CYBER LIABILITY WORKSHOP

Your Insurance Agency and Mid-Sized Clients
Are Not Immune
May 7, 2013

Kevin Ribble
E.V.P. Edgewater Holdings
President, EPRMA.org
kribble@edgewater.net
(214) 676-8662 (office)
(312) 431-1766 (fax)
Texas License # 1682508

Today's Agenda

- **Introduction to Panel**
- **Cyber Crime and insurance agencies & mid-size businesses**
- **Cyber Crime statistics**
- **Why are insurance agencies considered to Be at High-Risk?**
- **Types of Threats**
- **What is the potential harm to your agency and client's enterprise?**
- **Cyber litigation**
- **Case Studies**
- **Risk Transfer & Risk Management**
- **Summary**
- **Q&A**

Network Security / Data Risk

What is a Breach ?

- Unauthorized disclosure
- Unauthorized use or access
- Data compromised
  - *Data has value and creates duties*

What is Identity Theft?

- Fraudulent use of someone else's personal information
- Causes injury to property and person

About half of the states have approved legislation that criminalizes the unauthorized use of encoded credit card information.

For example, in Texas, a statute **requires restaurants and bars to post warning signs**, alerting employees against possession of or fraudulent use of someone else's identifying information.

Cyber Crime and Small Businesses

- Over 20% of small businesses have suffered a data breach[1]
- Number of attacks on rise, breach size declining, indicating cybercriminals go after smaller targets e.g. small enterprises (less security = easier attacks)
- Malicious attacks (hacking or inside theft) constitute 40% of recorded breaches in 2011
- Visa reports 80% all card breaches arise from Level 4 merchants (those with fewer than 50 employees)
- Each year, more than 10 million individual identity thefts

[1] **Poneman Institute Study on Cyber Crime**

Small Business Data Theft Risk Management Study

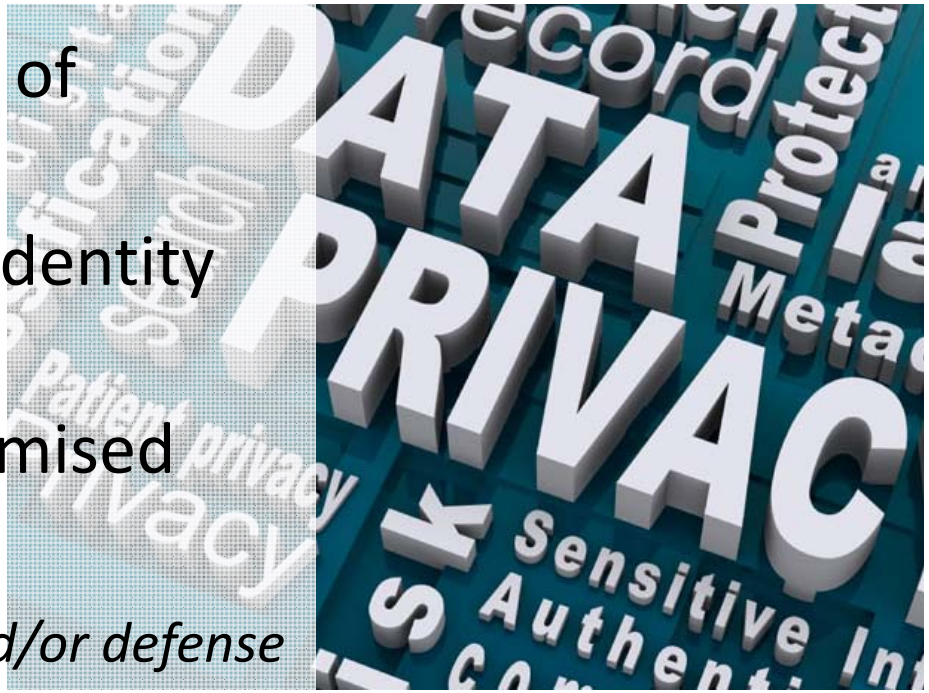
Data Under Siege

- 1992 – 2007, 2M unique malicious programs
- 2007 – 2009, 33.9M unique malicious programs
- 2010 hit new record 1.5 Billion (ump)
- 31% of IT specialist were aware of most deadly (ump)
- 87%, of system vulnerabilities were due to 3rd party applications, Microsoft, Java, IT infrastructure

- "U.S. Code Cracking Agency Works as if Compromised" – Reuters News 12 16 2010
- Global IT Security Risks Report, Kaspersky Lab 2012

Cyber Crime and Small Businesses

- ATM skimming generates losses of $50 million each year[1]
- One in 20 adults is at risk of identity theft
- One in 465 is a victim of identity theft
- Average cost per compromised document: $214
  - *Not including civil damages and/or defense costs)*



[1] **Electronic Funds Transfer Agency**

www.efta.org

Threats: Not “If” but “When”

Malicious Threats

- Hackers, extortionists, **disgruntled employees**, fraudsters
- **Malware, spyware, spam**,

- **Malware**, short for **malicious** (or malevolent) **software**, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software.[1] 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.[2]

  Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses.[

- **Phishing, pharming**
- A: Both pharming and phishing are methods used to steal personal information from unsuspecting people over the Internet.

  Phishing typically involves fraudulent bulk e-mail messages that guide recipients to legitimate-looking but fake Web sites and try to get them to supply personal information like account passwords.

  Pharming tampers with the domain-name server system so that traffic to a Web site is secretly redirected to a different site altogether, even though the browser seems to be displaying the Web address you wanted to visit.

Threats: Not “If” but “When”

Non-Malicious Threats

- Employee mistakes: Lost / stolen laptops and portable devices
- Application glitches
- Network operation and “sharing” trends
- Points of failure are now multiplied due to outsourcing
- Dependencies & data-sharing between biz partners including cloud servers
- Upstream & down stream vendors (ASPS, partners, ISPs)

Methods of Fraud

What Are Thieves Looking For?

- **PII & Cardholder Data**
- Social security numbers, names and addresses
  - Health insurance applications, claim BI indexes,
  - Primary Account Number (PAN)
  - CID number (this must never be stored)
  - Sensitive authentication data = card use and cardholder's identity
- **Methods Include**
  - Compromised card readers
  - Papers stored in unlocked filing cabinets
  - Data held in a payment system database
  - Hidden camera recordings entry of authentication data
  - Secret "tap" on your company's wired or wifi network

Why are Insurance Agencies & Small Businesses considered to be at High Risk?

The Risk to Insurance Agencies

Why are Insurance Agencies & Small Businesses considered to be at High Risk?

- Hackers and thieves are targeting Small Businesses, because:
  - Small businesses typically lack the resources and expertise to successfully fend-off – or even respond to – attacks
  - Lack of a formal IT department means that Payment Card Industry (PCI) Data Security compliance is particularly challenging for small organizations
    - The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that ALL companies that process, store or transmit credit card information maintain a secure environment.
- An attack or error of negligence could prove catastrophic for the typical insurance agency or small business

"Over 20% of small businesses had already suffered a data breach…. small businesses do not have adequate measures or remedies in place to protect themselves."

- Larry Ponemon
Ponemon Institute
Small Business Data Theft Risk Management Study

The Risk to Insurance Agencies

- Disgruntled employees – non-disclosure
- Loss of revenue, System crashes from hackers
- Data Breach (MGA claim data stolen) Medical Insurance applications stolen
- Your e-mail infects customers
- Agencies utilize social media, e-marketing materials, company blogs
- Lack of knowledge & resources to respond to breach, timely

Potential for Business Harm to Your Enterprise

What is the potential harm to your agency and client's enterprise?

- Business fall-out can be severe (including negligence *and* breach)
- Agency E&O / D&O
  - Failing to meet Payment Card Industry (PCI) rules or negligently managing PII data
    - State statutory notification, fines and penalties
    - Fines and Penalties (liquidated damages)
    - Termination of ability to accept payment cards
    - Reduction in business, lost customers (20% likely)
    - Cost of reissuing payment cards ($100 per card VISA)
    - Fraud losses (see civil damages)
    - Legal costs, settlements, and judgments
    - Increase in compliance costs
    - Going out of business (i.e., breach exceeds net worth of company)

CYBER LIABILITY LITIGATION

May 7, 2013

Martin K. LaPointe, Esq.
LaPointe Law, P.C.
1200 Shermer Road, Suite 310
One Lane Center
Northbrook, IL 60062
(847) 786-2500
mlapointe@lapointelaw.net

Cyber Lawsuit Basics

- Basic Negligence
- Duty + Breach + Causation = Lost elements
- Damages – Last element
  - Damages is where the case is litigated
- Damages mitigation = crucial

Government Lawsuits

- Gov't enforcement
  - State Attorney General
    - Conn. – HealthNet (breach of HIPPA-regulated data)
  - Federal Trade Commission (FTC)
    - ChoicePoint (breach of 163,000 consumers' data)
- Gov't enforcement – stems from state/federal laws
  - 46 states require notice after breach
  - D.C., Puerto Rico and Virgin Islands also require
  - Federal laws (*e.g.*, HIPPA, HITECH, FACTA)

Private Class Actions

- Developing area – stay tuned
- Possible consumer data classes
  - Possible 100's of thousands/millions
  - Class certification uncertain
    - Commonality, etc. must be established
    - *In re Hannaford Bros. Data Security* = No
- Damages exposure enormous
- MDL – nationwide coordination

Single Plaintiff Lawsuits

- Damages still “king”
- Burden on plaintiff to show damages
- Damages = actual not speculative
- *Krottner v. Starbucks*
  - *“risk of future harm”* – No
  - Must show “actual loss” from data misuse

Common Law Tort Damages

- Negligence
- Damages
  - Loss of business
  - Loss of reputation
  - Loss of privacy
  - Time loss
  - Pain & suffering
  - Possible punitive damages
    - Complete breakdown in data protection
    - Failure to mitigate

Bank Lawsuits

- Replacement of credit cards
- Fraudulent charges
- Interruption of business
- Consumer bank fees

Litigation costs

- Attorneys' fees
  - Breach oversight
  - Investigation
  - Notice
  - Proper handling of e-discovery
  - Litigation preparation
  - Review of contracts
  - Let the lawsuit begin (defense)

Litigation costs (cont'd)

- Costs of the breach
  - Forensics expert
  - Notice vendor
  - Restoring IDs
  - PR company
  - Call center vendor
  - ID theft insurance
  - Credit monitoring company

Litigation costs (cont'd)

- Plaintiff(s) demands
  - Lost time (work)
  - Reimburse fraudulent charges/fees
  - Replace credit cards
  - Credit monitoring
  - Repair credit/insurance
  - State/federal fines and penalties
  - Plaintiffs' attorneys' fees

Mitigation of Damages

- Importance cannot be overstated
  - Reduces actual damages
  - Reduces possibility and amount of fines
- Secure the breach
  - Hire forensics expert
  - Extent, source, fix
- Notice - ASAP

Mitigation of Damages (cont'd)

- Analyze data
- Monitor customer credit
- Repair customer credit when needed
- Purchase ID theft insurance
- PR/counteract negative press

Real-World Cyber Threats: What Happens After a Breach?

Target Markets Association

Baltimore, Maryland

Lori Nugent

Chair, Data Security &

Cyber Liability

Wilson Elser

7 May 2013

How do Breaches Happen?

- Lost or Stolen Laptop/Portable Device
- Office Break-in/Theft
- Mis-mailing
- Unauthorized Access by Vendors/Business Partners
  (e.g. Cleaners, Mailroom, Shredders, Large Project Participants)
- Unauthorized Access by Current/Former Employees
  (e.g. Taking Information When Leaving the Company)

Top Three Real-World Challenges Following a Breach:

1) Compliance with Global Security/Privacy Regulations
   – Most Triggered by
     Breached Individual's Residence,
     NOT Location of Breached Business

2) Impact of Breach on Reputation
   – Breach is a "Tipping Point"

3) Financial Difficulties Caused by a Breach

Financial Difficulties Caused by Breach:

- Unanticipated Investigation/Response Costs
- Reputational Damage
- Impact on:
  - Cash Flow/Earnings Projections
  - Valuation/Credit
  - Upstream Business Partners
  - Downstream Vendors
  - Customers

Does Cyber Insurance Address These Concerns?

- Application Process Benchmarks Cyber Security and Begins Enterprise Risk Management Dialog
- Access to Experienced Breach Responders/Services Supports Responding Well
- Coverage Minimizes Financial Difficulty Following Breach

After a Breach, Companies:

- Evaluate Adequacy of Breach Reserves/Insurance and Buy More Cyber Insurance
- Update and Test their Breach Response Plan, and Train Employees
- Address Vendors/Business Partners' Cyber Security Beyond Warranties and Indemnification Agreements
- Require that Vendors/Business Buy Cyber Insurance

What If Cyber Coverage Was NOT Purchased?

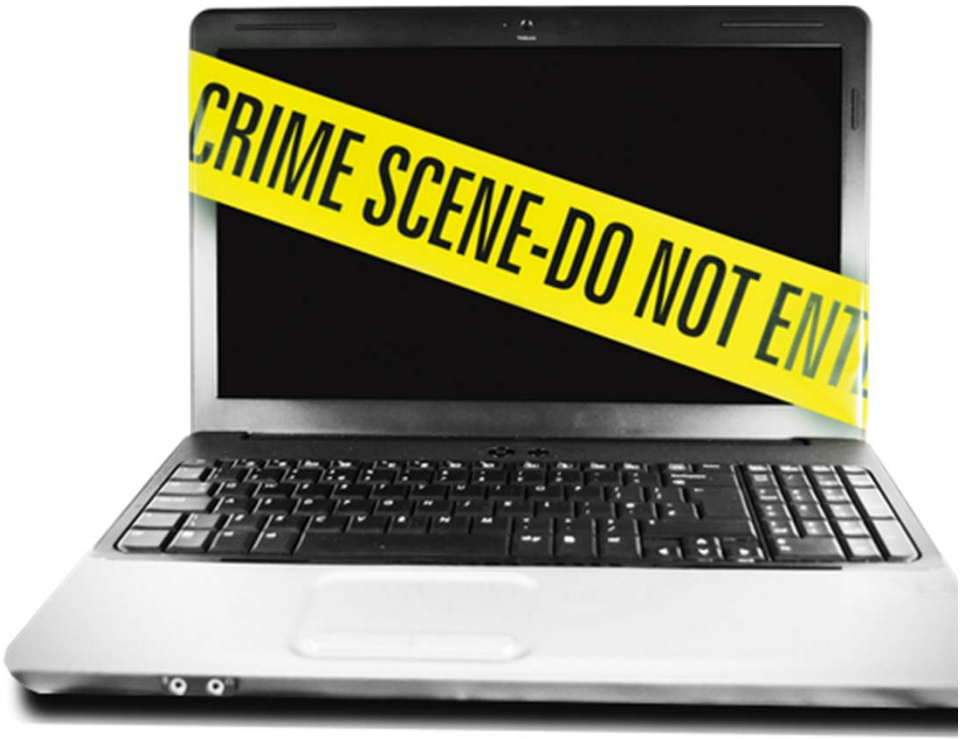
- Financial Distress
- Why Didn't My Broker Tell Me?
  - The "Tidy Blank" Problem
  - Just Like Additional Insured Problem?
  - Broker E&O?

Contact

Lori Nugent
Chair, Data Security & Cyber Liability
Wilson Elser
Chicago, Illinois
312.821.6177
Lori.nugent@wilsonelser.com

Best Solution

Risk Transfer & Risk Management



Policy Questions

- **Third-Party Liability**
- Coverage for transmission of virus to third party and 3rd party to others
- Copyright infringement from website
- Full prior acts vs. retro-date inception
- Coverage applies to both electronic and physical data breaches e.g. paper, laptop, disks, PDA etc. ?
- Coverage applies to both personal and company information?
- Coverage applies to employee and customer information – yes
- Information in care custody or control of insured's vendors include cloud servers and records being transported?
- Policy apply to accidental losses and leaks?
- Does application require PCI compliance or encryption?
- No insider exclusion?
- Direct intentional attacks are covered is "wild viruses" those not specifically targeting insured?

Policy Questions

- **Media liability**
- Media Liability is valid anywhere in world? Yes
- Coverage extend to include social networking , emails, twitter?
- Coverage apply to user-generated content (opinion boards for feedback)
- Liquidated damages and fines and penalties? Know position, provable court damages and fines are covered
- **Crisis Management**
- Policy apply to attorney fees to draft response to breach and related deliver costs?
- Is credit monitoring included for individuals?
- Will policy provide options to notification methods?
- **First Party business interruption**
- Do they offer contingent period after system restored?
- Based on time system is down or a stated time period?
- Wild viruses included

Recommended Cyber Coverage

What does System Damage & Interruption cover?	This is first party cover that protects companies against their own losses resulting from damage to data caused either deliberately by a malicious employee or hacker, or totally accidentally (the infamous “fat finger”). The system interruption cover stems directly from this but is restricted to malicious employees, hackers or computer viruses. This provides protection against loss of profits arising directly from these perils.
What does Cyber & Privacy Liability cover?	This provides liability coverage – including legal defense costs and indemnity payments – for claims brought against you arising from a data security breach, whether through electronic means or otherwise. This is provided on an “all risks basis”. The coverage is also extended to include liability protection against claims arising from you spreading a computer virus or from your systems being used to hack a third party.
What does System Damage & Interruption cover?	This provides first party cover for the cost of complying with breach notification laws. Coverage is also included for voluntary security breach notification, where this helps to mitigate adverse impact upon the company’s brand or reputation. The coverage itself will pay for the legal costs of drafting a breach letter, the cost of printing and posting the letter, credit monitoring costs, and forensic costs that may be required to identify the extent of the breach.
What does Media Liability cover?	This provides comprehensive liability coverage including legal defense costs as well as indemnity for damages and fines (where insurable). Essentially, this coverage protects against claims for intellectual property rights infringement (excluding patent) and defamation arising from content published by the company or on its behalf. This coverage also extends to social media and user generated content, including company and employee blogs.
What does regulatory privacy cover?	This provides coverage for the costs associated with defending yourself against a regulatory action brought against you as a direct result of a privacy breach. This includes actions brought by federal regulators such as the FTC and similar state or industry bodies. Coverage is also extended to include fines and penalties that are issued as a result, where these are insurable by law.

Recommended Cyber Coverage Limits

- System Damage & Interruption - 1M limits
- Cyber Privacy Liability – 250K limits
- Privacy Breach Notification – 1M limits
- Media Liability -1M limits
- Regulatory Privacy – 1M limit

How to Protect Your Company's Data

Comply with the golden 12 Rules

Goal	Rule
Build and Maintain a Secure Network	▪ Install and maintain a firewall configuration to protect data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder and HIPPA Data	▪ Protect stored data ▪ Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	▪ Use and regularly update anti-virus software ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ Restrict access to data by business need-to-know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain – and update – a policy that addresses information security

How to Protect Your Company's Data

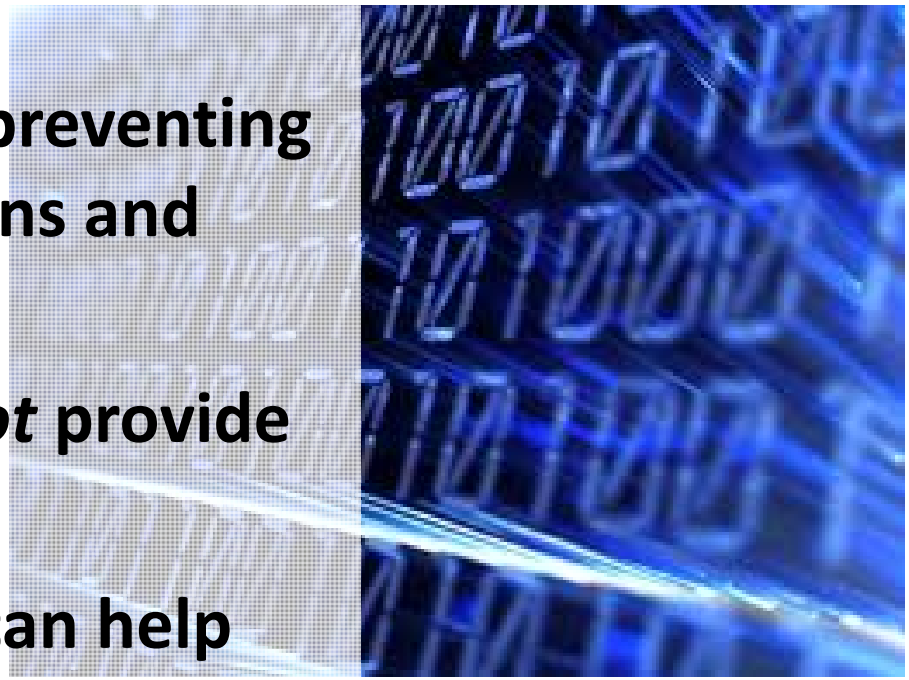
How to protect your company's data from theft (continued)

- Access to Experienced Breach Responders/Services
- Conduct background checks on all employees handling *or* having access to cardholder information
- Encrypt external sensitive internet communications
- Use shredders to destroy all sensitive information

Summary

Summary

- **Small Businesses are considered to be at High Risk**
- **Best Practices can aid in preventing an attack *before* it happens and reducing it after it occurs**
- **Typical insurance does *not* provide adequate coverage**
- **Cyber Liability coverage can help bridge the gap**



Questions?

Thank You!

kribble@edgewater.net