VERITEXT LEGAL SOLUTIONS

Data Security Breach!

Preparing for and Responding to The Inevitable Data Breach

HB LITIGATION CONFERENCES

Northeast Corporate Counsel Forum 2016

April 21, 2016 | Atlantic City

Speakers

Kathleen Barnett Einhorn
Genova Burns
keinhorn@genovaburns.com

Nicholas S. Goldin
Simpson Thacher & Bartlett LLP
ngoldin@stblaw.com

Austin P. Berglas
K2 Intelligence
aberglas@k2intelligence.com

Introduction – Cybersecurity: A Growing Threat

- Experts say that there are two types of companies in the United States:

> "Those that have been hacked and those that don't know they've been hacked."

  - Data breaches have become ubiquitous, affecting the local car wash to the multi-national corporation, and the absolute size of these data breaches has been increasing exponentially.

Introduction – Cybersecurity: A Growing Threat (*cont'd*)

- **Number of Breaches/Incidents**:

2,122
- Confirmed Data Breaches in 2014 (across 61 countries)*

28,070
- Average Number of Breached Records in the U.S.**

79,790
- Reported Security Incidents in 2014 (across 61 countries)*

* 2015 Verizon Report
** Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis / 2015 Cost of Data Breach Study: United States.

Introduction – Cybersecurity: A Growing Threat (*cont'd*)

- **Average Cost Per Data Breach for a U.S. Company: $6.53 million**

$610,000

- **Average Detection & Escalation Costs Per Breach** (*e.g.*, forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors)

$560,000

- **Average Notification Cost Per Breach** (*e.g.*, IT activities associated with creation of contact databases, determination of regulatory requirements, engagement of outside experts, postal expenditures)

$1.64 million

- **Avg. Post-Data Breach Cost** (*e.g.*, investigative activities, remediation, legal fees, product discounts, identity protection services)

$3.72 million

- **Average Lost Business Cost Per Breach** (*e.g.*, abnormal turnover of customers, increased customer acquisition activities, reputational losses, diminished goodwill)

Source: Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis / 2015 Cost of Data Breach Study: United States.

Introduction – Cybersecurity: A Growing Threat (*cont'd*)

Other Factors to Consider With Regard to Costs.

- ***Average Costs Rise Significantly With the Size of the Breach.***
  - U.S. companies that had data breaches compromising between 25,001 and 50,000 records spent an average of **$9.12 million**, and companies that had data breaches compromising over 50,000 records spent an average of **$11.92 million**.
- ***Potential Additional Costs.***
  - The above costs do not take into account potential litigation and settlement costs or potential regulatory settlements.

State Legislation: Data Breach Notification

- ***47*** states, as well as the Dist. of Columbia, Guam, Puerto Rico, and the Virgin Islands, currently have legislation requiring private or government entities to notify individuals of security breaches of information involving PII.
  - While the specifics of laws differ depending on the state, these laws typically:
    - provide which entities must comply with the law;
    - define "personal information" (*e.g.*, name + SSN, drivers license or state ID, account numbers, etc.);
    - define what constitutes a breach;
    - outline the notice requirements (*e.g.*, timing or method of notice and who must be notified); and
    - provide any exemptions (*e.g.*, for encrypted information).
  - States without data breach notification laws: Alabama, New Mexico, and South Dakota.

Types of Data Breaches

- Physical Breach
  - Physical theft of documents, computers, laptops, portable electronic devices, electronic media, paper files
  - Examples: Theft, Improper Disposal of Data, Unauthorized Access to Physical Systems, Improper Sharing of Data
- Electronic Breach
  - Unauthorized or deliberate attack to a network or computer system
  - Examples: Phishing, Network Intrusion, Hacking, Malware, Viruses
- Skimming
  - Installation of an external device to collect sensitive data
  - Examples: Credit Card Scanners

Common Data Vulnerabilities

- ***Improper Physical Security***
  - Office Security
  - Improper Computer Security (Lack of Firewalls, Anti-Virus Software, Intrusion Detection)
  - Unsecure Devices (Cell Phones, Ipads, Laptops, Remote Terminals/Access)
- ***Employees/ Internal Threats***
  - Untrained Employees
  - Disgruntled/ Terminated Employees
- ***Web Access Policies***
- ***Cloud Storage***
- ***Third-Party Service Providers/Vendors***

Common Causes of Data Breaches

- ***Hacking***
  - ***Weak or Stolen Credentials***
    - ***Stolen Passwords***
    - ***Cracking Tools***
    - ***Brute Force Attacks***
- ***Denial of Services Attacks***
- ***Physical Theft/Loss***
- ***Human Error***
  - ***Sending information to wrong recipient***
  - ***Publishing nonpublic data to public web server***
  - ***Improper disposal of data***
- ***Employee/Insider Breaches***
- ***Crimeware (Non-POS or cyberespionage attacks)***
  - ***Malware, Spyware/Keylogger attacks***
- ***Point of Sales (POS) Intrusions***
- ***Cyber Espionage***

Source: 2015 Verizon Report

.

Practical Tips

- **No "One Size Fits All" Approach.** While there is no "one size fits all" approach for all companies, here are **10 tips** that apply across the board to ensure that an organization is taking reasonable measures to **prevent, detect, and respond to** a data breach.

1. Leadership

- Each company should identify a senior person with clear responsibility for organization-wide security preparedness, who has support from the top of the organization.

2. Budget and Staffing

- Management needs to give serious consideration to how much of the budget and how much staff is adequate for proper cyber risk management.
  - Within the overall cyber budget, management should prioritize the allocation of funds in accordance with relative risk.

Practical Tips (*cont'd*)

3. Adopt Written Cybersecurity Program

- Organizations should formulate a comprehensive, written privacy and cybersecurity program consisting of reasonable and appropriate policies and procedures.
- As an initial matter, to create a robust cybersecurity program, an organization needs to:

(a) know where its data resides and who is accessing it

- Without knowing where information is stored and which custodians have access to it, the organization will face significant hurdles in adequately safeguarding this data.

AND

(a) understand each potential cyber risks/vulnerability it faces that could result in a hack and the gravity of those risks.

- Without performing this mandatory risk analysis, an organization cannot draft a risk management plan aimed at reducing risks and vulnerabilities to a reasonable and appropriate level, nor can it allocate its budget appropriately.
- In addition to cyber attacks, organizations face other cyber risks that could be significant (*e.g.*, misuse by current/departing employees, lost/stolen unencrypted devices, server vulnerabilities).

Practical Tips (*cont'd*)

- ***Hallmarks of a comprehensive privacy and cybersecurity program***. While cybersecurity programs differ depending on the organization's facts and circumstances, a robust program will:
  - Ensure that the organization monitors to avoid collecting and storing non-essential customer data;
  - Ensures that data is destroyed responsibly after it has outlived its business purpose;
  - Identify how access credentials are selected and allocated within the company;
  - Indicate the measures the company takes to protect against the downloading of malicious data;
  - Include policies and procedures for password creation and encryption of PII;
  - Specify additional security measures the organization implements and maintains to secure its data and safeguard PII in transmissions; and
  - Indicate the measures the company takes to reduce the risk that PII will be transferred from its internal network to the outside internet.
- The cybersecurity plan should be **reviewed and tested at least annually** (whether by an independent third party or in-house).

Practical Tips (*cont'd*)

4. Employee Training and Education

- Organizations should institute effective training programs that instruct employees on the appropriate handling and protection of PII.

5. Business Associates and Other Third-Party Vendors

A state-of-the-art cybersecurity program is less valuable if the organization's vendors that have access to the PII do not have similarly robust programs.

- For **vendors that do not need access to PII** to perform their job duties, organizations should ensure that they properly segment the parts of the network accessible to those vendors and the parts that house PII.

Practical Tips (*cont'd*)

- For **business associates** (which perform functions or provide services to covered entities that involve access to or use of PII), entities should restrict their access only to servers/information they need to do their job. In addition:
  - Prior to entrusting a business associate with PII, an organization should **ensure that the business associate will properly handle and secure PII** by, for example:
    - conducting due diligence regarding business associate's compliance with relevant statutes;
    - reviewing business associate's security policies; and
    - ensuring business associate is aware of and adheres to covered entity's information security policies.
  - **Contracts with business associates:**
    - should clearly provide that business associate will comply with applicable statutory requirements to safeguard PII that is created, received, maintained, or transmitted on behalf of covered entity;
    - should note whether business associate will subcontract any services to other vendors and, if so, require business associate to ensure that, to extent such subcontractors receive access to PII, they comply with applicable statutory requirements; and

.

Practical Tips (*cont'd*)

6. Legal Compliance and Regulatory

- Organizations should ensure that they have an effective system in place for staying abreast and complying with evolving federal, state, and international data security laws and regulations that are applicable to their operations.

7. Insurance

- Organizations should consider purchasing cyber liability insurance. In today's environment, it is no longer acceptable to forgo looking into possibility of investing in cyber liability insurance.

8. Detection

- Organizations should ensure they have state-of-the-art technology not only for preventing downloading of malicious software, but also for detecting/alerting organization to attempted breaches.
  - Should be coupled with training security employees on protocol for responding to such alerts.

Practical Tips (*cont'd*)

9. Breach Response Plan

- Organizations should be prepared to **respond to a breach quickly, efficiently, and calmly**. To do so, they should have a comprehensive, written breach response plan in place and should be clear on what will trigger the plan. As part of this plan, o

Form a Breach Response Team

- Team should be composed of people from key departments (including IT, legal, communications).
- Plan should identify individual functions and responsibilities in case of a breach.

Select an Individual with Ultimate Responsibility for Overall Implementation

Identify Outside Individuals that May Need to be Contacted in the Event of a Breach

- These may include legal, forensic, and public relations specialists, as well as other regulators and law enforcement authorities.

Consider Having Standing Contracts in Place with Outside Experts

- This avoids spending time on contract negotiation following a breach.

Outline Each Phase of the Incident Response

- Each stage should be included, from initial response activities (i.e., reporting breach), to strategies for fulfilling notification requirements under applicable laws, to breach response review/remediation.

Create Hypothetical Scenarios to Test the Plan ("Practice Run")

Ensure the Plan is Reviewed Regularly and Revised as Necessary

Practical Tips (*cont'd*)

10. Non-Digital Information and Physical Devices

- It is important to remember that non-digital PII should be safeguarded as well. Organizations should:
  - minimize, to the extent possible, the locations in which non-digital PII is stored; and
  - ensure the safe and secure storage of non-digital PII, such as by:
    - locking office doors and filing cabinets / installing card keys;
    - ensuring that documents and physical devices (such as disks, DVDs, flashdrives, computers) with PII are properly destroyed before disposal (such as by shredding or burning); and
    - being able to track computers and mobile devices to determine their location in the event they are lost or stolen.

Victim Preparation

- Ensure availability of :
  CISO, CSO, Legal, Senior System Administrator,
  Network Architect, Lead Developer
- Legal Banner/Computer Use Agreement
- Network Topography Maps
- Internal/External IP Address and Host List
- List of Network Devices (switches, routers)
- Incident Logs (security, host, IDS, web, database)
- Archived Network Traffic
- Forensic Images of Compromised Hosts
- Physical Access Logs (video, key cards)

Preventative Considerations

- Know your legal agreements with users and partner companies
- Make sure your IT Staff and Managing Partners are talking regularly
- Segment your networks (Finance vs. HR/Payroll vs. Case Work)
- Segment your authentication – Two Factor Authentication
- Application Security
- Security vs. Accessibility
- Who's monitoring the monitors?
- Remember: Any network link is a potential intrusion vector
- Have at least 2 to 3 IT staff members trained in cyber incident response