CLE @ Saul Ewing

Cybersecurity: More Than Just an IT Problem, it’s Everyone’s Problem

December 16, 2015
Wayne, PA
WELL-KNOWN RECENT CYBERATTACKS
WELL-KNOWN RECENT CYBERATTACKS (cont’d)
Types of Cyber Threats

• Advanced, Persistent, State-Sponsored Threats (APT)
  – Seeking information and strategic advantage
    • May exfiltrate information
    • May penetrate system and watch

• Organized Cybercrime
  – Seeking monetary gain or identity theft, so financial databases are often targeted
  – Short-term benefit until gap fixed
  – Market for stolen identities, financial information, proprietary information

• Individual Political Interest A/K/A Hacktivists
  – Seeking embarrassment or sensationalism

• Careless/Negligent loss of equipment/material
Where is This Coming From?

Verizon Data Breach Investigations Report:

- 98% of attacks are external
- 58% of data theft tied to activist groups
- 4% involve internal employees
- 1% or less involves business partners
- 81% utilize hacking
- 69% use malware
- 10% involve physical attacks on property / equipment
- 46% discovered the breach accidentally
IMPORTANT FACTS

• USA Today: 43% of companies have had a security breach

• The Sony Security breach was only 33rd on the list of 2014 security breaches by size – 32 larger security breaches than that of Sony in 2014

• Cybersecurity costs expected to increase 38% over the next 10 years

• Between 2009 and 2013, the number of cyber incidents doubled – 228,700 incidents in 2013

• Average cost = $200 per record to comply with notification laws

• Average cost of a security breach = $5.4 million, large breach cost estimate = $163 million
2015 Association of Corporate Counsel Study

- 1 in 4 Chief Legal Officers (CLO) experienced a data breach in the last 2 years
- Data/cybersecurity ranks only behind ethics/compliance and mergers/acquisitions in importance to CLOs
- Only 1 in 3 reporting companies carries data breach protection insurance
- According to the LA Times, cyberattacks jumped 44% in 2014 from 2013 statistics
- Lloyds of London reported that cyber crime costs exceed $400 billion per year
  - Lloyds also reported that by 2013 cybersecurity had risen to no. 3 on the list of concerns of boards of directors
- Cyber attacks are not limited to computer systems alone – at least one attack was reported to have used “smart” devices such as televisions and a refrigerator
- CSO Magazine/PWC 2015 study (of 500 respondents) found that:
  - 28% of the boards have no presentations from security leaders
  - 26% of security leaders make only an annual presentation to board
  - 42% did not view cybersecurity as a corporate governance issue
Federal Regulatory Response

• SEC/FTC response
  ▪ SEC Commissioner Aguilar – “[B]oards that chose to ignore or minimize the importance of cybersecurity oversight responsibility do so at their own peril.”
  ▪ “[E]nsuring the adequacy of a company’s cybersecurity measures needs to be a critical part of a board of director’s risk oversight responsibilities.”
  ▪ April 2014 SEC announced it would review 50 registrants to determine cybersecurity preparedness.
  ▪ FTC has begun over 40 actions against companies for failing to protect customer data.
Federal Regulatory Response (cont’d)

• Cybersecurity Information Sharing Act
  ▪ Passed the Senate on October 27, 2015
  ▪ Has to be reconciled with similar House bill
  ▪ Creates a voluntary threat information sharing vehicle with the Department of Homeland Security
  ▪ Includes liability protections from lawsuits for sharing certain types of information
  ▪ Provides some privacy safeguards for customers’ personal information
  ▪ Authorizes companies to use “countermeasures” – retaliatory actions aimed at disrupting or disabling computers of adversaries
  ▪ Critics dispute its usefulness and argue it might increase government surveillance and lacks sufficient privacy protections
State Regulatory Response

- 47 states and District of Columbia (no AL, NM, SD)

- Generic definition of personal information: An individual’s first name or first initial and last name plus one or more of following data elements: (i) Social Security number, (ii) driver’s license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account

- Frequent requirement to report to state official/AG

- Most laws require notification whenever there is a breach

- Some states require mandatory credit reporting!
State Regulatory Response Cont’d.

• **New Trend (CA, FL)** – user name and password breach now requires notification

• **NJ, MT and WY have already updated in 2015**
  - NJ: 1/15 – requiring health insurers to implement specific protections for computerized personal information data
  - MT: effective 10/1/15 adds medical record information, TIN, and AG notification
  - WY: effective 7/1/15 adds “shared (login) secrets or tokens known to be used for database authentication,” user name and password, birth or marriage certificate, medical information, health insurance information, biometric data, and TIN
• Cybersecurity also presents a potential for liability of board members and company officer
  - Business Judgment rule in Pennsylvania insulates an officer or director of a corporation from liability for a business decision made:
    - In good faith
    - When the director/officer is not interested in the subject of the business judgment
    - When the director/officer is informed with respect to the subject of the business judgment
    - When the director/officer rationally believes that the business judgment in question is in the best interest of the corporation

• As the SEC Commissioner Aguilar noted, a board that fails to deal with cybersecurity “does so at their own peril.”

• Since a board’s judgment must be informed to be protected by Business Judgment Rule, conversely a board that is uninformed likely violates its duty of care, nor can it be said that the officer or director acted in good faith if her he or she made no effort to be informed.

• Business Corporation Law permits a director to rely outside experts and management if he or she “reasonably believes” management to be credible and the experts to be competent. However, it is likely a breach of the duty of care to abdicate responsibility to management and the experts. 15 Pa C.S.A. §1712(a).
So what to do?
Recommended Board actions

- Board should become more conversant and educated on cybersecurity issues and the company’s cybersecurity practices and protocols
  - Some corporations (only 42 of the S&P 500) have created board-level risk committees responsible for privacy and security risks, with clear lines of reporting and authority. The committee should meet regularly and report directly to the board.

- Make cybersecurity a regular board agenda item, including regular presentations by officers (GC, CIO, CTO)
Recommended Board actions (cont’d)

• According to a NY Times survey only 11% of companies’ boards reported a high level of understanding of cybersecurity issues

• Briefings should occur on at least a quarterly basis and the board should make adequate time on the agenda

• Board should focus on, and require that the company has, identified and classified its data
  - Health data, personal information and financial information is particularly sensitive
  - The subject of statutes and regulations requiring heightened security
Board should hire appropriate personnel

- Full-time – many companies have hired a CIO or Chief Privacy Officer (CPO)

- Outside Experts
  - Could be hired if company is not in position to hire a full-time personnel
  - Could be utilized by CIO, CTO, or CPO to assist with legal or technical issues
  - Could be utilized to audit or assess cybersecurity practices and data protection systems and suggest areas for improvement
    - Board should consider assessments and any variances from management assessments and representations
Review of Policies

- Acceptable Use Policy
- Information Security
  - Data Stewardship
- Information Classification
- Records Retention
- Data/Equipment Destruction
- Privacy
  - Web
  - Internal
- Data Breach/Incident Response
- BYOD
- Vendor Policies

POLICIES MUST = PRACTICE
Privacy Programs & Technical Controls

- Data Inventories
- Privacy Impact Assessments
  - Channel your inner 5 year old: Why, Why, Why???
- Vendor Review/Certification
- Incident Response Planning
  - Tabletop Exercises
- Identity Management and Governance
  - Access certification
- Data Loss Prevention (DLP) Tools
Incident Response Plan

• Create and implement an incident response plan
  – What offices/roles should be involved in the initial response
  – Who will manage the investigation
  – A designated spokesperson on behalf of the company to media
  – Who will develop internal and external communications about the incident
  – A checklist of external parties for consultation or contact such as call centers, insurance brokers, outside counsel, and forensics companies

• Integrate the plan into the company’s overall governance, risk management, and business continuity framework
• Include Legal, IT, Privacy, Compliance, Risk, HR/Training, Corporate Communications and others as necessary in the plan creation process
• Review information security policies & procedures
• Review insurance coverage to plan and evaluate cybersecurity risk profile
Data Breach First Responders

• Incident Response Team should include:
  – Risk management
  – Business continuity
  – Communications
  – IT
  – Legal

• Communications Plan should include:
  – Designated Communications Coordinator
  – Internal communications
  – Breach letter (based on existing template)
  – External communications
After a Breach

• Activate Incident Response Plan
  – Designate a spokesperson
  – Conduct forensic investigation
  – Address vulnerabilities ASAP
  – Conduct a risk assessment

• Consider contacting law enforcement

• Contact insurers to notify

• Determine whether notification is necessary
  – Call center
  – Mailings

• Assess lessons learned
When Conducting an Investigation

• When investigating a cyber-security breach, involve the lawyers
  - Target created Data Breach Task Force at the request of in-house and outside counsel
  - Purpose was to educate counsel about aspects of the breach to allow them to provide informed legal advice
  - Different than the concurrent “ordinary course” investigation focused on remediation
When Conducting an Investigation

- Different teams from Verizon involved in each track of the investigation
- Court found that documents regarding the work of the Data Breach Task Force are protected from discovery as privileged and/or work product
- Documents regarding the ordinary course investigation are discoverable
Communicate in Plain Language

• Ensure the communication enables recipients to:
  – Find what they need;
  – Understand what they find; and
  – Use what they find to meet their needs

• Helpful writing techniques include:
  – Logical organization with the reader in mind
  – “You” and other pronouns
  – Active voice
  – Short sentences
  – Common, everyday words
  – Easy-to-read design features
A note about insurance coverage

- Coverage is in its formative stage, so policies can greatly differ
  - Companies would likely find it useful to hire a knowledgeable broker
  - Carriers are often paired with cybersecurity consultants who analyze the company’s security deficiencies for underwriting purposes
  - Insurance considerations
    - Company must figure out what it can afford to pay out-of-pocket for a cyber loss – will determine retention or deductible
• Coverage relates primarily to three areas of loss – liability, breach-response costs, and fines and penalties
• Understand what event triggers coverage – must be suited to company’s data usage and systems
• Exclusions – must ensure that primary risks are included
• Data coverage – policy must be consistent with company usage
• Breach response costs – should cover at least crisis management and breach notifications, credit monitoring, loss of business income, privacy regulatory defense and penalties, forensic investigations, legal fees, hacker damage costs
• Vendor/counsel selection – can company select its own?
Cybersecurity and Insurance

  - Patient records posted to Internet
  - CGL carrier sought declaratory judgment regarding duty to defend class actions
  - Court held that the breach was a “publication” of private information triggering the policy’s personal and advertising injury coverage
Cybersecurity and Insurance

  - Massive hacking scheme accessing private information of tens of millions of Sony PlayStation users, leading to more than 50 class action suits
  - Zurich denied coverage for the approximately $2 billion in losses claimed by Sony
Cybersecurity and Insurance

- Summary judgment in favor of Zurich
- Court agreed that a CGL policy would cover publication of private information but found there was no coverage here since the “publication” was not by Sony, but by third-party hackers
- Case settled while appeal was pending
Cybersecurity and Insurance

  ▪ Vendor transporting tapes with private information regarding 500,000 IBM employees
  ▪ Tapes fall off truck and never recovered
  ▪ No apparent use or publication of the data
Cybersecurity and Insurance

- Vendor voluntarily settles with IBM, paying over $6 million to cover notification and credit monitoring expenses
- Seeks coverage under CGL policy
- Federal denies coverage since no “publication” and no “suit”
- Connecticut Supreme Court sides with Federal on both issues
QUESTIONS?
Reference Materials

Reference Materials and Practical Tools
1. SANS Institute's, "Incident Handler's Handbook"
   http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
2. SANS Institute's, "An Incident Handling Process for Small and Medium Size Businesses"
   http://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791
3. SANS Institute's, "Incident Response: How to Fight Back"
   http://www.sans.org/reading-room/whitepapers/incident/incident-response-fight-35342
4. SANS Institute's, "Critical Security Control 18--Incident Response and Management"
   https://www.sans.org/critical-security-controls/control/18
Reference Materials and Practical Tools (continued)


Reference Materials

Reference Materials and Practical Tools (continued)

8. ISO/IEC 27035, "Security Incident Management"

9. AICPA Incident Response Plan

    http://www.verizonenterprise.com/DBIR/2015/