

# 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



Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013 and 252.227-7013 Alternate I.

This material was prepared for the exclusive use of Attendees of CERT Supply Chain Risk Management Symposium and may not be used for any other purpose without the written consent of [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon®, CERT® and CMMI® are registered marks of Carnegie Mellon University.

DM-0002066



# Key takeaways-BLUF

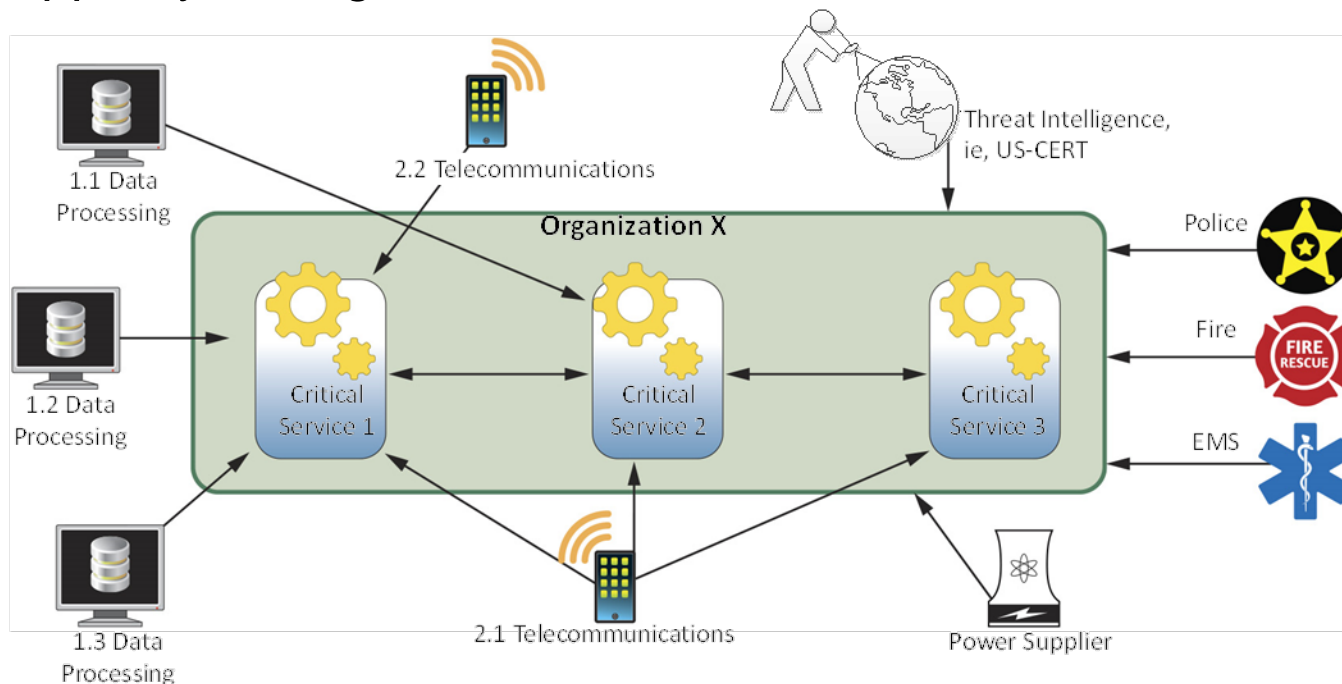
- Organizations are increasingly reliant on third party information technology services.
- Unless cyber security requirements are identified and communicated, organizations have little reason to believe their needs will be met.
- You can't outsource risk to your organization.
- Smart cyber security SLAs 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.”



Dragonfly: Cyberesp

SEI Intranet  
<http://www-internal.sei.cmu.edu/>

**ICS-CERT**  
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME ABOUT ICSJWG INFORMATION PRODUCTS TRAINING FAQ

**Control Systems**

Home

Calendar

ICSJWG

Information Products

Training

Recommended Practices

Assessments

**Alert (ICS-ALERT-14-176-02A)** More Alerts

ICS Focused Malware (Update A)

Original release date: June 27, 2014 | Last revised: July 01, 2014

Print Tweet Send Share

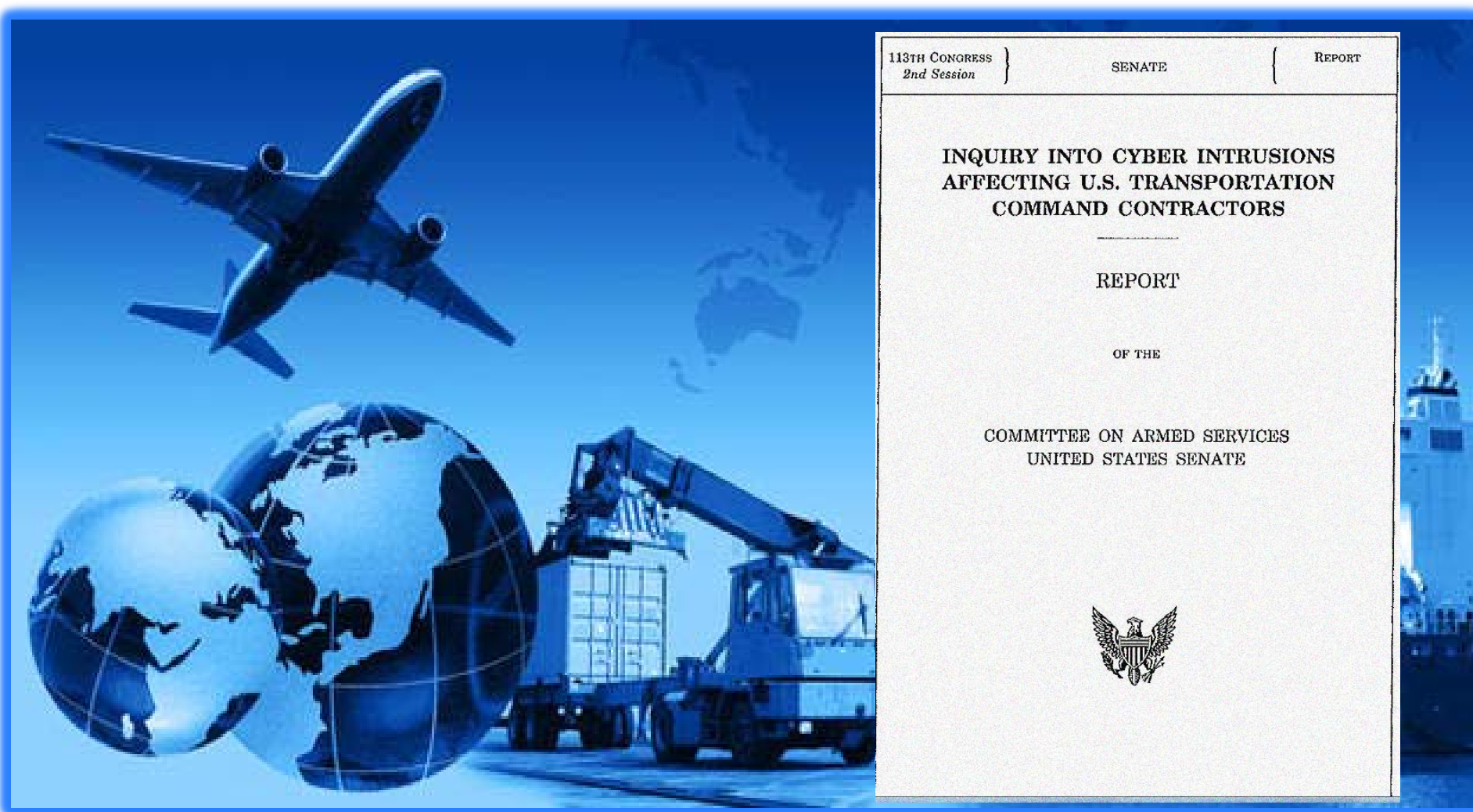
**Legal Notice**

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.





# Case study: TRANSCOM




113TH CONGRESS } SENATE { REPORT  
2nd Session

**INQUIRY INTO CYBER INTRUSIONS  
AFFECTING U.S. TRANSPORTATION  
COMMAND CONTRACTORS**

REPORT

OF THE

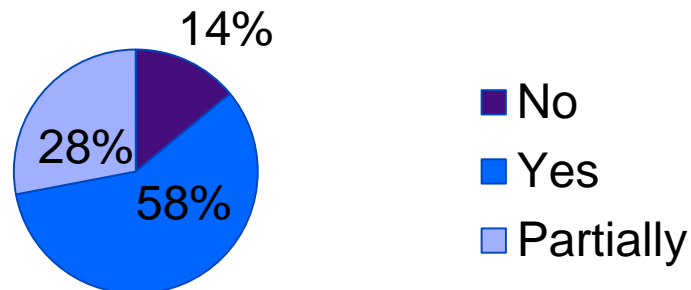
COMMITTEE ON ARMED SERVICES  
UNITED STATES SENATE



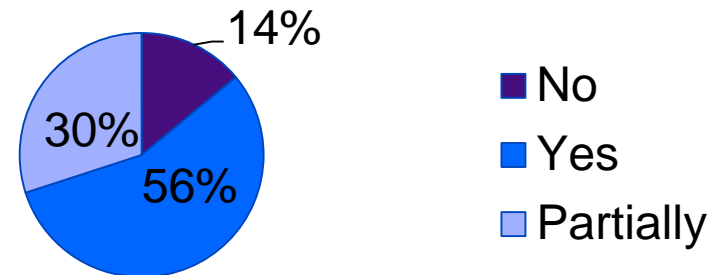


# State of cyber SLAs – field research

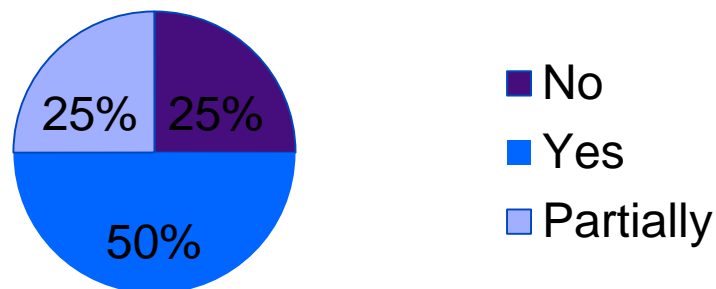
Does your organization document security objectives in agreements with third parties?



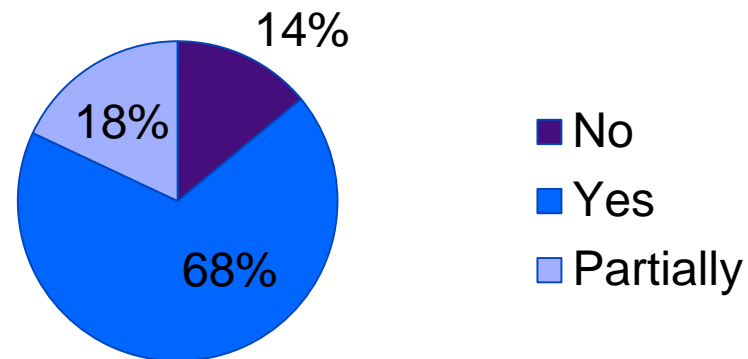
Does your organization include measures of security performance in agreements?



Does your organization monitor compliance to security objectives in agreements?



Is cybersecurity performance considered when selecting third parties?



# 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.<sup>1</sup>”
  - ▶ 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<sup>2</sup>

[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 - 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/>

### 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- Google Apps

“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

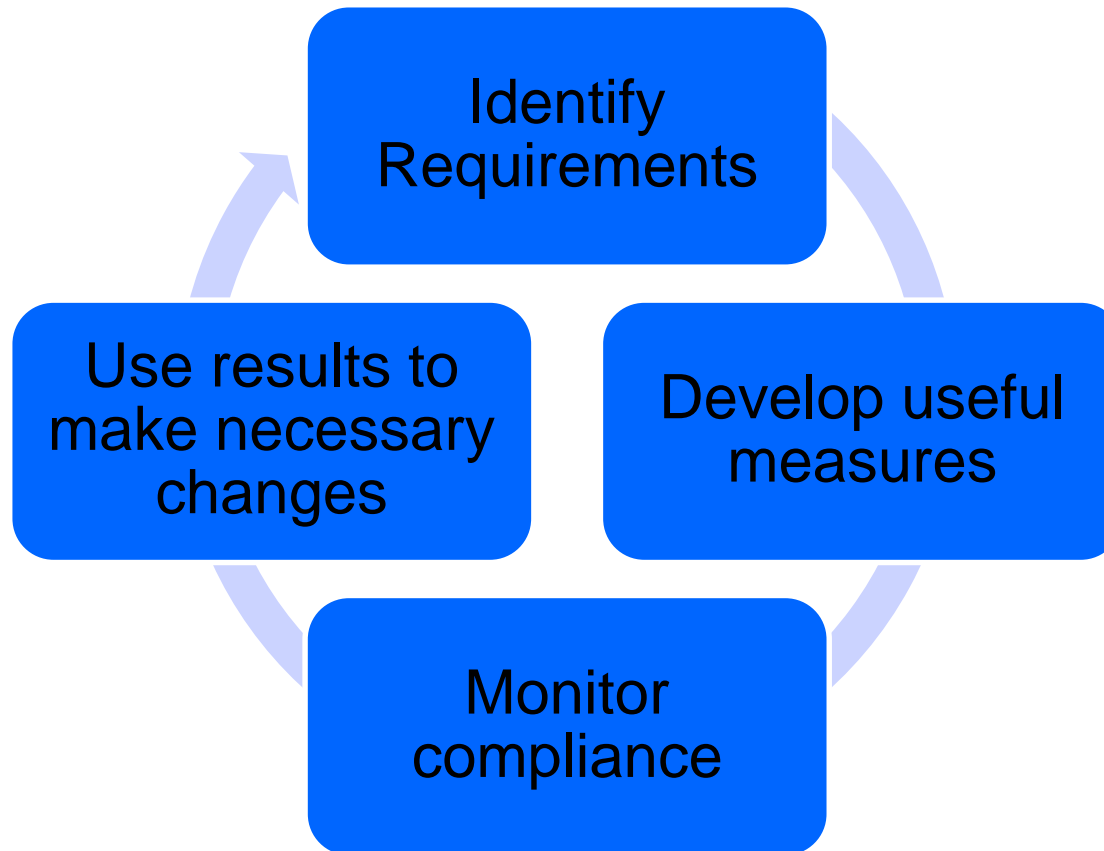
**“There will be no brown M&M’s in the backstage area, upon pain of forfeiture of the show, with full compensation.”**



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 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 of 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](mailto:mjb101@cert.org)

## Web

[www.sei.cmu.edu](http://www.sei.cmu.edu)

[www.sei.cmu.edu/contact.cfm](http://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](mailto:info@sei.cmu.edu)

Telephone: +1 412-268-5800

SEI Phone: +1 412-268-5800

SEI Fax: +1 412-268-6257

