

Trials & Tribulations: Cyber & Privacy Risks for Lawyers

July 31, 2015

Kari A. Timm



Michael Flanagan



Law Firm Cyber & Privacy Risks in the News

- Mar. 2015: Citigroup issues internal report warning of threat of attacks through law firms and criticizes firms for not reporting breaches
- Aug. 2014: Criminal defense firm Imhoff & Associates suffers reportable data breach after an unencrypted hard drive is stolen from his trunk
- Nov. 2013: McKenna Long & Aldridge suffers breach of employee information when third party used client's login credentials to access vendor database
- Feb. 2012: Puckett & Faraj attacked by Anonymous; client information posted on YouTube, website shut down and computer files deleted
- 2012: Mandiant reports 80 of the 100 largest US law firms had a malicious breach in 2011
- 2010: Seven Toronto firms hacked in effort to derail \$40 billion acquisition; hack discovered in 2012; Chinese gov't suspected
- 2010: Gipson, Hoffman & Pancione hit by sophisticated phishing attack from China after filing \$2.2 billion infringement suit against People's Republic
- FBI warns law firms of cyber risks
 - 2009 – Issues advisory warning firms they are specifically being targeted by hackers
 - 2011 – Organizes meetings with top law firms to warn of computer security and corporate espionage; the “soft underbelly of clients”

Cyber & Privacy Risks: What are They?

Computer Related/Operational Risks

- Damage to a computer system, including loss or corruption of data, hardware damage or a system shutdown

Informational Risks

- Loss of, unauthorized access to or theft of personal or confidential information belonging to others; including improper disposal of information
 - Electronic or paper
- Data collection and use

How is A Computer Compromised or Confidential Data Disclosed?

- Mistake: inadvertent disclosure
- Careless: lost equipment with no password protection or encryption; return or sale of office equipment with hard drives
- Inadequate Security: ineffective firewall; outdated virus programs
- Malicious: malware, DOS, botnet; unauthorized access (by insider or outsider); stolen equipment
- False Pretense: phishing; smishing; spoofing

Estimated Breach Costs

- Ponemon 2015 Costs of Data Breach Study
 - Average cost of breach - \$3.5 million (Globally); \$6.5 million in U.S.
 - US is most costly region - \$217/record
 - Cost higher for criminal or malicious attack - \$230/record (Compare to \$210/system glitches & \$198/human error)
- NetDiligence Cyber Claims Study 2014
 - \$956.21 average cost per record; \$19.84 median cost per record
- Verizon 2015 DBIR
 - Cautions against relying on per record costs; Suggests cost could be as low as \$0.58

Breakdown of Claims Costs

(NetDiligence Cyber Claims Study 2014)

- \$62.3 million in payouts on 85 claims
 - 48% on Crisis Services
 - Up to \$1.5 million in Forensics
 - Up to \$6.15 million in Notification Costs
 - Up to \$2.5 million in Legal Guidance
 - Up to \$135,000 in Public Relations
 - 15% of Legal Defense
 - 10% of Legal Settlements
 - 10% on Regulatory Defense
 - 6% on Regulatory Fines
 - 11% on PCI Fines

Factors Affecting Breach Costs

(Ponemon 2015 Cost of Data Breach Study)

Decrease

- Incident response team (-\$23.80)
- Extensive use of encryption (-\$19.00)
- CISO appointment (-\$12.20)
- Employee training (-\$11.00)
- Board level involvement (-\$9.80)

Increase

- Third party involvement in breach (+\$29.00)
- Quick notification (+\$12.70)
- Lost or stolen device (+\$12.00)
- Engagement of consultants (+\$2.40)

Notification

State Breach Notification Statutes

- Intended to mitigate the risk of consumer fraud and identity theft by requiring prompt notification of unauthorized access to personal information
- 47 states, DC, Puerto Rico and US VI
- Common features; but specifics differ
 - Coverage
 - Notification trigger
 - Notification
 - Timing
 - Remedies
 - Enforcement

Health Insurance Portability & Accountability Act (HIPAA)

- Established national standards to protect personal health information
- Pertains to “covered entities”
- Privacy Rule
 - Protects medical records and personal health information
 - Limits use and disclosure of personal health information
 - Gives patients the rights to obtain, examine and request correction of their health records.
- Security Rule
 - Requires safeguards to ensure confidentiality and security of electronic health information

Health Information Technology for Economic & Clinical Health Act (HITECH)

- Extends HIPAA to “business associates”
- Mandatory breach notification
 - Notice within 60 days
 - More than 500 affected individuals requires notice to HHS within 10 days and to prominent media outlets
 - Notice to include:
 - Description of what happened
 - Types of personal health information involved
 - Steps individuals can take to protect themselves
 - Steps covered entity is taking to investigate breach and mitigate its effects
 - Contact information for affected individuals to use to obtain additional information regarding breach

HITECH Continued...

- Increased tiered penalty structure (\$1.5 million cap)
 - No knowledge of breach
 - \$100 - \$50,000 per violation
 - Reasonable cause
 - \$ 1,000 - \$50,000 per violation
 - Willful neglect (Corrected)
 - \$10,000 - \$50,000 per violation
 - Willful neglect (Not corrected)
 - At least \$50,000 per violation, but up to \$1.5 million
- Mandatory penalties for “willful negligence”
- Criminal penalties may be imposed
- Grants authority to State AGs to bring actions
- Periodic audits by HHS
- Annual reports to Congress

Help! I've had a breach. Now What?

- First and foremost – retain privacy counsel
 - Attorney-client privilege
 - Documentation of incident and response
- Retain forensic consultant
- It's your reputation – is a PR firm necessary?
- What about notice to affected individuals?

Breach Notification Considerations

- Is it required?
 - If not, is there a benefit or other need?
- Timing of notification
 - Do not rush to notify; But what about the nosey media?
 - Law enforcement may delay notification
- Who must be notified
 - Affected individuals
 - Government or regulatory agencies
 - Banks
 - Media
- Drafting the notification letter
- Credit Monitoring: To offer or not?

How to Protect Your Firm from a Breach

Data Security Practices

- Know what information you have and where it is stored
 - Outside Vendors
 - Office equipment with hard drives
 - Mobile devices & portable storage devices
- Make sure system is kept up to date
- Require strong passwords that are changed frequently
- To encrypt or not to encrypt...that is the question
- Regular, off-site back-up
- Employee training/education

Incident Response Plan

- Develop & implement one!
- Create an incident response team
- Assess your risk
- Create an internal communication & decision making chain
- Identify outside service providers (i.e., privacy counsel, forensic experts, etc.) & clear them with your insurers
- Educate and train the necessary employees

Insurance Coverage: E&O v. Cyber

■ E&O Policies

- Must arise out of professional services
 - Breach of client data v. breach of employee data
- Wrongful Acts are usually negligent
- Damages may be limited; no first party costs

■ Cyber Policies

- Cover first and third party costs
- Cover intentional and negligent breaches
- Typically provide access to team of experts

Typical Coverages Offered

- Third Party
 - Privacy and Security Liability
 - 3rd Party Lawsuits (Defense and Indemnity)
 - Governmental and Regulatory Actions (Defense; Indemnity?)
 - PCI Investigations and Fines
- First Party
 - Crisis Management/Breach Response
 - Forensics
 - PR Consultants
 - Credit Monitoring/Identity Theft Insurance
 - Call Center
 - Data Restoration
 - Business Interruption
 - Cyber Extortion

Assessing Your Cyber Risks & Insurance Needs

- Know your data exposures
 - What, where and how much data do you collect and store
 - How is your data stored, backed up and accessed
- Profile industry based incidents
- Know your potential damages
- What coverage do your peers buy; in terms of both scope and amount
- Are you an attractive target
 - Do you handle mergers and acquisitions or intellectual property matters
 - Do you routinely collect vast amounts of PII/PHI in connection with cases
 - Do you accept credit card payments

Trials & Tribulations: Cyber & Privacy Risks for Lawyers

July 31, 2015

Kari A. Timm



Michael Flanagan

