Data Security & Privacy in the M&A Transaction

Association of Corporate Counsel – Charlotte Chapter
October 1, 2014

Presented by:

C. Andrew Konia
akonia@mcguirewoods.com
703.712.5071

Clare M. Lewis
clewis@mcguirewoods.com
434.977.2530

Ashley Matthews
amatthews@mcguirewoods.com
434.977.2570
Agenda

- Background, facts and figures
- Pre-deal diligence
- Negotiating the transaction
- Post-deal monitoring and management
Current Challenges

- Privacy (do unto others) and Security (done unto you)
- Various/conflicting government/quasi-government regulation/legislation
  - Agency level: FTC (§5), FFIEC, CFPB, NSA, SEC, DOE/OE, FERC, HHS, State AGs
  - Legislation: FCRA, GLBA, HIPAA, State Laws, EU DPD, etc.
  - Executive Branch (President’s February 2013 Executive Order)
  - Judicial interpretation
  - Industry groups/self-regulation: NTIA, PCI, ISO 27000 series, NIST, Institutional policies, etc.
- Cross-border transfer issues
- Contractual requirements (clients and vendors)
- Vendor failure (e.g., Target)
- Pervasive privacy concerns; “Hacktivism”; competing positions; ACLU involvement
Current Threats

Why does it matter?

▪ Any of these types of information…
  • Credit card/consumer financial (PII)
  • Personal Health Information (PHI)
  • Customer lists/Trade Secrets
  • Employee information (PII)

▪ …can be lost/stolen/abused…
  • Negligence (internal/external)
  • Intentionally harmful activity (internal/external)
  • Malware

▪ …resulting in…
  • Lawsuits, suspension/probation, reputational damage/loss of trust, breach of contract, fines (even without breach/damages), fiduciary issues
Price Tag/Consequences

- Breach-specific costs: wide variation in estimates
  - Studies: averages as low as $537,000; as high as $7.2MM
- Noncompliance
  - Possible agency sanctions; State AG actions for nondisclosure of breach
  - Audits (may be worst consequence)
  - Actual damages may be irrelevant
- Data Security Breach; Lawsuits
- Reputational Damage
  - Even without breach or noncompliance
  - Whistleblowing
  - Exponential effect of social media
- Director/Officer Liability; Fiduciary Duties (think Target)
Facts and Figures – General

- Hackers realize $445 billion in revenue
  - If consolidated, hacking would now be largest business in the world
  - Largest transfer of wealth in history
  - 150,000 job losses in EU; 200,000 in US, annually (6/9/14, CSIS)

- Since 2002: victim also the defendant

- Evolving data security standards raise the bar for adequate security (both litigation and regulatory)
  - Court provable security v. budgeting

- Who are the bad guys?: 87% outsiders; 46% insiders

- Lag in detection: Days (22%); Weeks (12%); Months (53%)
Facts and Figures – Effects on Valuation

▪ Average consolidated cost of lost record = $201 per record
  • Increase of 15%
  • Used in calculating damages and insurance recovery

▪ Key aggravating factors
  • Malicious/criminal attack (quality of breached information): ↑ $45
  • Stolen devices: ↑ $16
  • Involvement of multiple parties: ↑ $15
  • Repeat breach, type of records breached, location of breach, publicity

▪ Key mitigating factors
  • Strong security posture: ↓ $14
  • Comprehensive incident response plan: ↓ $13
  • Prompt notification: ↓ $10
  • Engaging third party consultants: ↓ $2

Source: Ponemon Institute: 2014 Cost of Data Breach Study: Global Analysis
Deal Survey

- **Level of Concern**: 30% of Acquirers, 19% of Sellers are “very concerned” about cybersecurity issues derailing transaction

- **Importance of cyber-related issues to acquirers (% responses “important” or “very important”):**
  - Seller is proven victim of attack: 90%
  - Seller ineffectively handled past breach: 87%
  - Seller had business disruption (DDoS): 83%
  - Seller lacks adequate policy: 75%
  - Seller lacks cyber-insurance: 57%

- **Most affected industries from M&A transaction perspective:**
  - Financial services/insurance, Defense, Technology/software (Energy 6th)

*Source: Global Security Finance, 2014 Survey on Cyber Security and the M&A Process*
Deal Survey (cont.)

**Due Diligence**
- 78% say cybersecurity is not analyzed in great depth, BUT…
  - 56% say lack of adequate cybersecurity diligence process could terminate deal
  - 39% say creation of cybersecurity policy will be condition to closing

**Potential impact of breach during diligence phase or mid-deal**
(% responses “very likely” or “likely”):
- Enhance reps and warranties: 59%
- Change material deal terms: 55%
- Reduce valuation: 45%
- Abandon transaction: 23%

**Cyber-risks significantly affecting deal process:**
- past 12 months (21%); next 18 months (41%)

**Fiduciary/standard of care implications**

The Diligence Process

- Importance of sector-specific approach vis-à-vis compliance
  - FFIEC vs. HIPAA vs. DOE/OE/FERC, etc.

- Systems/Safeguards investigations (PTA analysis; view records)
  - Overall protection of PII (collection, encryption, storage, destruction)
  - Actionable FTC items: failure to…
    - Designate coordinator, identify risks, implement and test security measures, limit access to information, encrypt sensitive information (at rest or in transit), limit retention, provide training, impose security obligations on third parties

- Policy/Program investigation (including *implementation*)
  - The WISP; notification regime

- Team investigation (ERT)
  - Intracorporate, interdisciplinary; authority, mission statement, plan

- Breach incidents/Past legal compliance
The Diligence Process (cont.)

- Audits
- Vendor analysis; Outsourcing; Cloud Computing
- Analysis of customer contracts/standard Ts and Cs
- Insurance
- Requests specific to data security and privacy (see checklist)
- Effect of deal structure
- Transfer of information during deal process
- Compliance vs. Security
WISP (Written Information Security Program)

- What is it?
  - Must be a complete security program (not just individual “policies” or security “controls”)

- What does it do?
  - Proves implementation and maintenance of “appropriate measures” to protect information
  - Assigns responsibility (management buy-in)
  - IDs information assets (data mapping)
  - Calls for risk assessment
  - Selects, develops & implements security controls
  - Addresses third party issues
  - Incorporates comprehensive training (employees and vendors)
  - Includes ongoing monitoring, to determine effectiveness
  - IDs legal/regulatory requirements; Responds to changes
The Negotiations Process – Reps & Warranties

- Specific categories *(see handout)*
  - Data Security
  - Privacy Policy/Privacy Protections/Collection, Use & Sale of Data
  - Compliance with Laws
  - Disputes and Claims
  - Cross-border data flows

- Considerations
  - Public vs. Private deal (conditions to closing vs. indemnification)
  - Risk allocation
  - Materiality & knowledge qualifiers
  - Scope, exceptions & time periods
  - Joint & several liability
  - Disclosure schedules
The Negotiations Process – Other Provisions

- Holdback/Indemnification/Limitations on Liability
  - Possible expansion of scope, survival periods, caps (or minimize basket)
  - Escrow

- Conditions to Closing/Pre-Closing Covenants
  - Audits
  - Policy changes and compliance, internal or external (with notice)
  - Breach protection (with notice)

- Post-Closing Covenants
  - Audits
  - Use of data (sell-side)

- Transition Agreements
Post-Deal Monitoring and Management

- **Buy-side**
  - Audits (leading to indemnification/purchase price adjustment)
  - Board counseling
  - Policy and team management and implementation
  - Take advantage of vendor management rights
  - Cyber/intrusion insurance
    - General coverage (including D&O)
    - Cyber-specific coverage (first party & third party)
    - Exclusions & conditions
    - Best practices

- **Sell-side**
  - Transition obligations
  - Audit and activity verification
  - Use of data