Legal Risk and Uncertainty in Managing Services, Vendors, and Contracts

2016 Enterprise IT Summit
Patrick Feehan
Joanna Grama
“DO NOT LET PERFECT BE THE ENEMY OF GOOD.”

- ME, AS I REVIEW THE RISK OF A CLOUD SERVICE PROVIDER OFFERING WE’VE (LIKELY) ALREADY PURCHASED.
Agenda

• Change/Cloud Service providers
• Context of Risk
• Trust
• Mechanisms of Risk Review and Management
  – Contract
  – SOC/Third party Certification
• Discussion/group activity
  – Parameters of Risk Inquiry
Change

Technology Advancement
1953
Dissatisfaction
Increasing Expectations

1965
CLOUD
Service Providers

2007
Minicomputer
Smaller Affordable
“US”

2011
Mobile Devices
Phone to Mobile Web
“WEEEEEEE!”

Technology Advancement
Dissatisfaction
Increasing Expectations

Internet and the Web
Global Info – Locally Linked “WE”

1991
Local Area Networks
Ethernet “US”

Technology Advancement
Dissatisfaction
Increasing Expectations

1983
Personal Computer
Microprocessors “ME”

Technology Advancement
Dissatisfaction
Increasing Expectations

Technology Advancement
Dissatisfaction
Increasing Expectations
Cloud Service Providers

Invariably, the Cloud Service Provider which draws our interest does so because of the technology

That technology becomes the driver

Risk considerations oftentimes backfill or establish (affirm) the risks of that technology, without necessarily changing the transaction’s trajectory.
Cloud Service Models

- **Apps as a Service**
- **Platform as a Service**
- **Infrastructure as a Service**

- Configuration Management
- Operating System
- Server Hardware, Storage, Backup, Encryption, Accounting
- Physical Space, Electricity, Environmental, and Security Controls
Context of Risk

The ERP Shift Engenders a Risk Management Shift

ERP Then (2010)

ERP is a software application that acts as the central college-wide information system. The ERP modules integrate all of the college’s units, departments and geographical locations into a single, shared, unified and enterprise-wide information system.
Context of Risk

The ERP Shift to Cloud or Cloud Hybrid

ERP Now (2016)

ERP solution integrates all functions into a minimum number of core administrative systems and common authoritative databases.
Context of Risk

Securitization of the Enterprise Transforms to Meet Threats

Network Security Then (2010 – Border Based)

Border Router
Perimeter firewall
Internal firewall
Intrusion Detection System
Policies & Procedures & Audits
Authentication
Access Controls
Context of Risk

Securitization of the Enterprise Transforms to Meet Threats

Network Security Now (2016)

Reconnaissance
- Harvesting Email Addresses
- Conference Information, System Administrators

Weaponization
- Creating a Deliverable Payload

Delivery
- Delivered to victim via email, web, USB, etc.

Exploitation
- Exploiting a Vulnerability to Execute on Victim’s System

Installation
- Installing Malware on the Asset

Command and Control
- Command and Control for Remote Manipulation of the Victim’s System

Actions on Objectives – Payload
- Hands on the Victim’s Keyboard, Accomplish Task

Lockheed Martin’s Cyber Kill Chain – Attacks Have an Operational Life Cycle (SANS)
Controls to Detect, Deny, Disrupt, Degrade, Deceive, Recover in the Face of New Threats

<table>
<thead>
<tr>
<th>Detect</th>
<th>Deny</th>
<th>Disrupt</th>
<th>Degrade</th>
<th>Deceive</th>
<th>Respond/ Contain/ Recover</th>
</tr>
</thead>
</table>

Security controls aim to detect, deny, disrupt, degrade... the attacks; however the enterprise is constituted.
## Context – Security Controls For Each Phase of the Attack – Mostly in Place

<table>
<thead>
<tr>
<th>Phase</th>
<th>Detect</th>
<th>Deny</th>
<th>Disrupt</th>
<th>Degrade</th>
<th>Deceive</th>
<th>Respond/ Contain/ Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recon</strong></td>
<td>Threat Intelligence, Web analytics, IDS, SIEM/Log Mgmt, Asset Mgmt</td>
<td>Information Sharing, Firewalls, IPS</td>
<td>Patch Mgmt</td>
<td>Patch Mgmt</td>
<td>Patch Mgmt</td>
<td>SIEM/Log Mgmt, Forensics</td>
</tr>
<tr>
<td><strong>Weaponization</strong></td>
<td>User training, SIEM/Log Mgmt, IDS, HIDS, Threat Intelligence</td>
<td>Change Mgmt, File Integrity, Whitelisting, WAF, Endpoint protection, Email protection, IPS, Firewalls, Threat Intelligence</td>
<td>Inline AV, Email protection, WAF</td>
<td>Patch Mgmt</td>
<td>Patch Mgmt</td>
<td>Patch Mgmt, Forensics</td>
</tr>
<tr>
<td><strong>Delivery</strong></td>
<td>Endpoint protection, HIDS, SIEM/Log Mgmt</td>
<td>Patch Mgmt, PAM, HIPS, Endpoint protection, Least privilege, Hardened config, File Integrity, Whitelisting, Execution blocking</td>
<td>DEP, EMET, Hardened config, HIPS, Endpoint protection</td>
<td>Least privilege</td>
<td>Least privilege</td>
<td>Honeypot, WAF, SIEM/Log Mgmt, Patch Mgmt, Forensics</td>
</tr>
<tr>
<td><strong>Exploitation/ Installation</strong></td>
<td>SIEM/Log Mgmt, IDS, HIDS, Endpoint protection, Threat Intelligence, DNS</td>
<td>Least Privilege, 2FA, Secure Password, IPS, Firewalls, Threat Intelligence</td>
<td>IPS</td>
<td>Tarpi</td>
<td>DNS Redirnt Honeypot</td>
<td>DNS Sinkholes, WAF, SIEM/Log Mgmt, Forensics, DNS</td>
</tr>
<tr>
<td><strong>Command and Control</strong></td>
<td>SIEM/Log Mgmt, IDS, HIDS, Endpoint protection, Threat Intelligence, DNS</td>
<td>SIEM/Log Mgmt, IDS, HIDS, Endpoint protection, Threat Intelligence, DNS</td>
<td>IPS</td>
<td>Tarpi</td>
<td>DNS Redirnt Honeypot</td>
<td>DNS Sinkholes, WAF, SIEM/Log Mgmt, Forensics, DNS</td>
</tr>
<tr>
<td><strong>Internal Recon/ Lateral Movement</strong></td>
<td>SIEM/Log Mgmt, PAM, AD, Asset Mgmt</td>
<td>Firewalls, Network segmentation, HFW, Egress filtering, Least privilege, PAM, 2FA, NAC</td>
<td>Hardened config, Network segmentation, NAC</td>
<td>Honeypot</td>
<td>SIEM/Log Mgmt, Forensics</td>
<td>Firewall ACLs, SIEM/Log Mgmt, Forensics, Cyber Insurance, Backups, PII scanning</td>
</tr>
<tr>
<td><strong>Action on Targets</strong></td>
<td>SIEM/Log Mgmt, Threat Intelligence,</td>
<td>Outbound ACL, Egress filtering, Threat Intelligence, Encryption</td>
<td>DLP, Network segmentation, 2FA, Encryption, PII scanning</td>
<td>Quality of Service, Email frotting</td>
<td>Honeypot</td>
<td>Firewall ACLs, SIEM/Log Mgmt, Forensics, Cyber Insurance, Backups, PII scanning</td>
</tr>
</tbody>
</table>
Context

Add in the Migration of Parts of the Enterprise to the Cloud and the Security Controls Potentially Broaden to Achieve the Same Aims Regardless of the Enterprise Location.

Holistic Ubiquitous Controls
- CASB
- DLP
- Virtual Firewall
- Next Gen Firewall
- Host Based Firewall
- Web Firewall
- Network Access Control
Trust

The Shift to Cloud or Hybrid-Cloud Requires Trust

Whom Do We Trust With Our Data?

We trust ourselves – our own infrastructure, our own systems, our own people. It is built into our policies and processes.

Maybe trust isn’t the right word. We understand our people. We can touch or see our own infrastructure.
Trust

The Shift to Cloud or Hybrid-Cloud Requires Trust

Whom Do We Trust With Our Data?

So if we are moving that infrastructure or some services, we seek some kind of assurance that a new infrastructure or service is as trustworthy as what we know, without the advantage of it being tactile, or at least tactile to someone in our organization.
Gartner suggests three different types of cloud vendors and in our recognition of the type, generates the level of comfort we have day to day, and the level of scrutiny we want day to day.

Gartner also warns:
- Going to the cloud will compromise some of your control.
- There is no perfect.
Gartner Level 1 Cloud Provider
Gartner Level 2 Cloud Provider
Gartner Level 3 Cloud Provider
Mechanisms of Risk Review and Management

You can always negotiate...something

The Contract:

1. SLA/SLEs
2. Authentication?
4. Liability – Our liability is subject to state law
5. Funding – We might not control ours.
7. Warranties? (excluded?)
8. Termination? Data Recovery on Termination?
9. Indemnification?
10. Data Backups? Encryption?
Mechanisms of Risk Review and Management

SOC Reports

SOC (Service Organization Control) Reports: Created by AICPA - User Entities (that’s us) that outsource internal functions to cloud service providers (called Service Organizations). We want to see these now and annually.

SOC 1 – Takes the place of SAS 70, reports on controls at a service organization relevant to a user entity's internal control over financial reporting. Helpful in talking to our own auditors.
Mechanisms of Risk Review and Management

SOC Reports

**Security:**
- IT Security Policy
- Security Awareness
- Risk Assessment
- Logical Access
- Physical Access
- Security Monitoring
- User Authentication
- Incident Management
- Personnel Security

**Availability**
- Availability Policy
- Backup
- Disaster Control
- Business Continuity

**SOC 2** – Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. Auditor’s tests of controls and results.
Mechanisms of Risk Review and Management

*What Third Party Certifications Do They Have?*

**ISO/IEC 27001:2013**

Specification for an information security management system (ISMS). Organizations may be certified compliant by an independent and accredited certification body on successful completion of a formal compliance audit. A CSP should want to share this certification.
Mechanisms of Risk Review and Management

Our Own “New Cloud Vendor Assessment Form” or similar. We conduct our own trust session. It may turn out fruitful:

<table>
<thead>
<tr>
<th>Question</th>
<th>Vendor Response</th>
<th>ITSG Assessment of Acceptability</th>
</tr>
</thead>
<tbody>
<tr>
<td>63</td>
<td>Johnson leverages collection services from Smith in Southern Idaho. The Southern site is a Tier IV, providing 99.95% uptime and multi-tenant security.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>64</td>
<td>How do you ensure access to your data facilities where customer data will be stored?</td>
<td>Yes</td>
</tr>
<tr>
<td>65</td>
<td>Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?</td>
<td>Detailed in Johnson SOC 2 Audit Document</td>
</tr>
<tr>
<td>66</td>
<td>How are these security controls monitored?</td>
<td>Yes, Detailed in Johnson SOC 2 Audit Document</td>
</tr>
<tr>
<td>67</td>
<td>Are the vendor premises separated into different control areas such as server computer room, operation area, loading delivery area, and others? Please specify how the access controls are in place in each separate area</td>
<td>Yes, Detailed in Johnson SOC 2 Audit Document</td>
</tr>
<tr>
<td>68</td>
<td>Are multiple tenants occupying this facility? If Yes, please specify how tenants are separated.</td>
<td>Yes, Physical cages</td>
</tr>
<tr>
<td>69</td>
<td>Is access to areas where work is performed for customer physically separated from that of other clients? If Yes, describe the separation.</td>
<td>Yes, Physical cages</td>
</tr>
<tr>
<td>70</td>
<td>Is access to the facility controlled by the use of a token-based card access control system? If Yes, describe the authorization process for requesting access, including changes.</td>
<td>Yes, Detailed in Johnson SOC 2 audit document</td>
</tr>
<tr>
<td>71</td>
<td>Are visitors required to sign in, receive ID badges and escorted while on premises?</td>
<td>Yes</td>
</tr>
<tr>
<td>72</td>
<td>Is the facility equipped with surveillance camera(s)?</td>
<td>Yes</td>
</tr>
<tr>
<td>73</td>
<td>Do security cameras cover inside and outside doors and confidential areas?</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Mechanisms of Risk Review and Management

Or less than amazing (imperfect, as we say):

<table>
<thead>
<tr>
<th>Question</th>
<th>Vendor Response (respond to questions that are applicable to the application or service provided)</th>
<th>ITSG Assessment of Acceptability (responses may include acceptable, not enough information provided, or N/A -- not applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there one person assigned to lead, manage and be accountable for security?</td>
<td>No</td>
<td>Not enough information provided</td>
</tr>
<tr>
<td>Is that person at least at a director level?</td>
<td>No</td>
<td>Not enough information provided</td>
</tr>
<tr>
<td>Does your company have a dedicated security team? If so, roughly how many people are on it.</td>
<td>No</td>
<td>Not enough information provided</td>
</tr>
<tr>
<td>Does your company have a corporate security policy? Please provide separately.</td>
<td>no</td>
<td>Not enough information provided</td>
</tr>
</tbody>
</table>
Mechanisms of Risk Review and Management

Our Own Internal Audit Demands Due Diligence – Use It

Our Own Audit – Do We outsource?

2. i) Does the Applicant outsource any part of their information handling, network, computer system, or information security function? Yes No

If “Yes”, indicate the name of the vendor providing the service:

<table>
<thead>
<tr>
<th>Service</th>
<th>Managed Security</th>
<th>Data Processing</th>
<th>Alert Log Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Processing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Service Provider</td>
<td><em>See Note</em></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Intrusion Detection:
Mechanisms of Risk Review and Management

Our Own Internal Audit Demands Due Diligence – Use It

Our Own Audit – What Is Our Due Diligence Before Outsourcing?

ii) Please check all due diligence that applies before engaging with a new vendor:

- [ ] Formal assessment of the security risks associated with the vendor
- [ ] A means to assess the vendors’ security posture such as SAS70, CICA Section 5970, BITS or otherwise
- [ ] Contractual provision to indemnify the organization in the event of a security failure or loss on confidential information

And Do We Verify?

iii) Does the Applicant have a formal process in place to verify that the services are being performed as dictated by the contract?  

- [ ] Yes  
- [ ] No
Discussion/group activity

*Talk amongst yourselves, 15 mins.*

**Parameters of Risk Inquiry**

- Items Which May or May Not Have Satisfactory Answers
- But We Ask Anyway

**Rank By:**

- Greatest concern
- Least concern
- Greatest concern, least satisfying answer
Parameters of Risk Inquiry

1. Auditing and forensics
2. Business continuity and disaster recovery
3. Data backups
4. Data segregation
5. Encryption of data
6. Institutional data availability
7. Institutional service availability
8. Operational security
9. Physical security
10. Security compliance and certifications
11. Service management
Thank You.

• Patrick Feehan – patrick.feehan@montgomerycollege.edu
• Joanna Grama - jgrama@educause.edu