So You Think You've Had a Data Breach - Now What?

Presented by
James Harrison
Alan Wilson

OM35
5/5/2018
3:00 PM
So you think you’ve had a data breach. ...Now what?

JAMES HARRISON

We will cover

- Understanding Data Breaches
- What to do BEFORE a Breach
- Responding to a Data Breach
- Keys to an Effective Incident Response Plan
- Protection with Cyber Liability Insurance
Understanding Data Breaches

What is an Information Security “Incident”? Any security event that compromises the integrity, confidentiality, or availability of client or firm information such as:

1. Virus, malware attack (including ransomware)
2. Network system failure; denial of service attacks
3. Unauthorized information access or disclosure
4. Unauthorized facility entry
5. Document mishandling, disposal
6. Loss or theft of computer equipment
What qualifies as a “Data Breach”?

Any 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
Law Firms Targeted

*Cybersecurity surveys of law firms:*

- **100%** of firms subjected to hacking attempts
- **25%** of law firms with over 100 attorneys have already had one or more confirmed data breaches
- **52%** of firms with 10-49 attorneys reported a cybersecurity or data breach incident
- **40%** were hacked and “unaware”
- **63%** of law firm attacks linked to 3rd party vendors/business associates
- Ransomware attacks increasing (DLA Piper)

*Source: Law.com, LogicForce, American Bar Association Survey 2015*

Recent Firms in the Headlines
The Cost of a Breach

**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*

---

What you can do now – **BEFORE** a Breach
Be Prepared. Minimize Damages.

- Create your Cyber Risk Management team
- Have a comprehensive Information Security Plan
  - Get compliant with data security regulations and industry best practices (Have evidence of compliance!)
- Have a Breach Response Plan
- Get cyber liability insurance (more later)

Get Familiar with Breach Response Regulations and Industry Standards
U.S. Federal Regulations

- **Federal Laws**
  - HIPAA-HITECH (personal health information)
  - GLBA (financial info & services)
  - Coming soon! *Data Security & Breach Notification Act*
    - 30 days to notify customers
    - 5 year jail sentence for concealing a breach

U.S. State Regulations

**State Data Breach Laws**

- All 50 states, D.C., Guam, Puerto Rico, Virgin Islands
- Response requirements vary by state
  - *Definition of a breach incident*
  - *Time period to notify affected persons*
- Must comply with laws where victims reside
- Special state regulations:
  - *NY Dept. of Financial Services data security compliance*
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
  - 72 hour breach notification requirement
  - 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 organizations
  - Several Canadian provinces also have data privacy laws

Typical Corporate-Required Cybersecurity 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)
Common Breach Response
Regulatory Requirements

- Proper investigation, analysis of the security incident
- Timely reporting to authorities
- Time limit for breach notification to affected persons
- Provide free identity protection, credit monitoring

What if it happens...
...When it happens
How to Respond to a Breach
Botched Responses = Disaster

What is a botched response?
- Lack of management concern, action
- Poor investigation, slow discovery
- Failure to report to authorities
- Negotiating with hackers, paying ransom
- Delayed or no notification to victims
- Failure to provide monitoring, recovery services

Benefits of Proper Response

With advance preparation, your firm can:
- Meet regulatory requirements for breach response
- Defend against regulatory fines, penalties
- Protect your firm’s reputation
- Minimize breach response costs (notification, remediation)
- Minimize recovery costs (investigation, fixes, consulting)
- Minimize downtime, impact on billable hours
Surviving a data breach starts with having a good Incident Response Plan

Incident Response Plan (IRP)

What should your IRP include?
1. Incident response team
2. Monitoring and incident reporting
3. Insurance, service provider notification
4. Investigation, analysis
5. Containment
6. Security updates, corrective action
7. Breach Response plan (for confirmed breach)
8. Review and update process
Breach Response Plan

Steps for handling a confirmed data breach incident:

1. **Breach notification to affected persons**
   - Within required time frames (federal, state laws, GDPR)
   - Mail, email, public announcement

2. **Notification to business client (owner of customer data)**
   - Decide whether to involve in breach response actions

3. **Reporting to authorities**
   - Follow regulatory requirements
   - Management discretion; legal counsel

4. **Victim remediation**
   - ID theft monitoring, recovery
   - Customer support call center
   - Website instructions, FAQs

5. **Communications/PR strategy**
   - Involve from the beginning to ensure consistent message
   - Limit communication when sharing information with employees, clients, vendors, law enforcement
Protecting the Firm with
Cyber Insurance

Alan Wilson

KEY TYPES OF CYBER BREACH EXPOSURE

- Responsibility for another’s data breach
- Lawsuit defense
- Fines and penalties
- Website and systems interruption
- Loss of income
- Digital forensics
- Breach notification, credit monitoring
- Restoration of data
- Ransomware
- Cyber deception
MOST SMALL BUSINESSES ARE NOT PREPARED FOR A DATA BREACH

Who will:
- Determine if breach actually occurred?
- Clean up the systems and restore data?
- Notify customers?
- Provide legal guidance and protection?
- Advise in a ransom scenario?
- Who will pay for all of this?

Specific exclusions exist in virtually all other commercial insurance policies for violations of privacy, loss of data, personal injury in online environment – and the trend is not going in the insured's favor.

DATA BREACH COST CALCULATOR
WHAT IS CYBER INSURANCE?

Insurance coverage designed to protect a business from:

- **Liability**
  - Unauthorized release of confidential information
  - Violation of a person’s rights to privacy
  - Personal injury in an electronic/social media environment
  - Intellectual property infringement
  - Violations of state or federal privacy laws
- Out-of-pocket expenses incurred to make the above problems go away

WHAT A CYBER INSURANCE POLICY SHOULD COVER

**Liability (3rd Party):**

- **Privacy Liability** – private info gets out, client gets sued
- **Privacy Regulatory Claims Coverage** – private info gets out, gov’t investigates/fines
- **Security Liability** – network gets breached, network transmits virus, etc. client gets sued
- **Multimedia Liability** – client responsible for IP infringement or personal injury online environment, clients gets sued
WHAT A CYBER INSURANCE POLICY SHOULD COVER

First Party:
- **Security Breach Response Coverage** — legal assistance, IT forensics, notification expense, PR, credit monitoring, call center services, etc.
- **Cyber Extortion** — expenses associated to mitigate an extortion threat or ransom
- **Business Income and Digital Asset Restoration** — lost $ due to covered network disruption
- **PCI DSS Assessment** — fines/penalties associated with breach of cardholder data
- **Cyber Deception (optional)** — loss of $ the insured willingly releases, based on fraudulent instruction

CONSIDERATIONS WHEN EVALUATING CYBER INSURANCE

- 24-Hour breach response team?
- Pre-breach services? Risk-management tools?
- Cyber Deception Coverage?
- Paper documents covered?
- Voluntary notifications available?
- Encrypted data exclusion?
- Prior acts covered?
INCIDENT RESPONSE

- **Response**
  - Is event real? >> Incident response plan
  - Breach Coach / Security Expert

- **Contact Law Enforcement?**

- **Notifications**
  - Contact Legal Counsel
  - Refer to State/Federal breach laws

- **Forensics and Breach Investigation**

---

INCIDENT RESPONSE

- **Remediation**
  - Credit Monitoring

- **Lawyers**
  - Defense of Civil Suits / Regulatory Fines and Penalties

- **Insurance Claim**

- **Public Relations**
STRONG CYBER INSURANCE POLICY COVERAGES

- Privacy Liability (including Employee Privacy)
- Privacy Regulatory Claims Coverage
- Security Breach Response Coverage
- Security Liability
- Multimedia Liability
- Cyber Extortion
- Business Income and Digital Asset Restoration
- PCI DSS Assessment
- Cyber Deception (Endorsement)
- GDPR Coverage

EDUCATE YOURSELF
ALACyber.com
Thank you!

For more information:

James Harrison, InfoSafe
james@invisus.com
(801) 724-6211

Alan Wilson, BreachPro
alan@gljinsurance.com
Your opinion matters!

Please take a moment now to complete the evaluation.

Thank You!