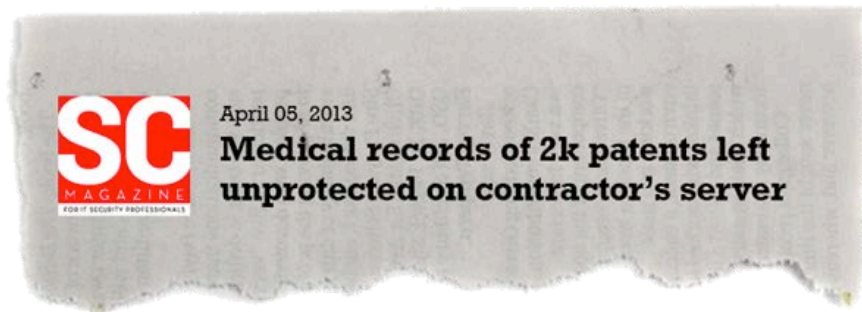


Erroneous Data Posting

Situation: Policyholder posts or prints PII in a public venue

Possible Scenarios

- Erroneous web site posting
- Failure to redact PII that may become public record prior to submission to a government entity



Loss or Theft of Physical Documents

Situation: Policyholder reports that paper documents containing PII were lost, stolen or exposed

Possible Scenarios

- Shipped documents fail to arrive at destination
- Documents improperly exposed due to flood, hurricane, tornado or other disaster
- Documents stolen or missing from premises following a break-in



Lost Back-up Data or Tape

Situation: Policyholder loses back-up data containing PII

Possible Scenarios

- Remote online storage service used by Policyholder suffers data security breach
- Back-up data tape being shipped to co-location facility is lost or missing
- Custody chain and access of back-up data tape is uncertain due to temporary loss and subsequent recovery of tape

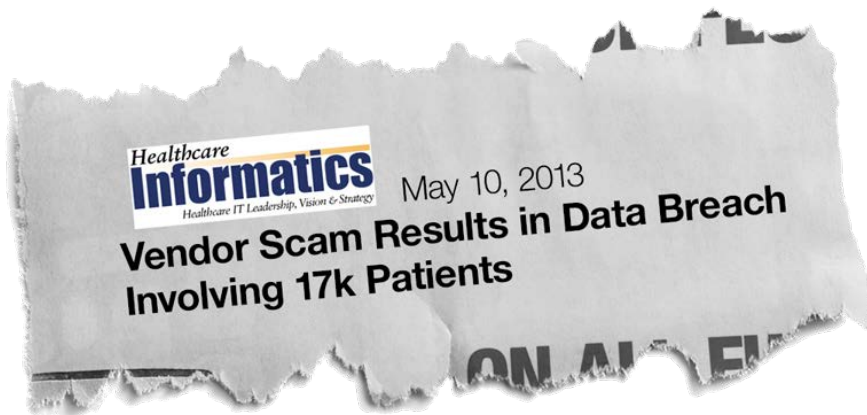


Breach Caused by a Third Party Vendor

Situation: Policyholder utilizes an outside vendor for services that involve PII or PHI of the Policyholder's customers, clients or employees and the vendor had a breach

Possible Scenarios

- Payroll processor or benefits provider suffers a breach that exposes employee PII
- Business process vendors lose data while handling PII for Policyholders

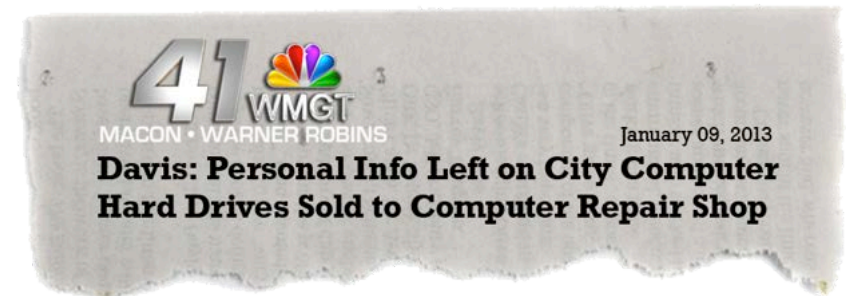


Improper Document/Equipment Disposal

Situation: Policyholder improperly disposes of documents or equipment that contain PII or PHI of the Policyholder's customers, clients or employees

Possible Scenarios

- Backup data tape submitted for destruction is unaccounted for
- Documents and/or document destruction storage areas are left unsecured
- Documents/equipment containing PII are improperly disposed of or are recycled or left exposed



Insider

Situation: Policyholder reports that an employee or contractor accessed files containing PII for reasons unrelated to their job function

Possible Scenarios

- A disgruntled employee announced his resignation and then was caught copying files from his computer to a flash drive
- A curious employee accessed his co-workers HR files



Franchisor



This would cover entities that provide some level of control over their franchisees' systems (card payment, property management, Point of Sale, Inventory management, etc.) as a part of the Franchise relationship under and pursuant to a Franchise agreement and payment of franchise fees.

NOTE: The estimated number of Franchise businesses in the U.S. varies between 750,000-900,000

Common Franchisors include industry specific players but could be made up of:

- **Hospitality (National chains of Hotels, Motels, etc.)**
- **Restaurants (fast food, sit down, food service, etc.)**
- **Home based businesses (Peer to peer or 'party' selling)**

PCI/EMV Issues



If you accept payment cards of any sort (Visa, Mastercard, Discover, AmEx, etc.) you need to look to your risks and liabilities associated with this payment method.

Consider the liabilities and costs regarding:

- **POS and Terminal management**
- **Whether your organization or someone else is actually managing and processing the cards**
 - **Determine what obligations your vendors have if there is a situation**



Data Ransom/DDoS Extortion Threats

Ensuring that your company's operational information is properly backed up regularly (and not simply overwritten with each backup) AND that full back up and restoration has been TESTED are very important for a number of situations.

Operational data/system backup is necessary for 'ransom-ware' threat minimization :

- **For business continuity**
- **To be able to easily recover from a data ransom situation**
- **To be able to easily identify any impacted data subjects (customers, patients, clients, employees, etc.) whose personal data may have been accessed or acquired in a breach**

DDoS Threat mitigation strategies should be considered for any businesses that have a potential website/network threat potential:

- **Municipalities**
- **Online retail**
- **Online Gaming**
- **Political organizations/non-profits**
- **Any organization in 'contentious opinion' industries or areas**

Social Engineering and Wire Transfer Protocols and Risks



Ensuring that your organization and your financial institutions have a set of pre-ordained processes and protocols around electronic funds transfers. This includes establishing authorized users and protocols with your bank on verification and methods of request. Also ensuring that accounting and HR individuals are trained to question requests for employee W2 and tax forms as well as other documents.

Things to consider:

- Wire Transfer transactions are looked at as *cash* transactions and once performed that 'bell' can't be un-rung
- Most socially engineered data breaches and wire transfer fraud losses are carried out using the organizations hierarchal structure and capitalizing on the power dynamic in management



Concluding Thoughts



Thank you

Eduard Goodman, J.D., LL.M., CIPP-US/C/E

Chief Privacy Officer

Scottsdale, Arizona

480.355.4940 direct

EGoodman@IDT911.com