SECUREWORLD

See Globally. Defend Locally.

Robert J. Scott

Privacy & Security Issues in Cloud Contracts

Play Cyberhunt: The game within the SecureWorld App! Have fun, network and win great prizes.

Don't forget to take the survey on the SecureWorld App. It will also be mailed to you at the conclusion of the conference.

After this presentation; view the slides on the SecureWorld App.

Speaker

Robert J. Scott

Cloud Computing Trends

- Forrester Research estimates the cloud market will reach $191 billion by 2020.[1]
- Estimated $940 billion in IT services spending in 2016. [2]
- 94 percent of companies expect more than a quarter of their workloads to be in the cloud within two years. [3]

[1]The Public Cloud Market Is Now In Hypergrowth: Sizing The Public Cloud Market, 2014 To 2020 (Forrester Research, April 24, 2014)

[2] Gartner Worldwide IT Spending Forecast

[3] State of the Market: Enterprise Cloud 2016 (Verizon)

Regulatory Compliance Risks

Industry-specific Regulation

- Gramm-Leach-Bliley Act – Financial
- HIPAA & HITECH – Healthcare
- PCI Compliance – Payment Systems

Broad Regulation

- State Data Privacy

GLBA Compliance Considerations

Service Provider:

Any party that is permitted access to a financial institution's customer information through the provision of services directly to the institution.

Vendor Selection:

Exercise appropriate due diligence in selecting service providers.

GLBA Compliance Considerations

Required Provisions:

- Require service providers by contract to implement appropriate measures designed to meet the objectives of the Security Guidelines.
- Where indicated by risk assessment, monitor service providers to confirm that they have satisfied their obligations under the contract.

GLBA Compliance Considerations

Required Provisions:

- Ensure service providers:
  - implement appropriate measures designed to protect against unauthorized access to or use of customer information maintained by the service provider that could result in substantial harm or inconvenience to any customer.
  - properly dispose of customer information.
  - take appropriate actions to address incidents of unauthorized access to the financial institutions' customer information, including notification to the institution as soon as possible following any such incident.

HIPAA Compliance

- Due Diligence
- Who requires a BAA
- What are adequate administrative and procedural safeguards
- What if a vendor will not agree to a BAA

HIPAA Security Rule

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit.
- Identify and protect against reasonably anticipated threats to the security or integrity of the information.
- Protect against reasonably anticipated, impermissible uses or disclosures.
- Ensure compliance by their workforce.

Security Measure Considerations

- Size, complexity, and capabilities
- Technical, hardware and software infrastructure
- Costs of security measures
- Likelihood and possible impact of potential risks to e-PHI
- Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment

Risk Assessment

Risk analysis process includes, but is not limited to, the following activities:

- Evaluate the likelihood and impact of potential risks to e-PHI
- Implement appropriate security measures to address risks identified in risk analysis
- Document chosen security measures and, where required, the rationale for adopting those measures
- Maintain continuous, reasonable, and appropriate security protections

Risk analysis should be an ongoing process of periodic and regular reviews.

Key Provisions in Cloud Contracts

- Insurance and indemnity requirements—especially for intellectual property infringement
- Regulatory compliance
- Subcontractor liability for third party services or software
- Effect of termination—return of customer data
- Service failure corrective action plan
- Security Commitments BAA
- Compliance with Laws

Indemnification Provisions

- What indemnification is the vendor offering?
- How do proposed terms compare to vendor contracting policies and procedures?
- Customers often use insurance to cover risks that would normally be addressed in indemnification provisions.

Limitation of Liability

- Calculating maximum liability
  - Usually tied to payments made under the agreement
  - Carve-outs – certain claims are not subject to the cap
- Liability risks related to security incidents

Risk Mitigation Strategies

- Require vendors to legally assume all liabilities associated with the service.
- Specify insurance coverage requirements including forensics, breach response, regulatory response and consumer claims.
- Use indemnity provisions to protect against liability.
- Edit limitation of liability provisions that would limit access to coverage.

Questions?

Contact Information

Robert J. Scott, Esq.
Managing Partner
rjscott@scottandscottllp.com
(214) 999-2902

Scott & Scott, LLP.
1256 Main Street, Suite 200
Southlake, TX 76092
www.scottandscottllp.com