Security in knowledge

CYBERSECURITY SLAs: MANANGING REQUIREMENTS AT ARM'S LENGTH

Matthew J. Butkovic, CISSP

Carnegie Mellon University, The Software Engineering Institute, CERT

Samuel A. Merrell, CISSP

Carnegie Mellon University, The Software Engineering Institute, CERT

RSA CONFERENCE 2013

Session ID: GRC-F42

Session Classification: INTERMEDIATE

Takeaways

- Organizations are increasing reliant on third-party information technology services. Examples include:
  - Cloud Computing
  - Data backup
  - Operating partners
- Unless cyber security requirements are identified and communicated, organizations have little reason to believe their needs will be met
- You can't outsource risk to your organization
- Cyber security SLAs can help reduce risk to your organization

Audience Poll

1. Does your organization document specific security objectives in agreements with third parties?
2. Does your organization include measures of cybersecurity performance in third party agreements?
3. Does your organization monitor compliance with security objectives in agreements with third parties?
4. Is cybersecurity performance considered when selecting third parties?

Agenda

- Consequences of Losing Control
- State of the Practice
- A Better Cyber Service Level Management Process

When Control is Lost

- *“One caveat of outsourcing is that you can outsource business functions, but you cannot outsource the risk and responsibility to a third party. These must be borne by the organization that asks the population to trust they will do the right thing with their data.”*

-Verizon 2012 Data Breach Investigations Report

When Control is Lost

- Why you should care about granting control of your data to service providers
  - Selected breach incidents
    - New York State Electric and Gas (2012)
    - California Department of Child Support Services (2012)
    - Thrift Savings Plan (2012)
    - Epsilon (2011)
    - Silverpop (2010)

Data Breach Liability

- An increasingly contentious issue in outsourcing
- Providers are looking to significantly limit liability
- Damage to brand and reputation can far exceed the compensation
- Clients are pushing for more specificity in security processes operated by the service provider

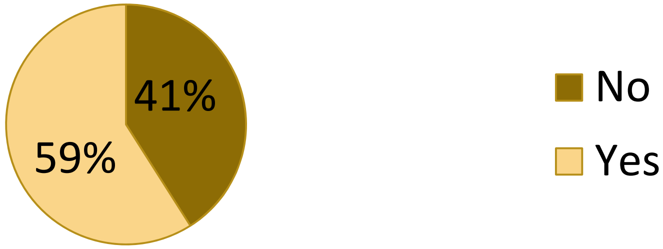
Overview of the State of the Practice:
What do organizations do today?

Risks in Dependencies

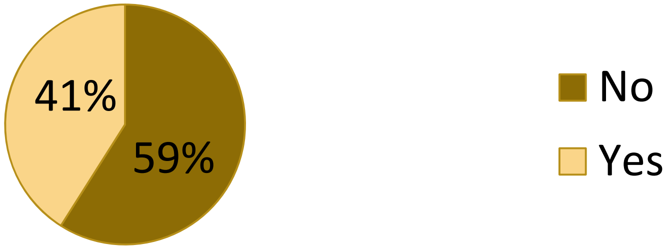
- Reliance on third parties means a potential loss of control
  - Reduced visibility into how your data is
    - Stored
    - Accessed
    - Transmitted
- The ownership of information security risk remains with you
  - This risk can be managed
    - Service Level Agreements
    - Robust management processes

State of Cyber SLAs – Field Research

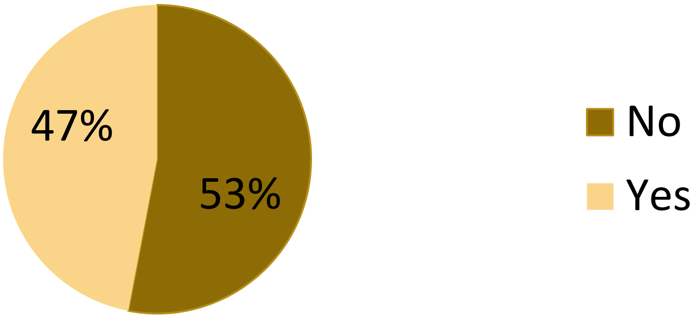
Does your organization document security objectives in agreements with third parties?



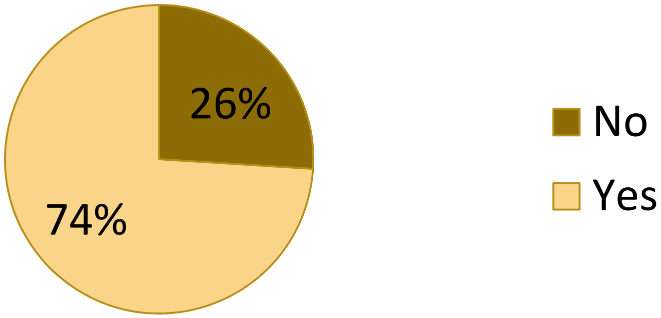
Does your organization include measures of security performance in agreements?



Does your organization monitor compliance to security objectives in agreements?



Is cybersecurity performance considered when selecting third parties?



Standard SLAs…

- … frequently indemnify the provider to the greatest extent possible, limiting the provider's exposure.
- …often lack specific cyber security measures, apart from availability metrics
- …usually place the burden of detecting and reporting failures on the customer
- "SLAs are not about increasing availability; their purpose is to provide the basis for post-incident legal combat.[1]"
  - Compensation paid for service failure is connected to the cost of the service, not to total losses
  - Ex: a large retailer loses $50m in business, but compensated $300 for the outage they experienced on Black Friday[2]

[1] [2] Bernard Golden, CIO.com, 09 November, 2011

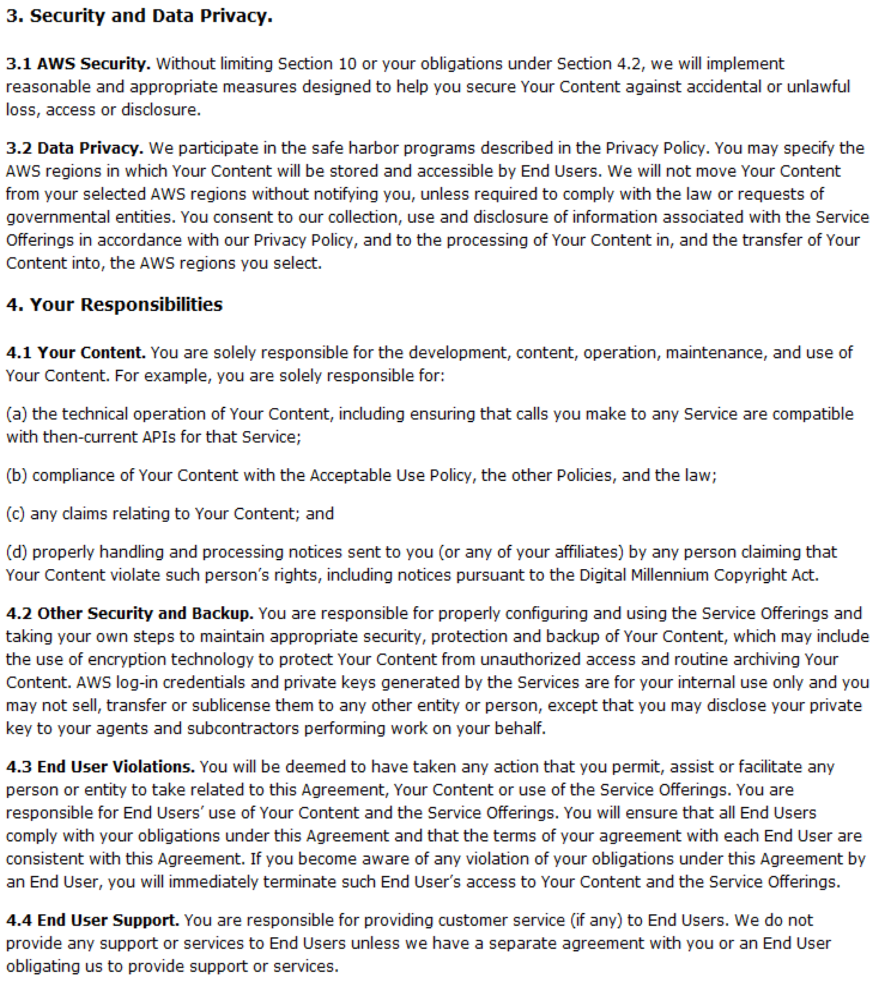
SLA Restitution

	Amazon EC2	Azure Compute	Google Apps	Rackspace	Terremark/ Verizon
Credit	10% if <99.95	10% if <99.95 25% if <99	3 days if<99.9 7 days if <99 15 days if <95	5-100%	$1/15 min up to 50% of bill
Bill affected	Future	Current	Current	Current	Future
Credit filing window	30 days	1 month	30 days	30 days	30 days
Other comments		Must report within 5 days	$ instead of service permitted		

Lisa Spainhower,"Cloud Provider High Availability", January 18, 2013 IFIP WG10.4 Conference on Dependable Computing and Fault Tolerance, Tavira, Portugal

Examples of Cloud SLAs

- "Reasonable and appropriate measures"
  - no specifics (difficult to hold the provider accountable)
- "You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security…"
- "Limitations of Liability"
  - not responsible for damages



3. Security and Data Privacy.

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

3.2 Data Privacy. We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities. You consent to our collection, use and disclosure of information associated with the Service Offerings in accordance with our Privacy Policy, and to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select.

4. Your Responsibilities

4.1 Your Content. You are solely responsible for the development, content, operation, maintenance, and use of Your Content. For example, you are solely responsible for:

(a) the technical operation of Your Content, including ensuring that calls you make to any Service are compatible with then-current APIs for that Service;

(b) compliance of Your Content with the Acceptable Use Policy, the other Policies, and the law;

(c) any claims relating to Your Content; and

(d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Content violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act.

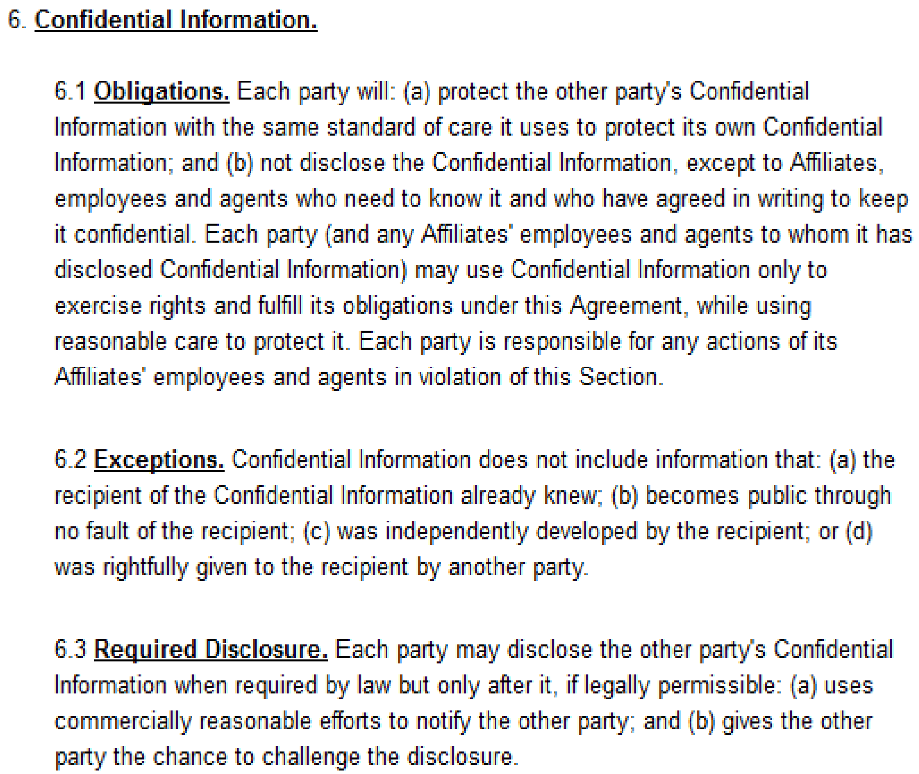
4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. AWS log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

4.3 End User Violations. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Agreement, Your Content or use of the Service Offerings. You are responsible for End Users' use of Your Content and the Service Offerings. You will ensure that all End Users comply with your obligations under this Agreement and that the terms of your agreement with each End User are consistent with this Agreement. If you become aware of any violation of your obligations under this Agreement by an End User, you will immediately terminate such End User's access to Your Content and the Service Offerings.

4.4 End User Support. You are responsible for providing customer service (if any) to End Users. We do not provide any support or services to End Users unless we have a separate agreement with you or an End User obligating us to provide support or services.

Examples of Cloud SLAs

- Vague language:
  - “Each party will protect the other party’s confidential information with the same standard of care it uses for its own information.”



6. Confidential Information.

6.1 **Obligations.** Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates' employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates' employees and agents in violation of this Section.

6.2 **Exceptions.** Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.

6.3 **Required Disclosure.** Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

Government Cloud Initiatives

- FedRAMP
  - Establishes a common set of security controls for cloud providers
  - Certifies that providers implement the required controls
  - Directs agencies to monitor compliance of providers
  - Does not provide agencies a method to alter requirements to manage different risks

Best Practices in Cyber SLAs

- SLA management practices auditors expect to find
  - “Specific and enforceable stipulations in the outsourcing agreement that activities performed by the service provider are subject to controls and audits as if they were performed by the service user itself”
  - “Inclusion of provisions requiring the service provider to monitor compliance with the SLA and proactively report any incidents or failures of controls”
  - “Adherence to the service user’s security policies”

Source: ISACA IS Auditing Guide G4: Outsourcing of IS Activities to Other Organizations

Best Practices in Cyber SLAs

- Guidance from CobiT (applicable control objectives)
  - DS1 Define and Manage Service Levels
    - DS1.1 Service Level Management Framework
    - DS1.2 Definition of Services
    - DS1.3 Service Level Agreements
    - DS1.4 Operating Level Agreements
    - DS1.5 Monitoring and Reporting of Service Level Achievements
    - DS1.6 Review of Service Level Agreements and Contracts

Source: CobiT User Guide for Service Managers

Best Practices in Cyber SLAs

- Guidance from NIST
  - Advocates that a lifecycle approach be applied to the development and management of third-party services
  - Provides lists of key questions and factor categories for services
  - Describes the "organizational factor" in service management

" *…In many cases, long accepted internal controls and business practices that have developed over time due to natural business unit divisions or regulatory requirements may have to be reconsidered when an IT security service provider is engaged."*

Source: NIST Special Publication 800-35-Guide to Information Technology Security Services

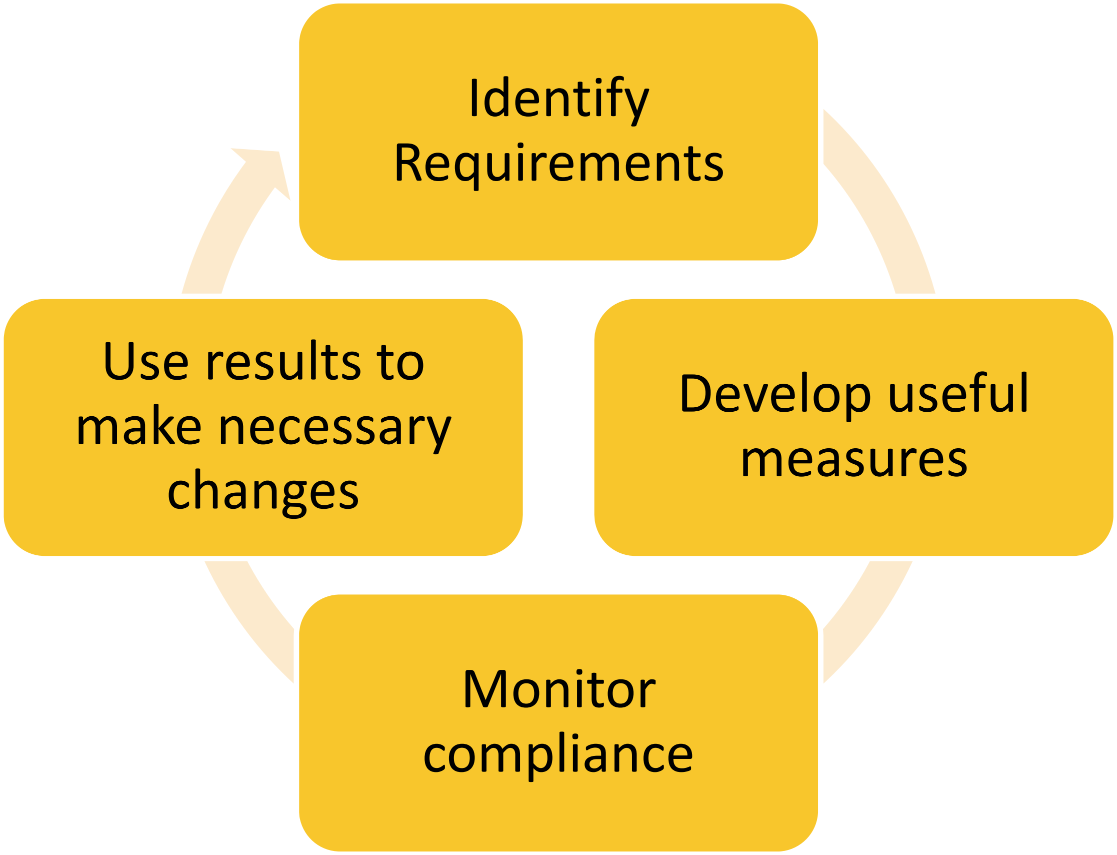
Best Practices in Cyber SLAs

- Guidance from ITIL
  - Service Level Management is component of Service Design
  - Security requirements should entry the lifecycle early
  - Security Management is highly integrated with Service Level Management

- Guidance from ISO/IEC 27002:2005
  - 6.2.1 Identification of risks related to external parties
  - 6.2.3 Addressing security in third-party agreements
  - 10.2.1 Service delivery
  - 10.2.2 Monitoring and review of third-party services
  - 10.2.3 Managing changes to third-party services

A BETTER CYBER SERVICE LEVEL MANAGEMENT PROCESS

Plan, Do, Check, Act



Identify Requirements

Develop useful measures

Monitor compliance

Use results to make necessary changes

Identify Cyber Requirements

- Confidentiality
  - Who has authorized access?
- Integrity
  - Who is authorized to make changes to the data?
- Availability
  - When does the data needed to be accessed?
- Use service (mission) requirements to develop requirements
  - Good:
    - Aligns with needs of the business
    - Can be a check against too much investment/expense
  - Bad:
    - Potentially expensive to develop

Develop Performance Measures

# of 9s	Availability	Downtime per Year	Downtime per Month	Downtime per Week
1	90.0000%	36.5 days	72 hours	16.8 hours
2	99.0000%	3.65 days	7.2 hours	1.68 hours
3	99.9000%	8.76 hours	43.8 minutes	10.1 minutes
4	99.9900%	52.56 minutes	4.32 minutes	1.01 minutes
5	99.9990%	5.25 minutes	25.9 seconds	6.05 seconds
6	99.9999%	31.5 seconds	2.59 seconds	0.605 seconds
7	99.99999%	3.15 seconds	0.259 seconds	0.0605 seconds

Ideas for Measures

- Percentage of (successful, failed) access attempts on confidential data by unauthorized (networks, users, processes)
- Number of incidents involving (successful, failed) unauthorized attempts to export data
- Percentage of inventoried confidential data accessed during cybersecurity incidents
- Number of incidents involving (successful, failed) unauthorized modifications to confidential data

Monitor Compliance

- Use established and agreed measures to monitor the provider
- Measure regularly, not just at the start and end of the relationship

Use the Results

- Use measures to:
  - Ensure your relationships continue to meet your business needs
  - Identify opportunities to adjust the cybersecurity controls for the service
  - Evaluate your cybersecurity investment and identify where investments can change
  - Select third party providers

SUMMARY

Security in knowledge

Conclusion

- Organizations are increasing reliance on third party services. Examples include:
  - Cloud Computing
  - Data backup
  - Operating partners
- Unless security requirements are identified and communicated, organizations have little reason to believe their needs will be met
- Better cyber SLA needs to be developed, as a part of a management process

Bibliography

- http://www.polleverywhere.com
- Verizon 2012 Data Breach Investigations Report
- http://securecomputing.com/
- "Cloud Computing and the Truth About SLAs" Bernard Golden, CIO.com, 09 November, 2011, http://www.cio.com.au/article/406835/cloud_computing_truth_about_slas/
- NIST Special Publication 800-35-Guide to Information Technology Security Services
- FedRAMP Concept of Operations v 1.2
- CobIT User Guide for Service Managers
- ISACA IS Auditing Guide G4: Outsourcing of IS Activities to Other Organizations
- ITIL (Information Technology Information Library) is owned and maintained by the British Office of Government Commerce.

THANK YOU!

Matthew Butkovic

Cybersecurity and Resilience
Measurement Center

mjb101@cert.org

SEI Customer Relations

For general inquiries
customer-relations@sei.cmu.edu
412-268-5800

Sam Merrell

Cybersecurity and Resilience
Measurement Center

smerrell@cert.org

www.cert.org/resilience