SMALL BUSINESS TRAINING SERIES

What You Should Know About Information Security and Compliance

Mark Conboy
Privacy 360, LLC

PRIVACY 360

INVISUS

InfoSafe

Data Breach Risks & Trends

- Confidential personal and business information is the new global currency of thieves
- Over 6 billion records compromised in 2017
- 85% of breaches are at small businesses
- 49% of breaches caused by employees
- Ransomware – 4,000 businesses a day held hostage
- Owner, executive accountability and liability
- Cyber insurance demand

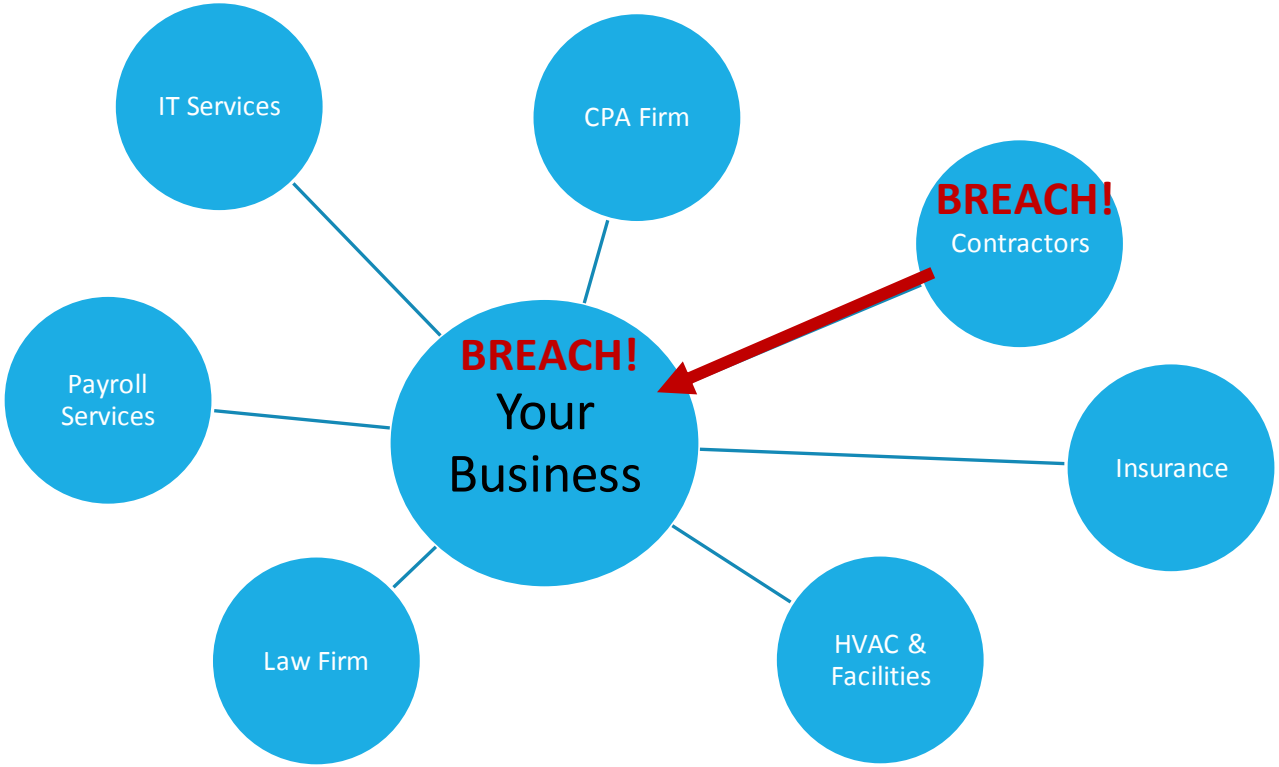
Source: IRS, FTC, U.S. Office of Civil Rights, ITRC, Breach Level Index

How Breaches Happen

- Hacking/Cyberattacks
- Employee Error/Negligence
- Insider Theft
- Email/Internet Exposure
- Physical Theft
- Vendors/Service Providers

Third Party Risks

- Your vendors and service providers can put your business at risk



What Qualifies as a Data Breach?

An incident in which any confidential personal or business information is *potentially* exposed, lost or stolen; including:

- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Personal Financial Information (PFI)
- Other Confidential Information
  - Contracts, business client data, intellectual property

The Financial Risk

If <u>your business</u> suffers even a small breach:

- Direct Costs (avg. $225 per record)
  - Investigation, PR, victim notification/remediation
- Regulatory Fines & Penalties
- Business Disruption
- Reputation Damage
  - Up to 33% of customers consider leaving
- Civil lawsuits

Example:

Only **1,000** records compromised:

➢ $225,000 in response and recovery costs

Source: Cost of Cybercrime Study 2017, Ponemon Institute

Identity Theft Statistics

- #1 crime in the country
- 6 billion records hacked in 2017
- 15.4 million victims in 2016
- 1 in 10 children are already victims
- 116 million SSNs compromised
- 1 in 3 Americans are victims of health care data breach
- 2 out of 3 Americans have been affected by data theft

Types of Identity Theft

- Child
- Tax
- Medical
- Government Benefits
- Financial
- Criminal
- Synthetic

Identity Theft is not just about Credit Cards!

Pressure from Customers

Businesses face **growing demand** to **provide proof** they meet minimum information security regulations and standards.

- Security **assessments** and **questionnaires** from customers
- The "**Business Associate**" regulatory requirement
  - If your customer is required to be compliant with any government or industry regulation, your business must also be in compliance.
- **Contractual requirements** in business, service agreements

Federal, State Regulations

- **Federal Laws**
  - HIPAA-HITECH (personal health information)
  - GLBA (financial info & services)
  - Red Flags Rule
  - 2017 - New laws coming
- **State Data Breach Laws**
  - 48 states
  - D.C., Guam, Puerto Rico and the Virgin Islands
  - Must be compliant where customers reside

International Regulations

- **EU – GDPR** (General Data Protection Regulation)
  - U.S. businesses must protect all personal data for individuals or businesses from any of the 28 EU countries
  - Penalties up to 4% of your annual revenue
- **Canada - PIPEDA**
  - National data privacy protection law covering all types of personal information
  - Several Canadian provinces also have data privacy laws

PIPEDA

Other Data Security Standards

- **PCI-DSS** (credit card security standards)
- **SOC 2** (AICPA/financial security audits and reports)
- **ISO 27001** (security audits & reports)
- **NIST** (Nat'l Institute of Standards & Technology)
- **ABA** (American Bar Association)
- **NAIC** (Nat'l Assoc. of Insurance Commissioners)

10 Key Areas of Compliance

1. Management Commitment, Assigned Responsibility
2. Information Security Plan (policies & procedures)
3. Regular Risk & Compliance Assessments
4. Technical Safeguards (security, monitoring, testing)
5. Physical Security

10 Key Areas of Compliance

6. Human Resource/Employee Training
7. Business Associate/Vendor Security
8. Business Continuity/Disaster Plan
9. Breach Response Plan
10. Ongoing Review, Testing, Updates to Policies & Controls

There are 60 to 80 unique information security and privacy requirements or best practices within these categories that your firm should follow and provide evidence of compliance.

Breach Prevention & Compliance

A new management responsibility
…and principle of business success.

Business Basics

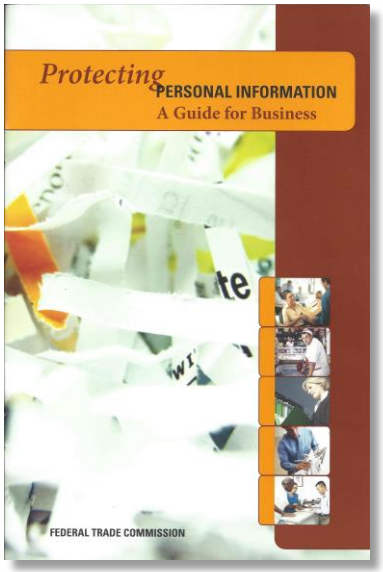
1. **Get executive level support and commitment**
   - Owners, executives must understand the risks and liabilities
   - Translate “security” into business planning
   - Investment in cybersecurity and a formalized compliance management program
   - Top down culture of security and privacy

2. **Assign responsibility and centralize the administration of your breach prevention & compliance program.**
   - Compliance Administrator – or Information Security Officer
   - All departments, functions collaborate

Business Basics

3 **Implement an Information Security Compliance Program.**

1. Formalized "Information Security Plan" (policies & procedures)
   a) Administrative, Physical and Technical Safeguards
2. Regular risk & compliance assessments
3. Implement necessary safeguards
4. Training – all personnel, ongoing
5. Secure 3rd party service provider relationships
6. Incident response plan
7. Consider cyber-liability insurance



Business Basics

4 **Audit readiness and legal defensibility.**

- Reports/Documentation - information security & compliance
- Regular program updates (keep it current)

5 **Customer trust and privacy assurance.**

- Provide customers with information privacy notice
- Ability to respond to requests for security audits from customers
- Show 3rd party certification

What Are Your Options

- **Hire a Consultant** – large organizations, expensive
- **Do It Yourself** – templates, not comprehensive
- **Do Nothing** – hope and pray
- **Use a Qualified 3rd Party Vendor** – small to medium-size organizations, cost effective

Thank you!

Q & A

Mark Conboy

561-339-2256

mark@privacy360.us