De-Mystifying Data Breaches and Information Security Compliance

ALA 2016 Annual Conference

Your connection
to knowledge, resources and networking

James Harrison
CEO, INVISUS

The Data Security Problem

It's a BIG problem, and it's GROWING:

- Confidential personal and business information is the new global **currency of thieves**
- Criminals targeting **large** and **small** organizations
- 164 million **SSN's** compromised in 2015
- 112 million **health records** compromised in 2015 (1 in 3 adults)
- 1.4 million **tax return** ID theft victims in 2014

Sources: ITRC, DHHS/OCR, IRS

The Data Security Problem

- 85% of breaches are at **small business**
- 49% of breaches caused by **employees**
- **Ransomware** – holding businesses hostage
  - 40% of attacks at companies less than 100 employees
  - Downtime a greater cost than the ransom itself
- **Third party** risks (vendors, service providers)
- Shifting **accountability** (execs under fire)

Sources: VISA, Ponemon Institute, LegalTech News

Law Firms are a Target

- **Mid-sized law firms** between 50 and 150 attorneys will be the most targeted by cybercriminals looking to gain access to sensitive data
- Planned phishing and ransomware attacks against law **firm partners** and **administrators**
- Hackers are also targeting **employees** of firms using lists of names, email, and social media accounts

Sources: LegalTech News, BusinessInsurance.com

How are Law Firms Doing?

ABA Data Breach Survey, 2015:

- 1 in 4 law firms have had a data breach incident
- 47% have no breach response plan
- 58% do not have an appointed information security and compliance manager
- 20% conduct regular 3rd party security assessments
- 34% of firms received a security audit request from clients

How are Law Firms Doing?

Marsh's Law Firm Cyber Survey, 2014:

- 72% of firms have not assessed how much a breach would cost them with the type of data they retain
- Less than 50% said their firm was insured against this risk

How is YOUR Firm Doing?

- **Doing "something"?** It's the IT guy's job…
- **Putting it off?** We've thought about it…
- **In denial?** It won't happen to us…

What's your plan of action?

Administrator's Role

- Every firm needs someone who is **trained** and can **manage** an "information security compliance" plan
- This is typically assigned as an **administrator's** responsibility
  - Coordinate with partners, IT staff, HR, facilities, etc.
- Being a compliance manager is a **key skill set** and resume builder for firm administrators going forward!

What You Need to Know

- What is Information Security COMPLIANCE?
- How data breaches happen
- Why this should be among your firm’s top priorities
- 10 things your firm should be doing to help prevent a breach and stay in compliance

Defining “Information Security”

“The protection of company, customer, employee or other confidential and proprietary information that is processed, stored or handled by the company, including electronic and paper-based information.”

- Often called cyber-security, data security
- Most think this is just a tech or IT issue
- But – today’s information security definition includes the company’s overall plan for technical, physical and administrative safeguards

Define “Compliance”

Information security compliance:

“The **implementation** and **management** of a formalized **Information Security Plan** for protecting confidential **customer and employee** information…

…in accordance with the minimum requirements in **federal**, **state** and **industry regulations** and standards.

What is Protected Information?

Personally Identifiable Information (PII):

- SSN
- DOB/Birth Certificate
- Email/Password/Username
- Name/Address/Phone
- Federal EIN
- Driver’s License
- Passport
- Military ID

What is Protected Information?

Personal Health Information (PHI):

- Medical Records/History
- Health Insurance
- Treatment/Medication
- Medical Billing/Claims

What is Protected Information?

Personal Financial Information (PFI):

- Payment Cards (credit/debit)
- Checking/Banking
- Payroll, W2, 1099
- Tax Returns, Information
- Credit Reports/Scores
- Accounting Records
- Investments
- Real Estate

What is a Data Breach?

"An incident in which a person's name and any personally identifiable information (PII), personal health information (PHI), or personal financial information (PFI) is put at risk due to exposure, loss or theft." (*electronic data or paper documents*)

How Breaches Happen

- Hacking (38%)
- Employee Error/Negligence (15%)
- Email/Internet Exposure (13%)
- Insider Theft (11%)
- Physical Theft (10%)

Source: ITRC 2015

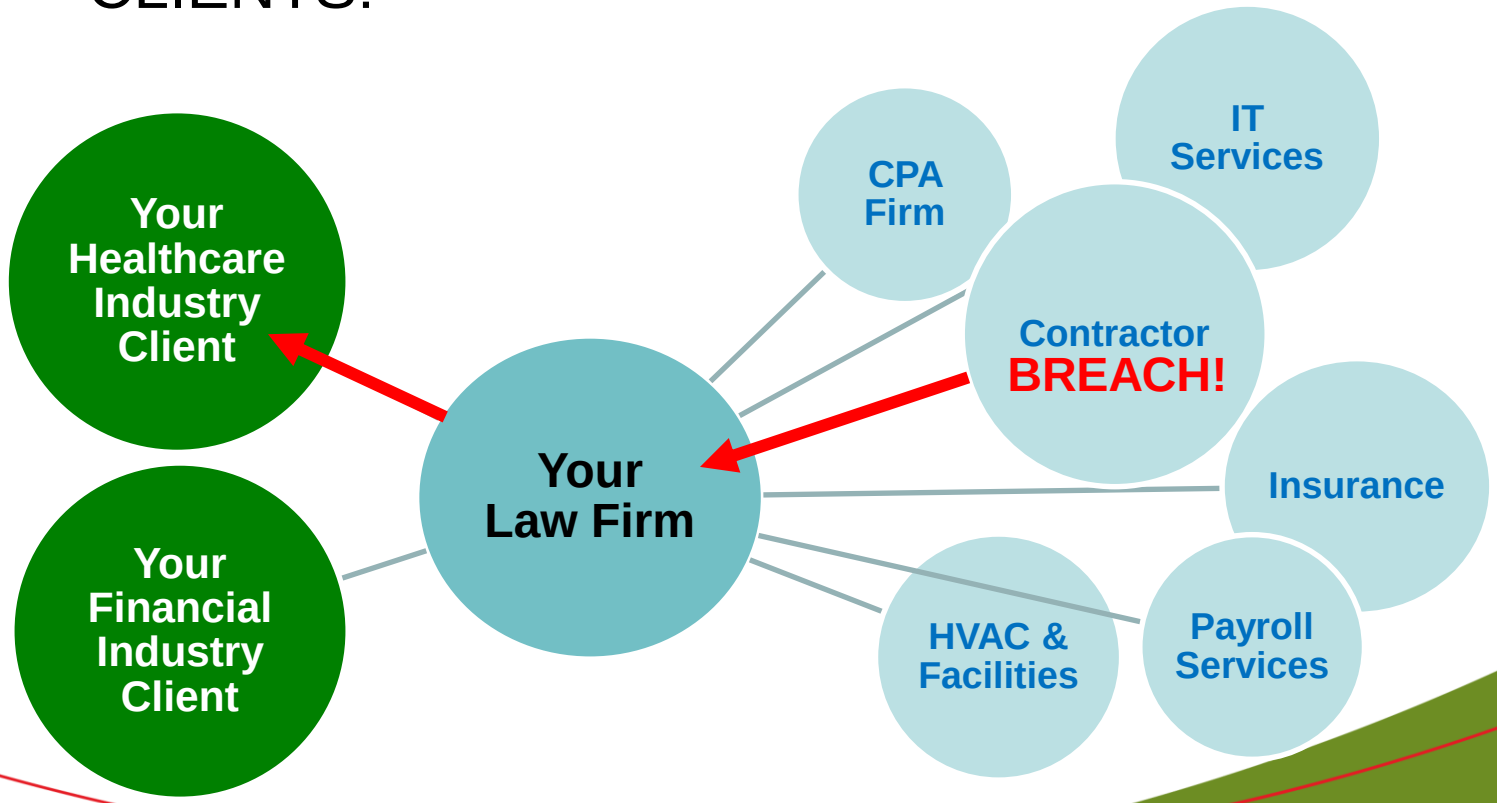
How Breaches Happen

- 3rd party Service Providers & Business Associates (9%)

Why should law firms be proactive in **breach prevention** and **compliance**?

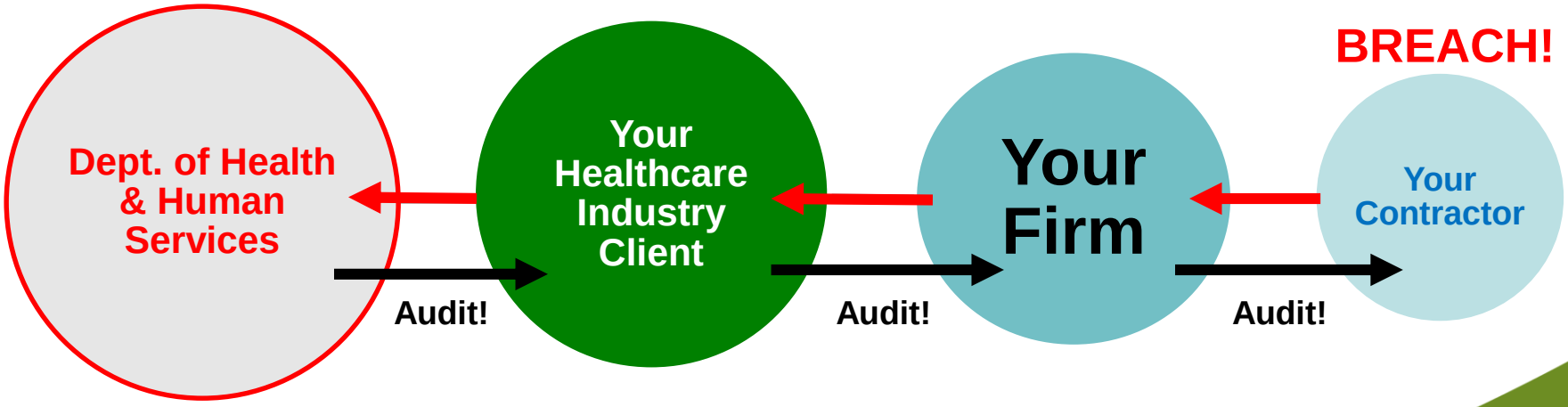
Caught in the Middle…

- A sub-contractor's breach affects YOU and YOUR CLIENTS!



Caught in the Middle…Audits!

- Your firm is caught in the data breach audit trail



The Risk to Firms

"Failing to take such action means greater **regulatory** and **litigation risk**."

"Non-compliance with cybersecurity norms are likely to damage the firm's **reputation** in the marketplace and with customers, suppliers, and other business partners."

(LegalTech News, March 2016)

Financial Risk

If your firm suffers a breach:

- Direct Costs -
  - $201 avg. recovery cost per record
- Regulatory fines & penalties
- Customer loss, reputational damage
  - Up to 33% of clients consider leaving
- Business disruption
- Civil lawsuits

Example Direct Costs:

2,500 records compromised:

- $170K in customer remediation
- $500K in total breach cost

Source: Cost of Cybercrime Study, Ponemon Institute 2015

3rd Party Audit Risk

If one of your business clients or business associates suffers a breach:

- THEY will likely be audited by federal, state or insurance regulators
- YOU will likely be audited as a service provider to that business

Under Pressure!

Law firms face **growing demands** to meet minimum information security standards and regulations.

Regulatory Pressure

Federal Laws:

- HIPAA-HITECH (health related information)
- Graham Leach Bliley Act (financial info & services)
- “Business Associate” requirement
  - Direct enforcement by the federal Office of Civil Rights over business associates of covered entities – including law firms
- 2017 - New federal laws coming

Regulatory Pressure

State Laws:

- 47 states with current laws
- Firms must consider the laws in all states where their clients reside

Industry Pressure

- American Bar Association
  - **ABA Resolution 109** - Calling for law firms to “implement and maintain an appropriate cybersecurity program”

Business Client Pressure

Security Audits & Proof of Compliance:

- HIPAA
- GLBA
- PCI-DSS
- AICPA – SOC audits and reports
- ISO 27001/27002 security audits & reports
- **Existing** Clients & **Prospective** Clients

The Basics of Breach Prevention & Compliance

10 things your firm should be doing

10 Best Practices

1. **Management Commitment**
   - Partners, managers must understand the risks and liabilities
   - Translate “security” into business planning
   - Investment in cybersecurity and a formalized compliance management program
   - Top down culture of security and privacy
2. **Assign Responsibility**
   - Compliance Program Administrator (or Information Security Officer)
   - Collaborate with all departments, management team

10 Best Practices

3. **Information Security Plan**
   - Fully documented security policies and procedures that meet regulatory and industry standards
   - All administrative, physical and technical safeguards outlined
4. **Risk and Compliance Assessments**
   - Done at least annually
   - Identify changes or gaps in security and compliance
5. **Implement and Maintain Safeguards**
   - Administrative, physical and technical security measures
   - Regular updates and vulnerability testing

10 Best Practices

6. **Employee Training**
   - Information security handbook, employee agreement
   - Initial and ongoing information security training
7. **Business Associate Agreements**
   - Assess security of 3rd party service providers, vendors, etc.
   - Information security agreement
8. **Incident Response Plan**
   - Incident response coordinator
   - Documented plan of action
   - Trial run

10 Best Practices

9. **Security and Compliance Reports**
   - Regulatory compliance reports (HIPAA, GLBA)
   - Industry best practices reports (SOC 2, ISO 27001, NIST)
   - Internal management reporting
   - Maintain legal defensibility
10. **Client Trust and Confidence**
   - Information privacy notice
   - Be ready for security audit & report requests from clients
   - Consider 3rd party compliance certification

Key Tip for Administrators

Make your job easier!

Get a Compliance Management System (CMS):

- Simplify, automate compliance management
- Compliance documentation & reports
- Client security audit reports
- Security training
- Security testing & reports
- Automatic compliance updates and reminders

Thank you.

YOUR OPINION MATTERS!

Please take a moment now to evaluate this presentation.