Responding to Client Cybersecurity Questionnaires

Presented by
James Harrison

OM30
5/5/2018
8:15 AM
We will cover

- Understanding Data Breaches
- What to Expect with an Audit
- Major Cybersecurity Standards and Regulations
- The 10 Key Areas of Compliance
- Key Recommendations
Understanding Data Breaches

What qualifies as a “Data Breach”? An incident in which confidential personal or business information has been exposed, lost or stolen; including:
- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Personal Financial Information (PFI)
- Other Confidential Information
**Personally Identifiable Information (PII)**

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

**Personal Health Information (PHI)**

- Medical Records/History
- Health Insurance/Employee Benefit Plans
- Treatment/Medication
- Medical Billing/Claims
Personal Financial Information (PFI)

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

Other Confidential Information

- Business information
  - Financials, accounting, banking, tax
  - Corporate filings, legal documents
  - HR, employee information
- Intellectual property, trade secrets
- Law enforcement records
How Data Breaches Happen

- Hacking/Cyberattacks/Email Phishing
- Employee Error/Negligence
- Insider Theft
- Physical Theft
- 3rd Party Vendors/Service Providers

Third Party Risks

- Your vendors and service providers can put your firm and your clients at risk!
Law Firms Targeted

Cybersecurity surveys of law firms:

- **100%** of firms subjected to hacking attempts
- **25%** of law firms report confirmed data breaches
- **40%** were breached and “unaware”
- **63%** of law firm attacks linked to 3rd party vendors/business associates
- Ransomware attacks increasing (DLA Piper)


The Financial Risk to Firms

If your firm suffers even a small breach:

- **Direct Costs** (avg. $225 per record, $398 medical)
  - Forensics, investigation, audits, PR
  - Victim notification, remediation
- **Regulatory Fines & Penalties**
- **Business Disruptions**
- **Reputational Damage, Client Loss**
  - Up to 33% consider leaving
- **Civil lawsuits** *(ex. Johnson & Bell)*

Example:
Only **1,000** records compromised:

- **$225,000** in response and recovery costs

Source: Cost of Cybercrime Study 2017, Ponemon Institute
Recent Firms in the Headlines

Growing Demand for Compliance

- Pressure from clients to invest and focus on cybersecurity
- 48% of firms subjected to cybersecurity audits last year
- Client-required information security audits doubled in 2017
- RPF, contractual requirements
- Annual audits, risk scorecards, security benchmarks
- Win/lose new clients

Source: Law.com, LogicForce Survey
What to Expect with a Cybersecurity Audit

Who will Audit Your Firm?

- Business clients (healthcare, insurance, financial services, etc)
- Corporate legal departments
- Government agencies (post breach)
  - OCR (Office for Civil Rights)
  - Federal Trade Commission
  - Federal and state attorneys general

Source: Law.com, LogicForce Survey
How are Audits Done?

- Self Assessment Questionnaire (SAQ):  
  - 80 to 200+ questions  
  - Different formats – spreadsheets, PDFs, online

- Short survey (10-20 questions)

- Audit review calls  
  - Further questions, clarification of answers  
  - Involves administrator, HR, IT manager, etc.

- Onsite visit sometimes required

- Based on major industry standards and regulations

Source: Law.com, LogicForce Survey

The Major Cybersecurity Standards and Regulations

(*the basis for audits*)
Primary Corporate Cybersecurity Standards

- **PCI-DSS** (credit card security standards)
- **FFIEC/SOC 2** (banking/financial security audits and reports)
- **ISO 27001** (International corporate standard, certification)
- **NIST Cybersecurity Framework** (Dept. of Commerce, National Institute of Standards & Technology)

---

U.S. Federal Regulations

- **HIPAA-HITECH** (medical, healthcare)
- **GLBA** (financial services)
- **FFIEC** (banking)
- **Data Security & Breach Notification Act** (*coming soon?*)
  - Specific requirements for protecting confidential data and responding to data breach incidents
U.S. State Regulations

**State Data Breach Laws**
- All 50 states, D.C., Guam, Puerto Rico, Virgin Islands
- Information security requirements differ by state
- Breach response requirements differ by state
- Must comply with state laws where victims reside

NY Dept. of Financial Services Cybersecurity Law

- **Who must comply?**
  - All NY licensed financial services companies (banks, investment services, insurance, etc.)
  - Any service providers (i.e. law firms) that do business with financial services companies that are doing business in NY
- Must maintain and follow a compliant information security plan
- Must **certify** with the state of NY annually
International Regulations

- **EU – GDPR (General Data Protection Regulation)**
  - U.S. businesses must protect all personal data for individuals or businesses from the 28 EU countries
  - Incl. law firms that handle EU data as a 3rd party service provider
  - Penalties up to 4% of your annual revenue

- **Canada - PIPEDA**
  - National data privacy protection law covering all types of personal information
  - Applies to all private sector businesses, organizations
  - Several Canadian provinces also have data privacy laws

10 Key Areas of Cybersecurity Compliance
(areas you’d be audited)
Areas of Compliance

1. Information Security Plan
2. Management Commitment
3. Risk & Compliance Assessments
4. Technical Safeguards
5. Physical Safeguards

Areas of Compliance

6. HR/Employee Training
7. Vendor Risk Management
8. Business Continuity
9. Breach Response
10. Review and Update

There are 100+ specific information security controls within these categories that your firm should follow and be able to provide evidence of compliance.
1. Information Security Plan

The firm’s documented plan detailing current information security policies, procedures and responsibilities

...for protecting confidential information against unauthorized access or inadvertent disclosure.

2. Management Commitment

Owners and executives are committed to safeguarding confidential client information

...by investing in and focusing on security

...by implementing and enforcing the firm’s Information Security Plan and promoting a culture of security.
3. Risk & Compliance Assessments

Regular assessment and review of current security policies and practices

...in order to identify areas of risk and implement appropriate security measures responsive to those risks.

4. Technical Safeguards

Technical security measures to prevent, detect and stop cyber attacks

...including network, website and computer security, data encryption, data backup, vulnerability testing, telecommuting security, mobile safeguards, etc.
5. Physical Safeguards

Security measures to prevent unauthorized physical access to offices, paper documents and computer equipment.

6. HR/Employee Training

Regular cybersecurity awareness training and education for all personnel

... based on firm’s security policies/procedures
7. Vendor Risk Management

Cybersecurity assessments and agreements for 3rd party vendors and service providers that have access to client data

...to ensure they have implemented and follow minimum industry or regulatory security standards.

8. Business Continuity

The firm’s policies and procedures for ensuring the continued security and availability of client data during an adverse or disruptive event

...such as technology failure or environmental disaster.
9. Breach Response

A detailed plan for detecting, responding to, and recovering from information security incidents
...to minimize financial and reputational impact.

10. Review and Update

Regular assessment, review and update of the firm’s Information Security Plan, employee training program, breach response plan, and other security measures.
Taking Action:

Key Recommendations for being “Audit-Ready”

Key Recommendations

1. Create **awareness and a “need for action”**
   - Partners, executives must understand the risks and liabilities
   - Exec training, industry news/articles (Legal Management, etc.)
   - Have an outside Risk & Compliance Assessment done
Key Recommendations

2 Get executive support and commitment
   ▪ Translate “information security” into core business planning
   ▪ Commit to investing in tools and resources
   ▪ Create a top down culture of security and privacy

3 Assign responsibility for your information security compliance efforts.
   ▪ Create an information security compliance team
     - Administrator, COO
     - IT Manager, CTO
     - Human Resource Director
     - 1 or 2 Managing Partners
   ▪ Designate an Information Security Compliance Manager, CPO or CISO
Key Recommendations

4 **Conduct a full Risk & Compliance Assessment now.**
   - Identify security and compliance gaps
   - Risk scorecard, security benchmarks
   - Measure potential financial risk
   - Involve administration, operations, HR, IT

5 **Implement/update your Information Security Plan.**
   - Reasonable and appropriate policies and procedures
   - Compliant with government, industry, client requirements
   - Training for all personnel
   - Secure 3rd party vendor, service provider relationships
   - Incident response plan, testing
Key Recommendations

6 Prepare for cybersecurity audits.
   - Establish internal audit response processes
   - Assign responsibility, train
   - Get 3rd party independent compliance certifications and reports

Tip for Administrators

Get a good information security Compliance Management program:
   - Risk and compliance assessment tools, support
   - Create and maintain your Information Security Plan
   - Implementation tools, resources, status reports
   - Employee training
   - Vulnerability testing & reports
   - Breach response plan, crisis management services
   - Compliance certifications, documents & reports
   - Automatic updates and reminders (keep you current)
   - Expert guidance and support
Tip for Administrators

Simple and affordable compliance management for law firms

Thank you!

For more information:

James Harrison
james@invisus.com
(801) 724-6211
Your opinion matters!

Please take a moment now to complete the evaluation.

Thank You!