Understanding Third-party Risk in the Cloud

Damian Chung
Business Information Security Officer

PROTECT DATA AND USERS EVERYWHERE
SAFELY ENABLE THE CLOUD AND WEB
DELIVER SECURITY THAT IS FAST AND SCALABLE

cybersummitmn
The Evolutionary Focus of Third-party Risk in the Risk Management Domain
# Third-party Risk Management Process

<table>
<thead>
<tr>
<th>Understand the risks associated with business requirements</th>
<th>Risk alignment with the third-party</th>
<th>Determine proper security controls</th>
<th>Evaluate and validate controls</th>
<th>Define a continuous monitoring program</th>
</tr>
</thead>
</table>

**UNDERSTANDING THIRD-PARTY RISK IN THE CLOUD**
Steps to Managing Third-party Risk

**Inherent Risk**

**STEP 1**
Relationship Risk

**STEP 2**
Business Profile Risk

**Mitigating Controls**

**STEP 3**
Security Controls Assessment

**STEP 4**
Controls Validation

**STEP 5**
Monitoring and Reporting

**Residual Risk**

MINUS

EQUALS
Traditional Assessments

- A third-party risk assessment questionnaire, but does it work for cloud applications?
- Use a third-party to evaluate third-party vendors
- Evaluate risk of an enterprise’s public IP
- Blind trust
- SLA and MSA reviews

The traditional way is on a collision course for failure!
Risks in the Cloud Are Real

Cloud service providers mitigate all risk, right?

Nope!

Companies know where their data is going

Companies know the type of data that is moving

Not Exactly

Companies know how the data is moving

Maybe…

Third-party risk management is broken!
Expectations vs. Realities of Addressing Third-party Risk
Digital Transformation Induced Shifts

The perimeter has dissolved, yet 90% of Enterprise Security spend is on-premise approaches.

- 90% Data created in the last two years
- 90% Enterprise devices that are mobile
- 85% Enterprise internet traffic has moved to SaaS / Cloud
- 2% Percentage of SaaS apps that IT controls and secures
What You Already Know about Third-party Risk in the Cloud

- Cloud applications are inexpensive
- Business is looking for “ease of use”
- Cloud applications must be fast with minimal latency
- Compliance standards highlight third-party risk
- Most applications are hosted in a cloud data center (AWS, Azure, Google Cloud)
**Compliance Measures**

- SOC Reports, cybersecurity insurance, NDAs, MSA's, SLA's
- Risk assessments required for compliance checks
  - National Institute Standards Technology (NIST) Special Publication (SP) 800-53r4 and NIST Cybersecurity Framework (CSF) v1.1 Standards and Frameworks
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Payments Card Industry (PCI) Data Security Standards
  - Federal Acquisition Regulation (FAR)
  - Gramm-Leach-Bliley (GLB)
- Do paper-based policies and statements mean security?
<table>
<thead>
<tr>
<th>What You May Not Already Know About Third-party Risk in the Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility of cloud applications</td>
</tr>
<tr>
<td>Types of data that resides in cloud applications</td>
</tr>
<tr>
<td>The risk of cloud applications</td>
</tr>
<tr>
<td>Identities being used for cloud applications</td>
</tr>
<tr>
<td>Types of data that is being used during a POC</td>
</tr>
</tbody>
</table>
How Traditional Threats are Evolving

- Hunting for publicly accessible IaaS resources like S3 buckets and repos
- Malware Infection through Cloud
- Using Cloud Resources for C&C or storing payloads
- Using the Cloud to Hide Phishing
- Exploiting Application vulnerabilities running on cloud services to launch attacks
- Brute forcing weak passwords for public facing services
Challenges to Addressing Third-party Risk in the Cloud

- Smaller companies with a unique solution may not have a security program.
- Many cloud applications have limited to no cybersecurity insurance.
- Third-parties are using sub-contractors, introducing fourth-party risk.
- There is a privacy concern of personal vs business data.
- Businesses are extending their virtual boundaries.
Improving Third-party Risk Assessment in the Cloud
How Are you Evolving?
The Future of Cloud Risk Assessments

Evaluate what data is being used
Configuration controls in place to monitor or block cloud applications
Identify potentially risky cloud applications
Ensure MSA includes the Right-to-Audit clause
Invoke identity challenges for access to sensitive data
How to Enable Your Business

Understand the business needs for cloud applications

Become a champion of digital transformation

Be agile to support business to build faster
VISIBILITY IS KING.
GET IT BACK.
## Recommendations

<table>
<thead>
<tr>
<th>Build relationships with supply chain and procurement</th>
<th>Extend data classification into cloud applications</th>
<th>Identify the cloud applications being used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educate the workforce</td>
<td>Be a partner with the business</td>
<td>Understand innovative risk</td>
</tr>
</tbody>
</table>
Ask the Right Questions:

1. Data Sovereignty: Where does the data live?
2. Ownership: Who owns the data rights?
3. Portability: Can we download data at end of contract?
4. Retention/Destruction at end of contract
5. Compliance: Standards and Certifications
## Insider, Data, & Configuration Controls

<table>
<thead>
<tr>
<th>Continuous Security Assessment</th>
<th>Breach Detection and Response</th>
<th>Cloud &amp; Web Service Data Protection</th>
<th>Insider Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhance visibility, prevent security exposure, and simplify governance &amp; compliance</td>
<td>Detect &amp; prioritize active threats across all web and cloud services</td>
<td>Identify, and Prevent sensitive data from being sent to uncontrolled Cloud and Web services.</td>
<td>Control access to unmanaged cloud services and prevent data exfiltration</td>
</tr>
<tr>
<td><strong>Data Protection</strong></td>
<td><strong>Threat Protection</strong></td>
<td><strong>Insider Threat Protection</strong></td>
<td></td>
</tr>
<tr>
<td>Detect malware sent to or from Cloud services or being executed from a trusted cloud</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Questions?

Visit the Netskope Booth