Preventing, Preparing For, and Protecting Your Company After a Data Breach

develop.idaho 2014
April 23, 2014

Presented By:
Cece Gassner, Esq., Perkins Coie LLP

Perkins Coie
Legal Counsel to Great Companies®

OVERVIEW

- Understanding the threat
  - Nature of the threat
  - Costs associated with breaches
- How to Prepare Before the Breach Occurs
  - Develop plan
  - Assess your data
  - Review contract provisions and insurance
- Hypothetical
  - Implement your response plans
  - Maximize your insurance

The Nature of the Threat

- Advanced Persistent Threat (APT)
  - Attributed to nation-state actor – China
  - Motivated by market and military advantage
  - Target sensitive and proprietary information, IP
- Hackers and organized crime
  - Motivated by financial gain
  - Target credit card numbers, consumer information, and log-in credentials

The Nature of the Threat

- In Chinese intrusion cases handled by Mandiant, 94% of the victim companies didn't realize their networks had been breached until someone else told them.
- On average, companies' networks had been breached for 416 days before the intrusion was detected.

The Nature of the Threat - APT

- "Nation-states willing to spend unlimited amounts of money for technology, intelligence gathering, and bribery can overcome just about any defense."

  -- Alan Paller, Director of Research, SANS Institute

- It's not a question of whether your network will be breached, it's a question of when, how quickly you'll detect it, and how effectively you'll respond.

- Chairman of the House Intelligence Committee: U.S. companies lost nearly $500 billion in proprietary information and intellectual property in 2011.

Nature of the Threat - Hackers

- Average cost of data breach response:

  $5.4 million

- Exploitations cited in law suits:
  - Outdated encryption
  - Hashing, but not salting
  - No network security plan
  - Inadequately trained personnel
  - No IDS, IPS
  - Failure to regularly test security (including through vulnerability scans)
  - Retention/destruction policy, proper destruction

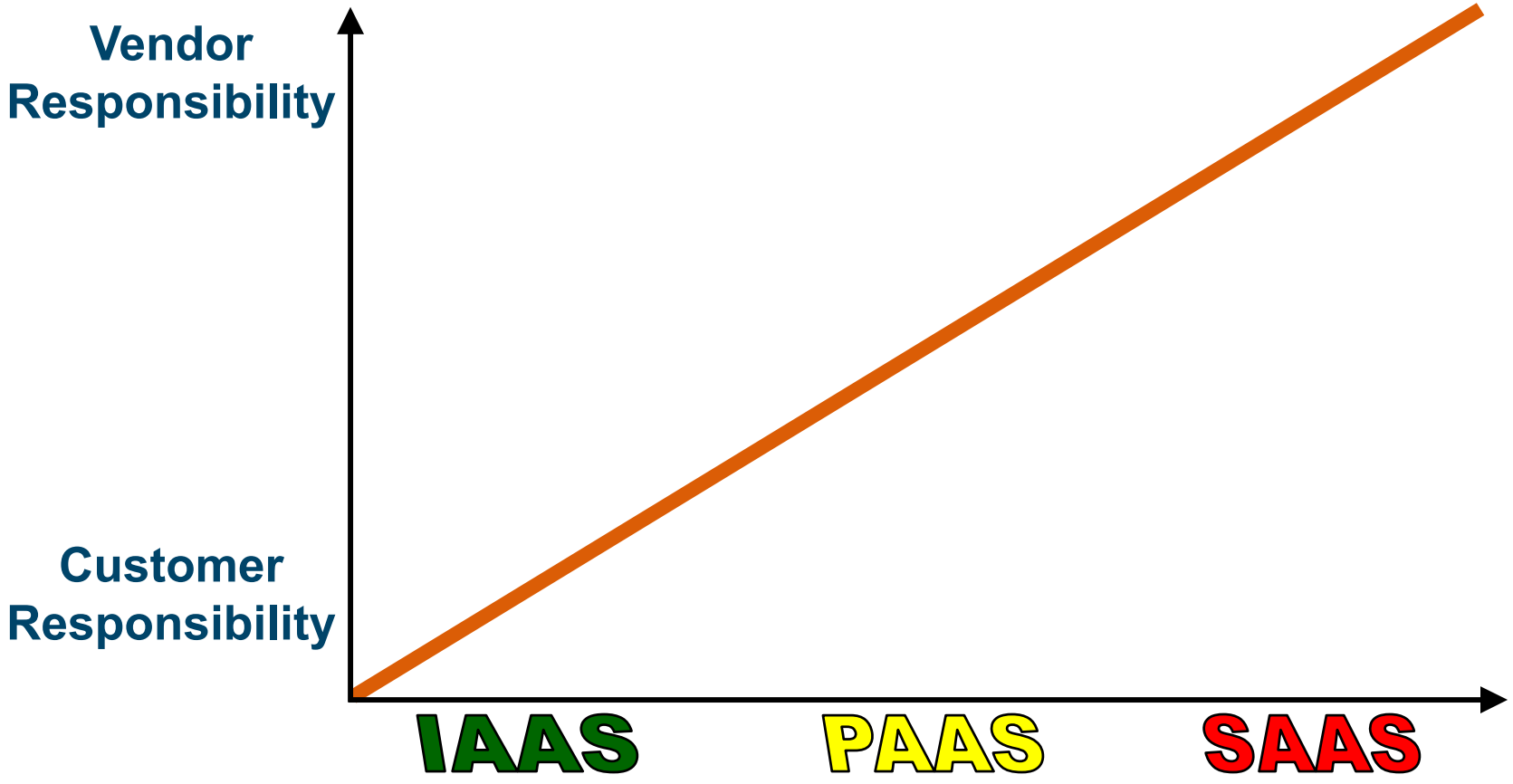
BE PREPARED BEFORE THE BREACH OCCURS

Perkins Coie
Legal Counsel to Great Companies®

PII Data Map: assessing your position and preparing for a data breach

- What do you have? (collection)
  - Classify Data
    - proprietary
    - confidential
    - regulated
- How do you use it? (use/storage)
- Where is it? (storage and sharing)
- Is it/will it be adequately protected? (storage and sharing)

Allocating Responsibility for Data Security Breach: cloud vendor as an example



Perkins Coie
Legal Counsel to Great Companies®

Key Actions

- Assess your data
- Develop and implement reasonable, consistent internal and external policies and procedures
  - Board level
  - External and internal privacy policies
    - Internal policies include data sharing rules and contract terms
  - Internal security policies (including sharing rules)
  - Breach response plans
- Follow and update

Key Actions

- Don’t ignore the red flags!!
  - Target: “Eh, probably nothing.”
  - 90 lawsuits filed against it so far
  - Over $61MM spent on their response to the data breach

Legal Risks & Obligations

- Federal, state consumer protection laws
- Federal law re: protected classes of info
- Breach Notification Laws – 47 states*
- Contract claims
- Common law claims
- SEC disclosure

Review Your Contracts: Key Terms Contemplate Breach

- Standard of care:
  - strict liability: vendor is fully responsible for authorized or unauthorized access, use and disclosure; OR
  - are reasonable technical, physical and administrative measures enough?
- Compliance with applicable laws, regulations and standards
- Notice of breach or suspected breach
- Duty to investigate, cooperate and remediate
- Control over notice and interaction with law enforcement
- Indemnification/ limitation on liability
- Transparency/audit
- Insurance

Sample Limitations on Liability: cloud as an example

Vendor's liability limited to:

- THE TOTAL AMOUNT PAID OR, WITH RESPECT TO ANY SINGLE INCIDENT, THE LESSER OF $500,000 OR THE AMOUNT PAID IN THE 12 MONTHS PRECEDING THE INCIDENT. (SaaS)

- Vendor is not liable to Customer for failing to provide the Services unless such failure results from a breach of the Service Level Agreement, or results from Vendor's gross negligence, willful misconduct, or intentional breach of the Agreement. Except for claims based on Vendor's willful misconduct, the maximum aggregate monetary liability of Vendor shall not exceed six times the monthly recurring fee. (IaaS)

Sample Limitations on Liability: cloud as an example (con't)

Vendor's liability limited to:

- CUSTOMER EXPRESSLY UNDERSTANDS AND AGREES THAT VENDOR, ITS SUBSIDIARIES AND AFFILIATES, AND ITS LICENSORS SHALL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES WHICH MAY BE INCURRED BY YOU, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY. (PaaS)

Review Your Insurance Policies

- Gather, preserve, and complete an historical insurance portfolio
- Review all lines of coverage
  - Cyber Risk/Privacy
  - Errors & Omissions (E&O)/Professional Liability
  - Directors and Officers (D&O)
  - Fidelity
  - Commercial General Liability (CGL)
  - Property
  - Other Policies/Indemnification Agreements

Cyber Risk/Privacy Policies

- Coverage Grants Vary Greatly
- "First-Party" Coverage:
  - Losses due to destroyed or damaged data; data restoration
  - Business Interruption
  - Extortion demands
- "Third-Party" Coverage
  - Privacy Liability
  - Unauthorized disclosure of confidential information
  - Costs to investigate breaches, satisfy notification obligations, defend against regulatory proceedings

Errors and Omissions/Professional Liability Policies

- Claims Made
- Protect the company from claims of liability for an act, error, or omission in rendering of a **service**
- Definition of professional services is critical
- Coverage grants vary widely

  Example: A bank's professional liability policy should cover the bank's investment advisors when a customer sues over investment losses.

Directors and Officers Policies

- D&O policies may provide coverage for:
  - A subpoena issued pursuant to an SEC investigation
  - A DOJ civil investigative demand and subpoena
  - A grand jury subpoena
  - An administrative subpoena from one state consumer protection agency and a civil investigative demand from another
  - Fraud and intentional conduct
  - Special litigation committee costs

Fidelity/Crime Policies

- Insure against losses of money, securities or inventory due to "employee dishonesty"
- Policies contain a number of related coverages
  - Forgery
  - Computer fraud
  - Computer theft
  - Data extraction
  - May offer broad coverage for investigation costs

Commercial General Liability Policies

- Covers third-party claims for “bodily injury,” “property damage,” and “personal and advertising injury”
- Broad duty to defend
- May provide coverage for:
  - Intentional conduct
  - Punitive damages
  - Class actions
  - Patent/Trademark
  - Counterclaims
  - Employment claims

Property Policies

- First-party property policies protect a policyholder's place of operations and inventory, and provide coverage for lost or damaged property.

- "All Risk" covers losses to real property caused by any peril not expressly excluded.
  - Once a policyholder shows that it has suffered a loss, the burden of proof shifts to the insurer to show that the loss is not covered.

- "Named Peril" covers only those perils expressly named.

Property Policies (Cont'd)

- First-party property policies may also provide coverage for:
  - Economic losses resulting from the interruption of your business due to physical loss of or damage to your property ("business interruption")
  - Economic losses resulting from the interruption of your business due to physical loss of or damage to the property of your buyers or suppliers ("contingent business interruption")
  - The increased, above-normal cost of business operations resulting from an insured peril ("extra expense")

Other Policies and Agreements

- **Is your company an additional insured under any other insurance policies?**
  - Certificates of insurance
  - Who controls the rights under the policy?
- **Review all indemnification agreements**
  - Does the indemnity respond first or the insurance?
  - Who controls the defense?

Hypothetical

Computer network of large, public retailing company with significant business to business logistics and direct to consumer lines of business is compromised by hackers for months before the hack is detected.

- Network is partially managed by a third-party vendor.
- Extent of intrusion is unclear
- Appears confidential customer, vendor and employee information has been compromised.

Response & Remediation

- Initiate your Incident Response Plan
- Implement communications plan
- Hire network security vendors to assist IT staff
- Notify law enforcement?

Commercial & Reputational Risks

- Depreciation of corporate assets
- Accelerate patent applications
- Monitor published patent applications, the market for signs of misappropriation
- Communications strategy tailored to government agencies, vendors, customers, the public

Provide Prompt Notice/Notice of Circumstances

- Avoid the time trap
  - All potentially relevant insurance companies should be noticed
  - Need procedures in place to ensure notice is given early
- Notice of circumstances
  - Differs from giving "notice" of claim
  - Provides coverage for subsequent claims after policy period ends
- Provide notice even if you have incomplete information

Present the Claim to Maximize Coverage

- Pick your words carefully
- Tricky Areas:
  - batch clauses
  - interrelated acts
  - investigation costs
  - proof of loss
  - claim vs. potential claim
  - occurrence vs. occurrences

- Example: You should frame multiple network breaches as one occurrence if policy has a high per occurrence deductible.

QUESTIONS?

Presenter Information

Cece Gassner is a counsel in the firm's Business practice with a focus on technology transactions and information privacy and security. She has experience in a variety of transactions, including intellectual property, technology transfers, content, and technology and software licensing agreements. She has advised technology- and life science-based clients regarding their domestic and international intellectual property-based transactions, devised intellectual property protection strategies, advised on clinical trial protocols and data collection, and created intellectual property management programs.

She can be reached directly at 208-387-7507 or cgassner@perkinscoie.com.