Lessons in External Dependency and Supply Chain Risk Management

October 14th, 2014
Agenda

Introduction and structure
Planning for External Dependencies Management
The Role and limitations of SLAs and agreements
Managing ongoing relationships
Identifying dependencies in complex systems
Monitoring and improving the program
Improving incident management with external entities
Conclusion – a resilience approach
Introduction and structure
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.
Example incidents

- Heartland Payment Systems (2009)
- Silverpop (2010)
- Epsilon (2011)
- New York State Electric and Gas (2012)
- California Department of Child Support Services (2012)
- Thrift Savings Plan (2012)
- Target (2013)
- Lowes (2014)
- AT&T (2014)
- Goodwill Industries International (2014)
- HAVEX / Dragonfly attacks on energy industry
- DOD TRANSCOM contractor breaches
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.

”
Case study: TRANSCOM
External Dependency Management

- Establish and Maintain the Plan
- Establish Relationships
- Monitor and Improve
- Manage Relationships

External Dependencies Management Process
External Dependency Management

- Establish and Maintain the Plan
- Monitor and Improve
- Manage Relationships
- Establish Relationships

External Dependencies Management Process
Planning for External Dependencies Management

Key goals:
- Identify program management objectives
- Identify services
- Prioritize services
- Identify service requirements
- Identify enterprise requirements
- Plan relationship formation
- Plan relationship management
Basic activities already a part of cyber resilience

- Identify services
- Prioritize services
- Identify service requirements
- Identify enterprise requirements

Identify Services
- Identify and prioritize services

Create Asset Inventory
- Identify assets, align assets to services, and inventory assets

Protect & Sustain Assets
- Establish risk management, resilience requirements, control objectives, and controls

Disruption Management
- Establish continuity requirements for assets and develop service continuity plans

Cyber Exercise
- Define objectives for cyber exercise, perform exercises, and evaluate results

Process Management and Improvement
External Dependency Management

- Establish and Maintain the Plan
- Monitor and Improve
- Establish Relationships
- Manage Relationships

External Dependencies Management Process
Question

Do the legal and contracting departments in your organization work closely with the operational staff to make sure contracts really serve their needs?
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
Polling Question 1

Does your organization consider the cybersecurity capability of third parties before forming relationships with them?
Polling Question 2

Does your organization always document security objectives in agreements with third parties that are critical to your business?
State of Cyber SLAs – field research

Does your organization document security objectives in agreements?

- Yes: 58%
- No: 42%

Does your organization monitor compliance to security objectives in agreements?

- Yes: 50%
- No: 50%

Does your organization use ability to meet cyber requirements as partner selection criteria?

- Yes: 68%
- No: 32%
Standard SLAs and Contracts . . .

Basic reasons to have a contract (partial list):

- Risk allocation
- Recovering damages
- Defining breach
- Drive behavior

However in practice Cyber SLAs can be:

- ...unidirectional (they are written by the vendor, and smaller customers have trouble changing them)
- ...lacking specific measures, apart from availability metrics
- ...frequently indemnify the provider to the greatest extent possible, limiting the provider's exposure.
Examples of Cloud SLAs - Amazon

“Reasonable and appropriate measures”
- no specifics
(cannot use to hold accountable)

“”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/
Question

When there are proposed changes to SLAs or third party contracts in your organization, are the operational staff promptly informed and asked for comment?
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: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.
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
Identifying Cyber Requirements

Confidentiality

- Who has authorized access?

Integrity

- Who is authorized to make changes to the data?

Availability

- When is the data needed to be accessed?
Using the Service to Develop Requirements

Use service requirements to develop requirements for information confidentiality and integrity

- **Good:**
  - Aligns with needs of the business
  - Is a check against too much investment/expense
- **Bad:**
  - Expensive to develop
A better SLA management process . . .

Plan, Do, Check, Act

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

© 2014 Carnegie Mellon University
Limitations of formal agreements

Question: What are the limitations of formal agreements in this case?

How do I prove breach?

What are my damages (in monetary terms)?
External Dependency Management

- Monitor and Improve
- Establish and Maintain the Plan
- Establish Relationships
- Manage Relationships

External Dependencies Management Process
Managing relationships: HAVEX malware / Dragonfly

“A newer approach used by the attackers involves compromising the update site for several industrial control system (ICS) software producers.”
A closer look: Havex incident and identifying ongoing dependencies

Procurement  Deployment  Operation

Who is managing this relationship?

Periodic software downloads from manufacturer website
Requirement: 100% integrity of downloaded software installers
Question

Does your organization have an established process to recognize external cyber dependencies?
Identifying dependencies: one possible approach

Service
ex: “9/11 Dispatch”

People

Info

Tech

Facilities

Business Processes

Standard relationships, assets to third parties

Employs
Stores
Owns

Protects
Transmits
Operates

Sustains
Processes
Protects
Maintains

Transports
Protects
Updates

Vets

Processes
Monitors

. . .

. . .

. . .
After identification: prioritization and tiering

Where do we start?
After identification: prioritization and tiering

By prioritizing:

For global transportation of material:
The critical external entities are . . .
The high impact external entities are . . .
The low impact external entities are . . .
Question

How does your organization prioritize vendors and other third parties for governance?
External Dependency Management

- Establish and Maintain the Plan
- Establish Relationships
- Manage Relationships
- Monitor and Improve Dependencies Management Process

© 2014 Carnegie Mellon University
For external dependencies management:

Are we actually implementing the program?

Are we detecting and correcting process exceptions?

Is the external dependency management activity effective?

Do we review the program with our stakeholders?

Are we improving the plan as needed?
For external dependencies management:

Are we actually implementing the program?

Are we detecting and correcting process exceptions?

Is the external dependency management activity effective?

Do we review the program with our stakeholders?

Are we improving the plan as needed?
List of possible effectiveness measures

- external dependencies risks or potential risks that remain unresolved
- open or unresolved high-risk supplier issues
- aging statement for corrective action reporting
- count of external entity relationships formed outside of the process
- emerging threats or risks that may affect key dependencies or suppliers
- number and frequency of critical service outages traceable to external entities
- percentage of external entities that have successfully passed third-party audits
- percentage of missed deliveries or shipping delays from external entities
- contracts or agreements that did not follow established procedures or policy
- percentage of SLAs across key external entities (e.g., tier 1 and tier 2 suppliers) that include resilience requirements in their agreements
- response times and other metrics relating to business continuity or cybersecurity drills conducted with external entities
Example area: Integrating service continuity and incident management

Figure 6: Who identifies data breaches

- UNRELATED PARTY: 28%
- FRAUD DETECTION: 24%
- USER: 10%
- CUSTOMER: 9%
- LAW ENFORCEMENT: 8%
- PERPETRATOR: 7%
- FINANCIAL AUDIT: 3%
- INTRUSION DETECTION: 2%
- LOG REVIEW: 1%
- FRAUD DETECTION: 1%
- INCIDENT RESPONSE: 1%
- IT AUDIT: 1%

Many organizations devote a disproportionate amount of time and money to detection methods that fall below the 1% mark.
External entity questions . . .

1. Does organizational incident management and service continuity planning account for dependence on external entities?

2. Do external entities participate in the organization’s incident management and service continuity planning?

3. Does the organization verify that external entities have service continuity and incident management plans that are consistent with the critical service?

4. Have criteria for the declaration of an incident been established and communicated?
Incident declaration criteria:

Report incidents that “affect organizational information resident or in transit on vendor systems”

How do we assess the effectiveness of this control?

Very challenging, some possibilities:

- Event reporting?
- Reporting on technical detection?
- Situational awareness and collaboration?
Question

How would you evaluate whether or not the external entities your organization depends on are doing effective incident management?
Conclusion – a resilience approach
Cyber Resilience Value Proposition

**Resilience management** provides support to *simplify* the management of complex cybersecurity challenges.

**Efficiency**: not too much and not too little; resilience equilibrium
- balancing risk and cost
- getting the most bang for your buck
- achieving compliance as a by-product of resilience management

**Roadmap**: what to do to manage cybersecurity; flexibility and scalability
- using an overarching approach - which standard is best
- deciding what versus how to manage cybersecurity risk

**Cybersecurity ecosystem**: addressing the interconnectedness challenge
- managing dependencies
- addressing both internal and external organizational challenges and silos
Process Maturity for Cyber Resilience

The degree of process maturity can help to answer several important questions when managing cyber resilience:

- How well are we performing today?
- Can we repeat our successes?
- Do we consistently produce expected results?
- Can we adapt seamlessly to changing risk environments?
- Are our processes stable enough to depend on them during times of stress?
- Can we predict how we will perform during times of stress?

Process maturity helps avoid the pitfalls of a project (set and forget) approach to cyber resilience and helps “make it stick.”
What Is Cyber Resilience?

“... the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents...”

- Presidential Policy Directive – PPD 21
  February 12, 2013

<table>
<thead>
<tr>
<th>Protect (Security)</th>
<th>Sustain (Continuity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform (Capability)</td>
<td>Repeat (Maturity)</td>
</tr>
</tbody>
</table>
Key practices based on recent field work

Does your organization have a plan for managing external dependencies?

- Yes: 79%
- No: 21%

Does your organization periodically measure external dependency activities to ensure they are effective?

- Yes: 70%
- No: 30%

Is there management oversight of the performance of external dependency management activities?

- Yes: 40%
- No: 60%

Relating to implementation of external dependency management practices, three activities seem to drive behavior*:

- Planning
- Measuring
- Reporting

*171 critical infrastructure organizations
External Dependency Management –
Work Underway at Carnegie Mellon CERT

Two key components:

1. An organizational assessment for external dependencies management

2. Exploring better ways for organizations to identify and prioritize cyber dependencies

“The Information and Communications Technology (ICT) services used by operators of critical infrastructure, on which the delivery of a critical infrastructure service depends.”
External Dependency Risk Management Assessment

**Purpose:** To understand the organization’s ability to manage the risks of dependence on external entities for information and communications technology related services. A focused examination of practices and capabilities for managing external entity risk.

Based on the *DHS Cyber Resilience Review* and the *CERT® Resilience Management Model (CERT® RMM)*, a process improvement model for managing operational resilience

- Developed by Carnegie Mellon University's Software Engineering Institute

Piloting of the approach is underway with critical infrastructure organizations
In Closing……

- External dependency management is one of today’s key business challenges
- Dependencies extend well beyond just your vendors
- Relationships and partnerships are key – organizations cannot effectively manage dependency risks on their own
- The complexities of the today’s cyber and physical disruption landscape requires new tools
- Taking a converged approach to the challenge is key
- Resilience management can help provide a roadmap to simplify the management of operational and dependency risks
CMU – CERT Supply Chain Risk Management Symposium, January 15th 2015 in the DC area. For information contact info@sei.cmu.edu

Contact Information:
John Haller – jhaller@cert.org
Matthew Butkovic – mjb101@cert.org