STERLING INSURANCE GROUP

RETHINK YOUR INSURANCE STRATEGY

Cyber Liability Exposure & Managing the Risk

Presented by: Joe Haney, CRA, CBWA

9/26/2016

SOBERING STATISTICS

- US Population: 320,000,000 (http://www.census.gov/popclock)
- Identity Theft Resource Center data:
  - Number of breaches from 2005 through 2014 = 5,029
- Total number of records exposed = 677,749,785
- The number of cyber-security incidents globally has increased by 48% to 42.8 million this year, according to a Price Waterhouse Coopers LLP survey

SOBERING STATISTICS

- On average it will cost a US organization $217 per record breached (5,000 records = $1,085,000)
- Consolidated findings show that malicious or criminal attacks are the most costly data breaches - $246 per record
- Malicious or criminal attacks are most often the cause of data breach globally (49%)
- The average financial impact per security incident - $6.5M (*Ponemon Institute, sponsored by IBM)*
- Breaches involving less that 10,000 records = $4.7M, more than 50,000 records = $11.9M

Source: Ponemon Institute: 2015 Cost of Data Breach: Global Analysis

Recap // 2015

- Total breaches: 781 - .0012% decrease over 2014 (782 in 2014)
- Total records exposed: 169,068,506 – 197% increase over 2014 (85M)
  - 39.9% of the data breaches occurred within the business/retail sector (312), with 9.6% of the total records exposed
  - 35.5% of the data breaches occurred within the Medical/Healthcare field, with 66.7% of the total records exposed.
- Hacking incidents represented the leading cause of data breach incidents, accounting for 37.9% of the breaches, increase of 8.4%
- Employee error/negligence came in at 14.9%, more than double from 2012
- Accidental exposure of information in 2015 jumped to 13.7%, insider theft at 10.6%, physical theft at 10.5%, and subcontractor/ 3rd party at 9%

Source: Ponemon Institute: 2015 Cost of Data Breach: Global Analysis

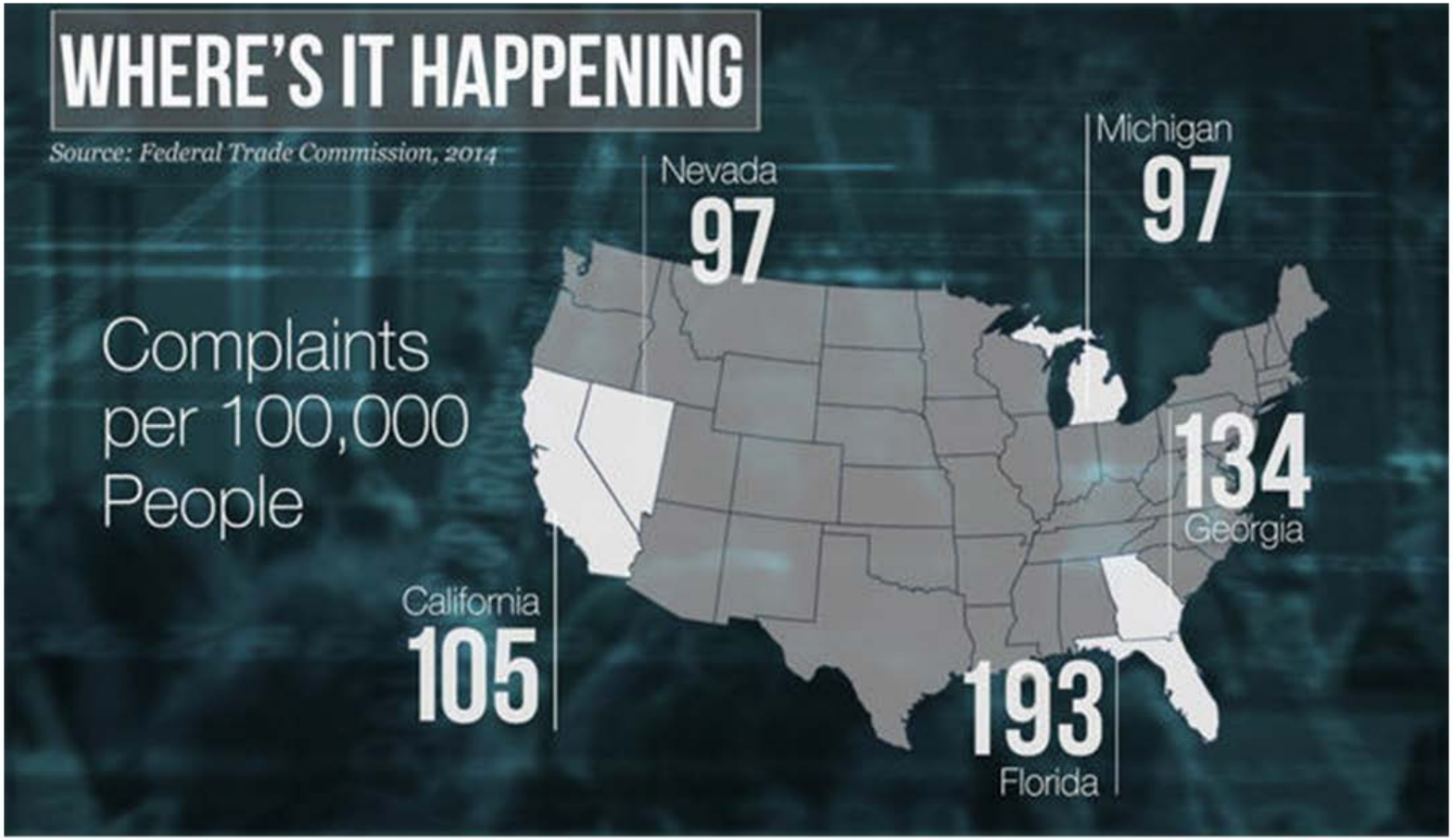
COST BY INDUSTRY

Heavily regulated industries such as healthcare, education, pharmaceutical and financial services has a per capita data breach cost substantially above the overall mean:

Healthcare: $359 (medical information can be worth 10x more than CC numbers which are sold on underground forums).

EDUCATION - $294
PHARMACEUTICAL - $227
FINANCIAL - $206
RETAIL - $105

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



IDENTITY THEFT COMPLAINTS // MICHIGAN

$217 PER RECORD?

Typical activities for discovery and the immediate response to the data breach include the following:

- Conducting investigations and forensics to determine the root cause of the data breach
- Determining the probable victims of the data breach
- Organizing the incident response team
- Conducting communication and public relations outreach
- Preparing notice documents and other required disclosures to data breach victims and regulators
- Implementing call center producers and specialized training

Source: Ponemon Institute: 2015 Cost of Data Breach: Global Analysis

$217 PER RECORD?

The following are typical activities conducted in the aftermath of discovering the data breach:

- Audit and consulting services
- Legal services for defense
- Legal services for compliance
- Free or discounted services to victims of the breach
- Identity protection services
- Lost customer business based on calculating customer churn or turnover
- Customer acquisition and loyalty program costs

Source: Ponemon Institute: 2015 Cost of Data Breach: Global Analysis

Target – Prepared – Not so much…….

- In House Risk Managers

Still the exposures exists and the damage was done.

- Fallout
  - CEO – Steinhafel - Gone! 23 million a year he was making
  - CIO – Beth Jacobs – Gone!
- Limits
  - $100 Million in limits carried
  - Thought they were adequately protected – Not Enough. 200,000 plus claim, 214 per customer Know your exposures
  - They believe now it was in excess of 300,000 claims on the cyber breach

NO MEDIA ATTENTION?

Shaker Clinic

- State: OH
- Breach Type: Paper
- Breach Category: Medical/Healthcare
- # of record reported – 617

Shaker Clinic in Ohio, a psychiatric care facility for adults and seniors, reported that 617 patients were notified of loss of paper records on February 18.

617 compromised records x $359 (healthcare related) = $221,503 organizational cost.

Publication: phiprivacy.net / hhs.gov

JIMMY JOHNS // 2014

- 216 of 2,000 stores affected
- Breached entry was caused through POS system provided by third party
- Damages have not been disclosed, but Jimmy Johns forced to front computer forensic costs as well as customer satisfaction.

http://krebsonsecurity.com/2014/09/jimmy-johns-confirms-breach-at-216-stores

Claim Examples

✓Corrupted data

Example: A communications company sues for lost revenue and expenses to recover billing files for wireless customers that were deleted by their software vendor who was updating the system.

Indemnity Paid: $750,000

Defense Costs Paid: $150,000

More Examples

- 130 million credit card numbers were stolen from Heartland payment Systems (HPS) by an outside hacker
  - HPS's stock price had fallen 74% 45 days after the breach
  - The breach cost HPS upwards of $70 million

- Kaiser Permanente was fined $200,000 for publicly posting 150 patient names, addresses and medical records on their website

- A 2012 data breach insurance claims study done by Net Diligence found that the average cost of legal defense for a data breach was $582,000 and the average cost of a settlement was over $2 million!

Insurance

Growing Need For Cyber Liability Insurance

- As technology in business evolves - the value of a strong cyber liability insurance policy will only continue to grow.

- The rise in the amount of information stored and transferred electronically increases dramatically the potential exposures facing businesses.

Why Cyber Liability Insurance?

- A traditional business liability policy is extremely unlikely to protect against most cyber exposures.

- Standard commercial policies are written to insure against injury or physical loss and will do little, if anything, to shield you from electronic damages and the associated costs they may incur.

AVAILABLE COVERAGE / / THE BASICS

First Party-Post breach response:
Forensic investigation, proper notification of affected individuals, credit card monitoring, and establishing a call center.
As of August 1, 2015, only Alabama, New Mexico and South Dakota have no laws related to security breach notification.

Third Party:
Coverage for financial damages to clients resulting from a security breach of your data or data for which you are responsible

Business Interruption:
Reimbursement for your reduction in profit during a system outage period

System Damage:
Rectification costs for retrieving, restoring or replacing any of your computer programs

AVAILABLE COVERAGE / / THE BASICS

Threats/extortion:
Ransom payment to prevent unauthorized access to your computer system, introduction of a virus, revealing confidential data including protected health information, and reputational harm by posting false or misleading comments about you on social media sites

Multimedia:
Intellectual property rights infringement (no patent), Defamation (libel, slander), misappropriation of content and trade secrets

Cyber Crime:
Unauthorized electronic funds transfer, theft of money or other financial assets

Public Relations:
Crisis and reputation management

COVERAGE / / KEY ITEMS

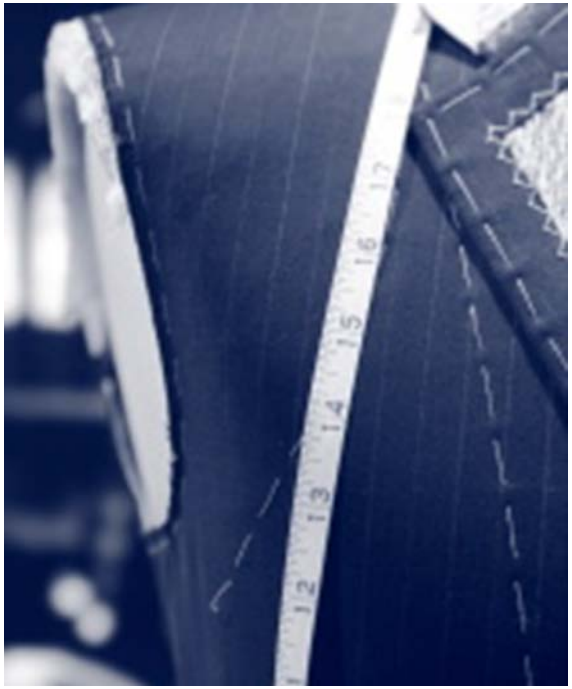
- Contractual Liability
- PCI and HIPAA/HITECH Fines and Penalties
- Regulatory fines & penalties
- Future loss of customers: U.S. organizations have the highest lost business costs ($3.3M). Lost business costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses, and diminished goodwill.

KEY ITEMS / / CONTINUED

- Full prior acts
- Insured identity theft (not clients)
- Territory
- Phishing
- True World Wide coverage

TAYLORING THE POLICY

- What are the clients operations?
- What regulatory environment does the client operate within?
- What kind of sensitive information is stored? How much data is stored?
- Is data outsourced? What contracts are in place with vendors? Who is assuming liability?
- Does the client accept credit cards?
- How do they generate revenue? How would downtime impact the business?
- Use of websites, computers, tablets, smartphones?



I’m Not a Target

OBJECTION

A breach won't happen to us – We are not a target

40% of all cyber attacks target business with fewer than 500 employees
- National Cybersecurity Awareness Campaign: Homeland Security

Only a small percentage of cyber attacks are considered targeted attacks, meaning the attacker group is going after a particular company or group of companies in order to steal specific data

"It's easy for small businesses to become lax in regards to their Internet security, thinking they're too small for hackers to bother with. However, according to the Minnesota Cyber Crime Task Force, these are the businesses which are squarely in the crosshairs of cyber criminals."

-Dana Badgerow, President and CEO of the Better Business Bureau

OBJECTION

We are not a target… or large like Target

- Employee negligence puts an organization at risk!
- How do you manage mobile device use? Bring your own device (BYOD)
- Lack of IT infrastructure & enforcement of data security policy
- Do you regularly back up data? A Ponemon institute study revealed 62% of small-medium organizations were not confident in avoiding substantial downtime in the event of data breach/systems event.

OBJECTION

I have coverage under other policies (GL, D&O)

- See Sony PlayStation case:

New York trial court recently ruled in a (CGL) policy coverage case that Zurich American Insurance Co. has no duty to defend Sony Corp. of America

Justice Oing said acts by third-party hackers do not constitute "oral or written publication in any manner of the material that violates a person's right of privacy" in the Coverage B (personal and advertising injury coverage) under the CGL policy issued by Zurich.

Source: http://www.insurancejournal.com/news/east/2014/03/17/323551.htm

OVERVIEW

Cyber Liability Insurance – What's covered and why do I need it?

Third Party Coverage

- Communications and Media Liability Coverage
- Network and Information Security Liability Coverage
- Technology Errors and Omissions Liability Coverage

First Party Coverage

- Cyber Expense Reimbursement
- Security Breach Notification and Remediation Expense
- Crisis Management Service Expense
- Business Interruption and Extra Expense
- Extortion Expense

OVERVIEW //CONTINUED

- Cyber extortion – Hackers can hijack and ransom websites, networks and stored data, denying access to you or your customers.
  - Potential Loss of Revenue
  - Paying the hacker's demands
  - Rebuilding if damage is done.

- Business interruption – Balance Sheet Protection
  - Loss of your revenue due to a covered event

OVERVIEW //CONTINUED

Cyber Liability Insurance is specifically designed to address the risks that come with using modern technology

- Risks that other types of business policy coverage simply won't.
- The level of coverage your business needs is based on your individual operations and can vary depending on your range of exposure.

It is important to work with a broker that can identify your areas of risk so a policy can be tailored to fit your unique situation.

What Else Do I Need To Do?

Internal Controls - Privacy and Data Security

1. Conduct an inventory to help you answer the following questions;

   - What kind of data do you have in your business?
   - How is that data handled and protected?
   - Who has access to that data and under what circumstances?
   - Your business could have a large assortment of data of varying value.

2. Once you've identified your data, keep a record of its location and move it to more appropriate locations as needed.

3. Develop a privacy policy – Show your clients that you value their information.
   Your privacy policy should address the following types of data:
   - *Personally identifiable information* – Often referred to as PII, this information includes such things as first and last names, home or business addresses, email addresses, credit card and bank account numbers, taxpayer identification numbers, patient numbers and Social Security numbers. It can also include gender, age and date of birth, city of birth or residence, driver's license number and home and cellphone numbers.
   - *Personal health information*
   - *Customer information*

4. Protect data collected on the Internet.

5. Create layers of security.
   - Inventory your data
   - Identify and protect your sensitive and valuable data.
   - Control access to your data.
   - Secure your data.
   - Back up your data.

6. Plan for data loss or theft.
   - Scams and Fraud
     - Phishing
     - On-Line Fraud
     - Train employees to recognize social engineering
     - Protect against malware
     - Be aware of spyware and adware

7. Additional areas of concern

- Network Security
- Website Security
- Email
- Mobile Devices
- Employees
- Facility Security
- Payment Cards / Credit Cards

Incident Response – What do we do?

Types of breaches

- Physical breaches
- Network and system security breaches
- Data breaches

Action Items, if breach occurs

- Engage Insurance provider if coverage is in place.
- Notify law enforcement and/or customers, if necessary.
- Work cohesively across technical and leadership teams to limit the damage.
- Begin recovery effort.

- **Key Disaster Recovery Principles**
  - *Don't wait until it's too late*
  - *Protect information completely*
  - *Get employees involved*
  - *Test frequently*
  - *Review your plan*
  - *Be prepared*
- **Hold a "lesson learned" meeting.**

- **Questions?**

- **Thank you!**

Joe Haney, CRA, CBWA
President
Sterling Insurance Group
(586) 323-5700