Cyber SLAs: Practice and Limitations in “Outsourcing Risk”

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Matthew Butkovic, CISSP, CISA
Technical Manager, CERT Division
January 15, 2015
Key takeaways-BLUF

- Organizations are increasingly reliant on third party information technology services.
- 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.
- Smart cyber security SLAs can help reduce risk to your organization.
What do we mean by external dependencies management?

Managing the risk of depending on external entities to support your organization’s high value services.

External Dependency Management focuses on external entities that provide, sustain, or operate Information and Communications Technology (ICT) to support your organization.
Risk in external dependencies

“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
    - Lowes (2014)
    - DoD TRANSCOM (2014)
    - HAVEX (2014)
    - AT&T (2014)
    - Target (2013)
    - New York State Electric and Gas (2012)
    - California Department of Child Support Services (2012)
    - Thrift Savings Plan (2012)
    - Epsilon (2011)
    - Silverpop (2010)
Case study: HAVEX malware / Dragonfly

"A newer approach used by the attackers involves compromising the update site for several industrial control system (ICS) software producers."
State of cyber SLAs – field research

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

- No: 28%
- Yes: 58%
- Partially: 14%

Does your organization include measures of security performance in agreements?

- No: 30%
- Yes: 56%
- Partially: 14%

Does your organization monitor compliance to security objectives in agreements?

- No: 25%
- Yes: 25%
- Partially: 50%

Is cybersecurity performance considered when selecting third parties?

- No: 18%
- Yes: 68%
- Partially: 14%
Closer look: the role and limitations of formal agreements and SLAs

Organizations should:

- Establish and maintain requirements for external entities
- Include requirements in SLAs and other agreements
- Monitor performance against these agreements

Key point: Managers should understand the role and limitations of contracts and formal agreements
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 Friday²

# SLA restitution

<table>
<thead>
<tr>
<th>Credit</th>
<th>Amazon EC2</th>
<th>Azure Compute</th>
<th>Google Apps</th>
<th>Rackspac e</th>
<th>Terremark/Verizon</th>
</tr>
</thead>
<tbody>
<tr>
<td>10% if &lt;99.95</td>
<td>10% if &lt;99.95</td>
<td>10% if &lt;99.95</td>
<td>3 days if &lt;99.9</td>
<td>5-100%</td>
<td>$1/15 min up to 50% of bill</td>
</tr>
<tr>
<td>25% if &lt;99</td>
<td>7 days if &lt;99</td>
<td>15 days if &lt;95</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bill affected</td>
<td>Future</td>
<td>Current</td>
<td>Current</td>
<td>Current</td>
<td>Future</td>
</tr>
<tr>
<td>Credit filing window</td>
<td>30 days</td>
<td>1 month</td>
<td>30 days</td>
<td>30 days</td>
<td>30 days</td>
</tr>
<tr>
<td>Other comments</td>
<td>Must report within 5 days</td>
<td>$ instead of service permitted</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 - Amazon

“Reasonable and appropriate measures”

“You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security…”

“Limitations of Liability”

- Amazon not responsible for damages

http://aws.amazon.com/s3-sla/
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.
What the auditors expect

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
Interdisciplinary approach

What can Van Halen teach us about Service Level Agreements?
Article 126-Van Halen Contract

“There will be no brown M&M’s in the backstage area, upon pain of forfeiture of the show, with full compensation.”

Source http://www.npr.org/blogs/therecord/2012/02/14/146880432/the-truth-about-van-halen-and-those-brown-m-ms
Plan, Do, Check, Act

- Identify Requirements
- Use results to make necessary changes
- Develop useful measures
- Monitor compliance
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
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

- Reliance on external suppliers, vendors, and third-party entities have to be managed as a risk.
- Smart SLAs can be leveraged to better management external dependencies.
- Make sure to specify at the “requirements” or “control objective” level of detail rather than specific controls.

Getting started:
- taking an inventory or your current providers
- assessing their potential impact on the resilience of mission/service
- and reviewing current SLAs to identify ambiguous language
Contact Information

Matthew Butkovic
Technical Manager
Cybersecurity Assurance
CS2 Directorate
Telephone: +1 412-268-6727
Email: mjb101@cert.org

Web
www.sei.cmu.edu
www.sei.cmu.edu/contact.cfm

U.S. Mail
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Customer Relations
Email: info@sei.cmu.edu
Telephone: +1 412-268-5800
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257