Using Contracts to Cover Your SaaS

January 24, 2019

Meet Your Presenters

Helena Ledic - Associate General Counsel, CSC

Jeff Leventhal – Technology Attorney

Eric Wheeler - Director of IT Operations and Security, Alterra Mountain Company

Disclaimer: The views expressed by the presenters are not necessarily the views shared or endorsed by their corporations or CSC®. This presentation is for informational purposes only and does not constitute legal advice.

Our Agenda:

1. Clearing Up the Clouds
2. The roles Legal, Business, Security, and Procurement have in vendor selection
3. Risk/Reward with SaaS providers
4. Risk analysis of SaaS vendors
5. Understanding the terms in a SaaS contract
6. Ongoing monitoring after the SaaS vendor is onboarded
7. Recap

1

Clearing Up the Clouds

Types of Cloud

- **Infrastructure as a service** - delivers computer infrastructure such as hardware, storage, and servers (e.g., AWS).
- **Platform as a service** - provides a platform allowing customers to develop, run, and manage web applications (e.g., Force).
- **Software as a service** – hosts applications and made available to customers over a network (e.g., Office 365).

CSC

2

The roles Legal, Business, Security, and Procurement have in vendor selection

Responsibilities

Legal

- Understands and articulates contractual and regulatory risk
- Reviews and negotiates legal contract terms

Business

- Reviews and negotiates commercial terms
- Manages vendor performance
- Renews or terminates the contractual relationship

Information Security

- Reviews and negotiates security terms
- Conducts due diligence with vendor security program

Procurement

- Helps manage vendor selection process
- Facilitates the contracting process

CSC

3

Risk/Reward with SaaS providers

Rewards

- **Scalability -** Provide services using large-scale computing resources with the flexibility to add or remove IT capacity to meet peak and fluctuating service demands.
- **Automatic software updates -** Patch management is not typically needed.
- **Security -** Companies such as Microsoft and Amazon have the technology, expertise, and resources to develop premier security.
- **App Modernization -** Adopt modern development and application management technology to more easily improve IT efficiency.

CSC

Considerations

- **Physical security –** Fear that significant SaaS providers could be future targets.
- **Data residency -** Depending on the provider, you may have little control over where data is stored.
- **Disaster recovery -** SaaS provider's disaster recovery capabilities vitally important.
- **Subcontractors –** Will subcontractors have access to your data? How are they vetted?
- **Exit Strategy** – How easy will it be for you to get out of a contract, leave a platform and take your data?

CSC

4

Risk analysis of SaaS vendors

Vendor Solicitation/Selection

First you need to discuss…what is the business need?

What type of data will they store?

- PHI/PCI/PII
- Regulated data
- Trade secrets
- Employee data
- Customer data

What type of technology is necessary, now and in the near future?

- Technology roadmap

CSC

Vendor Solicitation/Selection

Initial Risk Assessment

- Security, availability, and confidentiality
- Vendor expertise
- Insurance coverage

Documentation

- SOC reports, ISO accreditations, etc.
- References and reputation
- Pen tests, vulnerability scans
- Security questionnaire
- Policies/Procedures
- Subcontractors/Vendor Management

Opportunity to Grow / Evolve

- Support of Enterprise functionality
- Advanced application management
- Broad choice of PaaS technologies, including DBaaS, IdaaS, etc.

CSC

5

Understanding the terms in a SaaS contract

Due diligence in understanding the terms in your SaaS contract

Information Security Program

- Policies should be modeled after the ISO 27001 or similar framework

Privacy

- Data processing terms for PII
- State Laws (i.e. Massachusetts, California), GDPR, HIPAA, etc.

Data ownership

- Does the agreement have language which allows the vendor to sell or use/share data for purposes other than providing the service?

Data residency

- Does the agreement give you a choice where your data will be stored, where it may be accessed from, and does it restrict the vendor from storing or accessing in locations that are not deemed "adequate" under GDPR?

CSC

Service Level Agreements

How are service level objectives defined?

- Critical response times may vary across providers.
- Measurements may vary across vendors:
  - Example:

$$\left[\left(\frac{total - nonexcluded - excluded}{total - excluded}\right) * 100\right] \geq 99\%$$

What is the credit process like for service level interruptions? Typically:

- Customers required to take specific actions in order to claim the credit
- Customers have a set time frame within which to provide proof after service has been restored
- SaaS provider makes the final unilateral judgment on service credits

CSC

Best Practices:
Business Continuity/Disaster Recovery

- Review and confirm responsibility for business continuity and disaster recovery procedures
- Review any published RTO/RPOs

- Consider whether the provider needs to have redundancies (offices/datacenters)

CSC

Best Practices: Right to Audit

- Determine the level of audit
  - Regulatory requirements must be considered
  - Recognize competing interests of other customers on shared infrastructure
- Get insight into a provider's security posture at a frequency you are comfortable with
- If credit card data is in scope, ensure the provider is PCI certified

CSC

Best Practices: Encryption

- Encrypt data at rest
- Use approved public algorithms such as AES or SHA-256
- Evolve your encryption with time
- Know who maintains the encryption keys?
    - Customer, vendor, or both?
- Encrypt data in transit
    - Prohibit unencrypted data on portable devices.

CSC

Best Practices: Penetration Tests and Vulnerability Scans

- Pen tests should be performed annually by a reputable third party and documented in audit reports.
- Ongoing communication between the customer and the provider is critical.
- Suggested remediation timelines are dependent on the service, value of data, compensating controls, etc., and can vary widely.

Breach of Contract Resulting in Security Breach - Notification and Remediation Recommendations

- Confirmed breach notification within regulatory requirements
  – (GDPR's 72 hours is for controllers)

- Dedicated email address or hotline/phone number

- The provider must fix the vulnerability which resulted in the breach

CSC

Limitation of Liability: Things to Look For

- Is the vendor offering any secondary caps?
- Does the vendor offer differing aggregate liability?
- Does the vendor exclude gross negligence from liability caps?
- Does the vendor offer differing indemnification and disclaimer clauses?
- Key is understanding the allocation of risk-responsibility
    - Vendor should own what it can mitigate, the rest is allocated

CSC

Limitation of Liability: Standard Clauses

- Typically favor the SaaS provider
- Limit compensation provided in case of a security breach
- Provider not held liable for losses caused by the inability to use the service
- Liability caps vary but are rarely more than the previous 12 months of billing

Limitation of Liability: Standard Clauses *Cont.*

- Carefully review the provider's aggregate liability; this differs across providers
- Make sure you have language that excludes caps in cases of gross negligence
- Compare indemnification and disclaimer clauses between different SaaS providers to see which is most favorable to customer

CSC

CSC

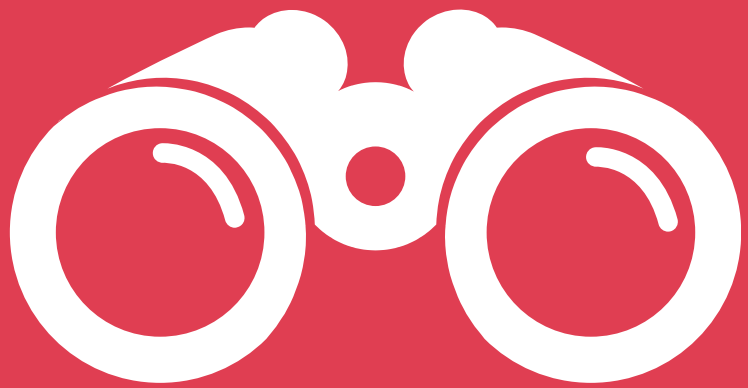
6

Ongoing monitoring after a SaaS vendor is onboarded

Continue to Monitor

Documentation such as:

- SOC reports
- DR test results
- Information security policies
- Security questionnaires
- Service level objective performance
- Insurance
- Hotline numbers



CSC

Reasons to Terminate

- Vendor ceases SaaS business operations
- Bankruptcy/receivership
- Failure to meet SLAs
- Failure to cure a breach
- Customer's failure to pay

- What happens to the data if you leave the provider?
  - Were you able to recover all your data?
  - If the provider kept your data, is their a destruction/deletion policy in place?

7

Quick recap

Recap

A working partnership with legal, business, information security and procurement is key in vendor selection

Risk assessments prior to the contract stage are vital

SaaS vendors are not the same and negotiation strategies may vary

Continue to perform due diligence

CSC

Questions?

Contact Info

Helena Ledic

helena.ledic@cscglobal.com

Jeff Leventhal

jeflev5280@comcast.net

Eric Wheeler

ewheeler@alterramtnco.com

CSC