King & Spalding — Data, Privacy & Security

King & Spalding’s 60 plus lawyer Data, Privacy & Security ("DPS") Practice is best known for:

• Experienced crisis and security incident response managers
• Former government lawyers who balance cooperating with law enforcement and defending regulator investigations
• Bona fide trial attorneys with track records of successfully defending data breach and privacy class actions and litigation
• Seasoned counselors who apply the “real world” to data privacy and security governance
• Law360 Privacy Practice Group of the Year, Law360 Privacy MVP and two Cybersecurity Docket Top Incident Response 30 awards
Agenda

- Overview
- Incident Awareness
- Incident Investigation Part I
- Incident Investigation Part II
- Questions / Discussion
Purpose of the Exercise

• Simulate incident to expose participants to process and workflows
• Primarily focused on process components
• Less focused on technical components
• Provoke thought and discussion about security incident preparedness and response
“Real World” Incident Response

- Defensible Policies
- Corporate Policies & Practices
- Litigation & Investigation
- Security Incident
- Collaborative Support
- Preparation
- Incident Response
- Defensible Incident Management

King & Spalding
5
Case Background

- Organization profile:
  - $5 B multinational manufacturer
  - Operations across United States
  - Business to Business
  - 30,000 employees
Security Incident

- Human Resources Department:
  - HR employee reports to supervisor that a week ago she sent an email in response to a request from the CFO, which attached a spreadsheet including W-2 information for employees.
  - After reviewing the email again today, she noticed an IP address which did not look familiar.
  - The supervisor reported the incident to the HR Director.
Incident Awareness

- Companies become aware of an incident in any number of ways, including communications from:
  - Third party vendors
  - Independent security researchers
  - FBI or other law enforcement agencies
  - Customers
  - Employees

**Day 1**

- Make an initial assessment of the scope and nature of the incident
- Collect and preserve data related to the incident
- Decide to invoke your IRP
- Inform appropriate stakeholders
- Develop plan of action
Investigation Part I

- Internal and forensic investigations begin
- Frequent interaction with Stakeholders
- Identify scope of incident and begin short term remediation
- Develop narrative to minimize risk

Day 2

- Legal directs privileged internal and forensic investigations
- Decision is made for internal IT to handle review
- IT identifies and retrieves copy of phishing email and foreign IP address
- IT searches for other similar emails
Investigation Part II

- End of internal and forensic investigation, beginning of long-term remediation
- Keep in mind potential legal actions (e.g., litigation, regulatory inquiries)

Day 4

- Legal, IT and Forensic experts find answers to questions regarding scope and legal exposure
- Scope of incident includes two phishing emails, but only one involved a reply response
- The reply email included a spreadsheet with W-2 information of 20,000 employees
- Initial focus is on warning employees and reducing risk
Notification

- Notifications
  - Regulators
  - Law Enforcement
  - Media
  - Insurance Carriers
  - Vendors
  - Customers
  - Employees

Days 5 - 8

- Notification Obligations
  - IRS
  - State Attorneys General
  - Individuals

- 47 states, D.C., & U.S. territories
- Consistent approach to notifications and case narrative to minimize legal and business harm
Support For the Long Run

Workflows in Action

- Review and provide notice for cyber liability coverage
- Regulatory inquiries
- Press coverage
- Class action complaint
The Long Battle & Lessons Learned

• Legal proceedings and investigations continue
• IT remains vigilant in securing and monitoring all systems and upgrading safeguards
• Review the response, learn from the experience, and prepare for the next one
Questions?