Cyber Security Risk Management

For ACC America

November 6, 2014

Jim Halpert
Co-Chair Global Privacy & Security Practice
jim.halpert@DLAPiper.com
Trends

- Point of Sale Attacks
  - Malware
  - Skimming
- Industrial Control Systems and Critical Infrastructure
- Advanced Persistent Threats (APTs)
- Man-in-the-Middle Attacks
- Phishing/Spear Phishing
- Botnets
- Mobile device exploits
- SQL injection attacks
- Insider threats
Getting Started

- Map data in your systems – what’s where
- Classify data assets you need to protect by level of sensitivity
  (e.g. trade secrets, credentials, information subject to contractual obligations, information that would trigger data breach notice obligation)
- Track confidentiality obligations and label all information that must be protected
- Establish cross-organizational data governance team
- Processes must be tailored to work within organization’s operational and technical structures
Data Classification

- Define policies and processes to protect data in accordance with its level of sensitivity
- Train managers and employees to policies, processes
- Follow process every time an obligation is created & high risk information is received or created
- Identify point of contact for employee questions about labelling or confidentiality obligations
- Technical controls complementing operational process
- Conduct regular audits to discover vulnerabilities before issues arise
Cyber Risk – Board level issue

- Examples of Board level impact
  - Target CEO resignation this spring
  - ISS demanded that 9 directors step down
  - More than 80 class action lawsuits from the same incident
- Derivative suit against Wyndham Board that suffered several breaches
- These incidents pose Legal and Reputational Risk to Directors & C-suite
- There is difference between media focused and real risks
- BUT Congress, State AGs, regulators and the market respond to media risks → reputational risk must be taken seriously
- It is important to have strong policies and practices managed below Board level
  - Cyber security defense, incident response, pen testing, auditing
Board Governance Approach

- Board Role: Oversee the company’s cyber security program, *not manage it directly*
  1) Review reports from senior management regarding cyber security risks, cyber attacks, and cyber risk management plans
  2) Monitor whether the company is adequately managing cyber risk, including whether sufficient resources are devoted to cyber security
  3) Records should document oversight steps, briefings
Cyber Security Risk Governance

Enterprise-wide Governance

- Enterprise-wide risk, not just an IT risk
- Appoint a cyber risk management team with all substantial stakeholder departments represented (including Legal, Finance, HR, IT, and Risk Management)
  - Led by a senior manager with cross-departmental authority
  - Team reports to the full Board or Committee of the Board
- Develop incident response and preparation protocols
  - Breach response protocol, tabletop exercises, review contractual obligations with vendors/customers
- Clearly establish cross-departmental ownership and roles and responsibilities
Keeping Up with Changing Threat Landscape

- Highly dynamic risk, so team should:
  - Meet regularly and develop reports to the Board
  - Track and report metrics that quantify the impact of cyber threat risk management efforts
  - Include evaluation of cyber threat risk environment and management as part of regular reviews, e.g.:
    - Current state of threats & defenses at peer entities
    - Qualified reviewers of logs for suspicious activity
    - Conducting penetration testing
    - Examining and updating white lists & black lists for threat actors
    - Maintaining incident response preparedness
    - Legal requirements review
Board IT Expertise

- Emerging Board Recruiting Need: expertise to oversee company cyber security programs
- 3 Options in use at Public Companies:
  - Board member with technical expertise who receives briefings or
  - Briefings from third party experts, government agencies, etc., or
  - Using independent advisors (external auditors, outside counsel) who have a multi-client, industry wide perspective
Cyber Security Risk Governance

Overseeing Risk Management Strategy

- Oversee development and adoption of risk management plan
- Assess the cyber risks facing the company
  - What “crown jewels” need to be protected at all cost
    - E.g., IP, business strategy, breach notice data, credentials
  - Need to have multiple layers of security behind the firewall
  - Oversee continuous evaluation of sufficiency
- Which cyber risks to avoid, accept, mitigate or transfer through insurance
  - Evaluate plans associated with each decision and if resources are sufficient to achieve desired protection
- Ensure budget is sufficient and appropriately allocated
Risk Analysis and Management Strategies

- Determining your current state of security
  - Internal assessments and audits (incl. network architecture)
  - Vulnerability and penetration testing (internal and external)
  - Bounty programs
  - Third party partners/vendors

- Remediation and mitigation
  - Closure of vulnerabilities, patch placement, and validation
  - OS/software/hardware upgrades
  - Improved segmentation, encryption and other strategies
  - Training and the human element
  - Remote systems and employees, and mobile devices
  - Improve intrusion prevention system/intrusion detection system (IPS/IDS) monitoring efficacy
Litigation and Regulatory Risk

- Class Action Litigation
  - Consumer oriented
  - Special classes (banks, business partners, and others)
- Card issuer litigation
- Shareholder derivative litigation
- FTC and State AG investigations and enforcement proceedings
- Breach of contract actions from/with partners
- Payment card brand fines and disputes
- Insurance coverage litigation
- Attacks on critical infrastructure could present worse claims
Incident Response Preparation and Practice

- Preparing a breach incident response plan
  - Team identification and mobilization (24 x 7 availability)
  - Role of counsel and the privilege in an investigation
  - Forensic and PR teams
  - Preventing data loss and immediate security changes
  - Securing evidence and logs, and documentation
  - Law enforcement involvement
  - Defining legal obligations vis-à-vis individuals, AGs, card brands

- Practice
  - Tabletop exercises with PR, counsel, forensics, C-suite
  - Training
  - Periodic updating (e.g., of team and contact info)
Investigating a Breach and Working with Law Enforcement

- Executing on the Incident Response Plan
  - Addressing conflicts or bias issues in assembling the response team
  - Leading the technical forensic examination
  - Need for immediate PR and/or notification to affected parties
  - Early (and transparent) contact with regulators

- Law Enforcement
  - Compliance with process for evidence
  - Covert investigations and delayed notification
  - Victim notification by law enforcement
  - Press
International Considerations

- U.S. laws follow the residency of the person whose data was breached, outside the U.S. sometimes country where are established

- Not uncommon for a breach to implicate 48 breach notice laws + international requirements
  - Affect both notice obligations and some investigative protocols
  - Privilege rules vary
  - Data protection law limits on investigations vary

- Consider where to investigate, to cooperate with law enforcement, to locate incident response team members
Vendor Risk Management Strategies

- Data Transfer Considerations
  - Who do you really need to have access to your network or risky data?
  - International transfers of personal data are regulated in much of the world
    - Apply even to intra-group transfers
    - Strategies for intra-group transfers by multi-jurisdictional companies
      - Binding Corporate Rules (EU compliance focused)
      - Intra-group data transfer agreement (can address EU and global privacy requirements)
    - Strategies for cross-border vendor transfers
      - Model Clauses (EU data in scope)
      - Template data processing language for all vendor agreements
  - Breach notice can expose violations
Vendor Risk Management Strategies

- In light of supply chain incidents such as Target’s, supply chain risk is very much a focus of regulators
  - FTC, financial services regulators, DoD, etc.
- Vendor screening now expected
  - Can draw on established standards, PCI-DSS 3.0, Cybersecurity Framework, ISO Family, SSAE 16
  - IT to work with legal on vendor security screening criteria
  - Procurement/legal imposes to extent possible through appendix
  - Develop and apply contract negotiation “playbook”
  - Track vendor security commitments and target agreements that need upgrading
Vendor Risk Management Strategies

FedRAMP Example:

- The Federal Risk and Authorization Management Program ("FedRAMP"), which applies to the acquisition of commercial and non-commercial cloud services
- Applies to all agencies or cloud service providers that use, host, or want to host Federal information in a cloud environment
  - FedRAMP requires Federal Agencies to secure cloud computing services in a unified manner by implementing a standard baseline set of security controls
  - Cloud Service Providers obtain a FedRAMP “authorization” after demonstrating compliance with stringent FedRAMP requirements, which include the NIST 800-53 Rev. 4 requirements
    - Amazon and Salesforce are examples of FedRAMP-compliant CSPs
Vendor Risk Management Strategies

- Contractual Provisions
  - Seek consistent contractual provisions that hold the supply chain fully accountable. Be specific where needed (e.g., comply with PCI-DSS) and broad (protect ALL information and PREVENT breach)
  - Reject the common supplier argument that they are “not your insurance policy”
    - If the supplier has access to sensitive data, part of their job is to protect it -- the supplier should not escape this responsibility
  - Information security, privacy, indemnification, limitation on liability, and warranty provisions are key
  - You will be accountable to others for your suppliers; if your supplier’s liability to you is capped at a small amount, you hold the bag
  - Audit rights/independent 3rd party audit are necessary to monitor compliance with agreement terms, laws and your commitments to others
Vendor Risk Management Strategies

- **Contractual Provisions**
  - Can shift security incident obligations by contract
  - Key Terms - notification to contract party of even suspected incidents, what indemnification covers, caps on indemnification
  - Want right to audit after incidents to assure remediation
  - And right to, cooperation with, transition to another provider after a serious incident
Vendor Risk Management Strategies

- Address the Broader Supply Chain Risk
  - You not only buy the risk of your contract “partners” but also their subcontractors and software and component suppliers
  - Many businesses do not take this risk into account adequately
    - Who else has effective access to my network/my data?
  - Be your own data detective, follow the data flows and ensure protection as appropriate each step of the way
  - Do not be lulled into the assessment that because we hired well-known Supplier X – everything must be ok
  - Have a regular, repeatable program that validates Supplier compliance throughout the chain with requirements before, during and after the contract signing process
  - Ensure Suppliers keep up with evolving threats; do not rely only on canned audit reports
In the U.S. notify:

- Individuals – with state time limits
  - Shortest are: Florida (30 days after discovery with 15 day extension), Indiana expects 30 days, IA, OH, VT (45 days)

- Card processors (for payment card data) uploading card numbers
  - Best done as soon as practicable to prevent potential card fraud

- State AGs or another state official in a few states
  - Shortest are: Puerto Rico Consumer Affairs Dept. in 10 days, VT 14 business days (unless swear on form provided on the AG’s website that have compliant info security and breach response plans)

- Specified content under different state laws
  - Usually have at least 4 forms of notice letters in nationwide breach

- Where major risk to individuals, good idea to call

- KrebsOnSecurity blog can leak breaches, pressure quick response
Breach Litigation

- Consumer class actions:
  - Standing has become more difficult to establish
    - Clapper v. Amnesty International made standing harder to establish
  - California has not followed (see Sony Playstation and Adobe litigation)
  - Plaintiffs counsel are getting more creative (see LinkedIn)

- “Special” class actions
  - Privity and economic loss doctrine defenses
  - Too early to tell: ongoing business relationships, sophisticated parties, significant resources

- Derivative litigation
  - Liability for Directors and Officers
  - Demand futility cases
  - Pre-suit demand cases
Expenses and Insurance

- Breach notice costs can be huge (Target, TJX)
- Ponemon Institute 2014 survey average - $200 per record affected
  - But significantly less if have an incident response program in place
  - Costs can include: forensic investigation, legal, PR, notice handling, call centers, class action litigation, payment card and regulator investigations and fines, SEC disclosures, business interruption, stock price fluctuations, loss of good will

- Cyber Insurance Market is Maturing
  - Can obtain coverage for most of the above costs
  - But not goodwill/reputational, or catastrophic losses
  - Review exclusions and limits carefully as well as any conditions
Sophisticated Oversight Questions

- How do you track what digital information is entering and leaving our organization and where that information is going?
  - Mature identity and access management systems, data loss prevention technologies and robust 24x7 monitoring of inbound and outbound communications are needed because Firewalls are commonly breached.

- How do you know who’s really logging into your network and from where?
  - Authenticate whether the person using legitimate credentials is actually that person using sophisticated 2-factor authentication, log-in location verification.

- How do you control what software is running on devices?
  - In addition to anti-virus and other anti-malware technologies, identify code running on systems, implement enforceable employee policies concerning information technology usage.
Sophisticated Oversight Questions

- How do you limit the information you voluntarily make available to a cyber adversary?
  - Have policies/training/enforcement re employees sharing information on social media sites, job postings that include company organizational structure, information technology skill requirements, etc.

- What does your cyber security organization look like and is it appropriately staffed?
  - Clear lines of accountability between senior security executive to the CEO along with a separately managed budget, with regular Board briefings. Clear, well understood communication re threats, various levels of intrusions and impact on the company.

- How extensive is employee training?
  - Enlist employees in the fight for cyber security. “Insiders” are the single biggest vulnerability to cyber attacks, so employee awareness programs can be among the most cost-effective interventions.