RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: CSV-R03

The Legal Pitfalls of Failing to Develop Secure Cloud Services

Cristin Goodwin
Senior Attorney, Trustworthy Computing & Regulatory Affairs
Microsoft Corporation

Edward McNicholas
Global Leader, Privacy & Data Security Practice
Sidley Austin LLP
@SidleyNewsroom
www.Sidley.com\InfoLaw

Overview and How to Apply Today's Discussion

- **Framing**: Which laws are most relevant when considering developing for the cloud and balancing cloud security risks?
- **Overview**: Relevant legal paradigms
- **Scenarios**: Cloud security issues and concerns
- **Discussion**: You should come away with a baseline of key legal questions around developing and operating secure cloud services

Who Wants to Hold You Accountable?

Federal Trade Commission
Protecting America's Consumers

cfpb
Consumer Financial Protection Bureau

Department of Health & Human Services USA
Office for Civil Rights

United States Senate

U.S. House of Representatives

State of Connecticut
Truth · Equity · Justice
Judicial Branch

The Attorney General
Texas

U.S. Securities and Exchange Commission
MCMXXXIV

Office of the Attorney General
California Department of Justice
Liberty and justice under law

State of New York
Attorney General
Excelsior

Thinking about developing for a cloud service?

Statutory Obligations (Federal and State)	Civil Obligations Tort Law Reasonableness (Negligence)	Regulatory Obligations Direct or customer's	Contractual Obligations Corporate Governance	Standards	Best Practices

Mental checklist your lawyer's thinking about

The Kind of Technology Lawyers Worry About

Conflicting Legal Paradigms

Strict Liability

Often based in statute, such as data breach notification laws

No fault insurance approach

Socially-useful but potentially dangerous could trigger liability (i.e., collections of data)

Internalization of costs

Negligence

Based in civil law, as a standard of care

Industry standards \ best practices

Companies have an incentive to act reasonably to improve compliance and mitigate liability

Evolving questions around standard of care for coders, operators, and users – in particular for critical infrastructures

Contracts

Based on the four corners of the contract

Civil law very deferential to the terms

May limit remedies, damages, and set out very specific obligations that matter greatly in crises

App Store terms can count!

Adding Legal Complexity: The Laws of Other Countries and the Cloud

Global Issues

Increasing legislative and standards and compliance requirements worldwide

- Brazil, China, Germany, EU, Russia

European Union proceedings in play

- Data Protection Directive covers all processing of “personal data”; high penalties (2-5% of **global revenue**)
- Network and Information Security Directive

Cloud Specific Issues

Differing legal regimes complicate “cloud governance”, in particular around data

Cross-border data transfers, remote processing, and storage increase the risk of disclosure to governments, litigants, other third parties

Perception of magnified risks of data loss due to hacking, security breaches, or inadvertent disclosure, destruction of data

Location still matters legally.

Security Scenarios

Compromise of a *3rd party cloud app* that impacts your corporate network, potential impact to customer data

Compromise of the *cloud service provider's service*, potential impact to customer data

Development of Apps for the Cloud

Your business is using a 3rd party cloud app supporting your main product, and it holds customer data. It appears to have leaked customer data.

- What does the contract say? Any remedies or protections or requirements?
  - Investigation, response (including comms), notice to customers, duty to collaborate
  - Are you indemnified for this incident by the 3rd party?
- Do you have the ability to investigate directly versus dependency on app provider to investigate?
  - Asserting Attorney Client Privilege in the investigation
  - Do you need to pull in outside assistance (technical, legal) to aid in the investigation?
  - If there are other app customers impacted, is there information that can be shared that would aid your response?

Your business is using a 3rd party cloud app supporting your main product, and it holds customer data. It appears to have leaked customer data. (continued)

- Is the 3rd party app provider managing PR adequately? Are the 3rd party's statements adding to your legal risks?
- Is this event material? Does it trigger SEC reporting? Have you notified your Board?
- Do you need or want to contact law enforcement?

Compromise of the cloud service provider, potential impact to customer data.

- What does the contract say? Any remedies or protections or requirements?
  - Investigation, response (including comms), notice to customers, duty to collaborate
  - What audit rights do you have?
  - Are you comfortable with the adequacy of the CSP's compliance capabilities?

Compromise of the cloud service provider, potential impact to customer data.

(continued)

- Do you have the ability to investigate directly versus dependency on service provider to investigate?
  - Asserting Attorney Client Privilege in the investigation
  - Do you need to pull in outside assistance (technical, legal) to aid in the investigation?
  - Is the cloud service provider managing PR adequately?
  - Is this event material? Does it trigger SEC reporting? Have you notified your Board?
  - Do you need or want to contact law enforcement?

- CSP is preparing for class action, government inquiries, major media issues – what do you need as the customer to manage your legal risks?

Developing Apps for the Cloud.

- Standards and Best Practices matter a lot:
  - Are there standards or best practices must follow for development on a particular platform or for a particular service?
  - Are you using relevant laws or standards to help manage your customers' risks, to make your app more attractive for them?
  - Are there other relevant global standards or certifications that help mitigate downstream risks? (i.e., ISO 27034)

Developing Apps for the Cloud. (continued)

- What do the terms of the App store or sales platform for your app? Do they talk to security or your obligations in development or in an incident?
- Things to consider when you are developing:
  - Do you have an incident response plan? Does it include legal and PR?
  - What forensic capabilities do you have?
  - How secure is *your* infrastructure?
  - What promises can or should you make in your EULA?

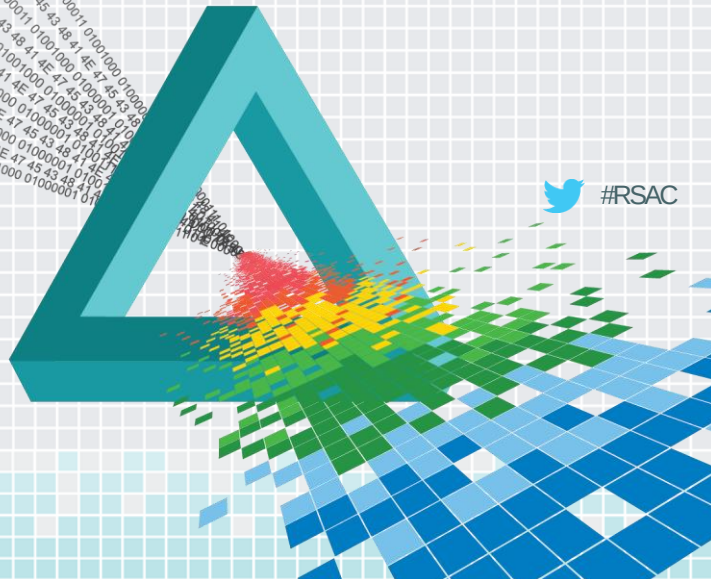
Applying What You've Learned

- Next week you should:
  - Know your lawyer and begin a conversation about the legal aspects of managing cyber risks
- In the first three months following this presentation you should:
  - Develop a regime to mitigate the risks around developing or using cloud services
- Within six months you should:
  - Be actively mitigating risks that arise when developing a cloud service

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Backup Slides and Additional Information



Federal and State Legal Concerns

Federal Issues

- No comprehensive federal privacy or cybersecurity laws
- Sector-specific requirements growing (Healthcare, Financial Services)

State Issues

- State information security laws requiring “reasonable” security and specific action
- Massachusetts Information Security Regulations
- State data breach requirements can vary by jurisdiction

Potential Legal Consequences of Incidents

- US implications
  - FTC investigation
  - Multistate AG investigation
  - SEC investigation
  - Congressional hearings and inquiries
- Other global implications
  - PCI Investigation for credit card loss
  - Discussions with the insurance carrier about coverage
- Litigation extravaganza
  - Breach of contract
  - Consumer class action litigation
  - Shareholder derivative action alleging failure of Board oversight

Moving Beyond Forms

Growing In Relevance: The NIST Framework

#RSAC

www.nist.gov/cyberframework (February 12, 2014)

Step 1: Prioritize and Scope.

Step 2: Orient.

Step 3: Create a Current Profile.

Step 4: Conduct a Risk Assessment.

Step 5: Create a Target Profile.

Step 6: Determine, Analyze, and Prioritize Gaps.

Step 7: Implement Action Plan.

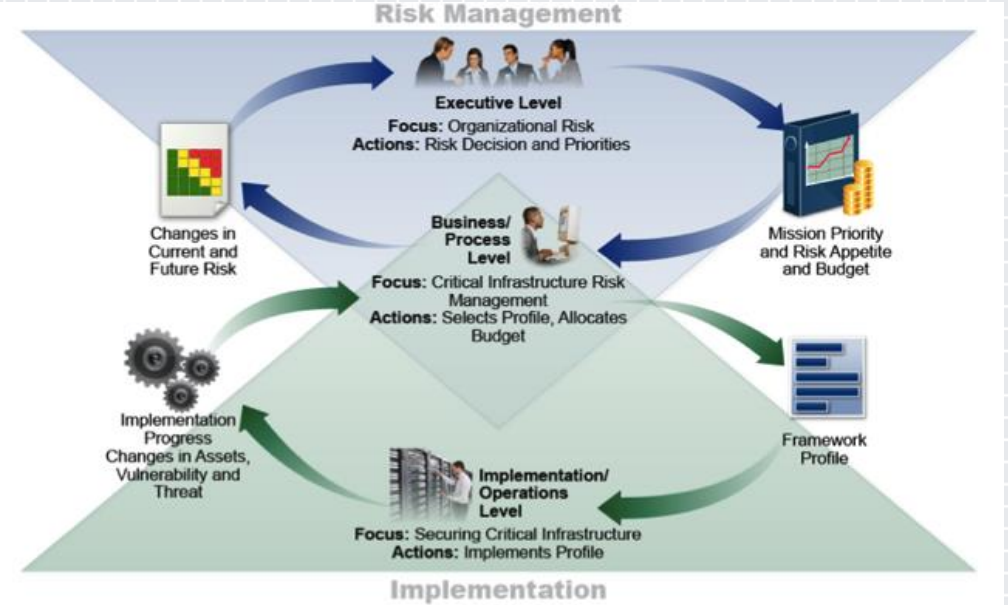


Figure 2: Notional Information and Decision Flows within an Organization

Good Questions to Ask:

- Are we “critical infrastructure” operators? Are my clients or prospective clients “critical infrastructure” operators?
- Will my clients be subject to privacy and security regulation and expect\need their cloud service to comply?
- Do we know what sort of data is being processed and the legal requirements that apply to it?
- What cloud compliance or certifications are available, and would help customers manage their own risks?
- What have we learned through past incidents have we experienced? Are we learning internally?
- Do we have an up-to-date method for ensuring security in development and operations?
- What commitments have we made in the applicable contract or privacy policy?
- Who is monitoring best industry practices?