NEXTGEN VENDOR RISK MANAGEMENT

How To Raise the Bar for <>aaS Providers

Mike Jackson
OVERVIEW

• Risk Management
• Vendor Risk Management
• Real Stories of Security MSSPs
• Tricks of the Trade: Raising the Bar
• <>aaS Risk Dump
A PROBABLE BAD DAY IN INFORMATION SECURITY…

Data Theft of the Wrong Kind? ATO? Third Party’s Third Party’s Third Party Breach, Distributed Denial of Service Attack (DDOS)? Insider Fraud? Yes but how about when...

- ...the security team finds out that the company does not exist to run a information security program
- ...or security spending is a business decision anchored to the business’ economic engine
- ...or if the security team shoots the economic engine in the foot with technology or policy, that people really get upset
The world is a risky place, no one makes it out alive.
RISK MANAGEMENT

- **Risk is talk about loss exposure**—the probable frequency and probable magnitude of future loss (in dollar amounts preferably)
- **We are not very good at discerning future risk**

Economists Estimate Human Civilization Still Years Away From Turning Profit – The Onion

- “In many ways, humanity still hasn’t recovered from the collapse of colonialism, when it was poised to become very profitable indeed,” said Holloway, explaining that mankind “made a killing” through the mid-20th century but that its exploitation of new assets proved unsustainable. “The abolition of slavery and indentured servitude have also severely hampered profitability, causing labor costs to spiral out of control and pushing off the financial break-even point for humanity by at least a millennium. Whatever the case, human beings need to boost earnings somewhere if they’re ever going to get out of the red. Thankfully, they do have the new iPhone rollout on the horizon next year, so that should be a pretty big boost for them,” she added.
RISK MANAGEMENT

- Between 1970 and 2007 Mueller and Stewart asserted in a separate paper published in *Foreign Affairs* that a total of 3,292 Americans (not counting those in war zones) were killed by terrorists resulting in an annual risk of one in 3.5 million.
  - Americans were more likely to die in an accident involving a bathtub (one in 950,000 annualized)
  - A home appliance (one in 1.5 million annualized)
  - Struck by lightning (one in 960,000 annualized)
  - Struck by lightning twice in a lifetime (one in 9 million aggregate)
  - A deer (one in two million annualized) ….and on and on and on and we haven’t even touched on higher probability health related loss of life events (cancer, smoking, etc..)
Information security (to a business person) is about putting things in place to reduce loss exposure (risk) in order to be more profitable long term.
Paranoia is simply the result of ineffective risk management.

Paranoia is the art of overthinking, literally creating problems that may not be there.

Business leaders understand that the biggest risk to a business is having one. They live in the tension of risks every day, of which cyber risk is only one of many damaging possibilities. This is why frameworks exist to manage risks—to create peace of mind—to know that they are aware of loss exposure possibilities and are in the driver’s seat of managing, mitigating, accepting, or transferring that risk base on appetite.

“We’ve eliminated all risks to the business by cutting everyone’s pay checks to pay for it.”
Throwing your RCM at an attacker is not an effective countermeasure. The RCM is not designed to protect you. It’s designed to govern and manage risk.

Perhaps the single most effective countermeasure—well run (managed) IT.
My Data + Little Confidence in my Cost Contained and Resource Strapped Security Program <>aaS
VRM

- Does my vendor have their act together?
- Concluding on the effectiveness of a <>aaS provider internal control environment in order to properly respond to risks they may present
- Includes risk scoring vendors and periodic reviews against a set of criteria to ensure risk levels do not degrade past an acceptable threshold
- Responses include:
  - Mitigate (contract language, on site audits, don’t buy that service)
  - Accept (service may be so valuable that risks don’t matter)
  - Transfer (insurance, limitation of liability or warranty provisions)
VRM HIGH LEVEL

Data Classification
Business Criticality

Weight Riskiness—Determine Approach

Approach to VRM

Weight * Risk Score

Review Schedule
Response Activity

Like all things breach related, it ain’t that easy or simple.
Investors get it. Why not information security?
COMMON TOP DOWN APPROACHES

- Certifications and Attestations
  - FEDRamp, ISO 27001
- Control Reports
  - SAS70 → SSAE 16 → SOC 1, 2, 3 Type I, II
- Questionnaires
  - https://github.com/google/vsaq
- Guided Conversations / References

Paranoia Here?
CERTIFICATIONS AND ATTESTATIONS

- ISO Attestation – NO CONTROL TEST EVIDENCE!!
- Nothing about this in the MSA. After you read it, it has no bearing on the agreement unless you add something to the MSA.
- Subjective opinion of paid assessor by company (could be anyone)
- Assessor more often than not struggles to understand technology
- Top down checkmark, bottom up holes everywhere? Exactly.
- Cyber insurance underwriting help please?

We have examined assertion that (1) the description of its controls supporting the ISO/IEC 27001:2013 (“ISO 27001”) certified information security management system (“ISMS”) for the global cloud operations (collectively “the controls supporting the ISMS”) included in Section 3 (the “description”) provided to organizations that use the global cloud operations as of July 7, 2016 (the “report date”), is fairly presented and that (2) the controls supporting the ISMS, as stated in the description, were designed and implemented to achieve the control objectives, stated in Annex A of ISO 27001 and were implemented as of the report date, is presented in accordance with the criteria set forth in assertion in Section 2. management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with the attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting the fairness of the presentation of the description and the design and implementation of controls supporting the ISMS and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature of controls, controls supporting the ISMS may not prevent, or detect and correct, all errors or omissions relevant to the ISMS. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design of the controls supporting the ISMS is subject to the risk that the ISMS may change or the controls at may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in assertion in Section 2,

a. The description fairly presents the controls supporting the ISMS that were designed and implemented as of July 7, 2016; and

b. The controls supporting the ISMS, as stated in the description, were designed and implemented to achieve the control objectives, stated in Annex A of ISO 27001.
CONTROL REPORTS (SOC 2 TYPE II)

- Same issues apply from certifications and attestations
- But we have CONTROL TEST EVIDENCE!! ....albeit with a false sense of security (bottom up holes still everywhere)
  - Look for exceptions ask for subsequent evidence of the control
  - Nothing on missed patches on critical servers involving SSL, SSH, DNS that provide remote command prompt access or facilitate a DOS attack
  - Nothing on OWASP top 10
  - Etc, etc
- Do check for any CUECs and subservice providers and respond accordingly (watch for hosted data centers and third parties or lack thereof.

- **Recommended new frontier:**
  - Pen test results
  - Vulnerability assessments
  - SSLLabs scan
  - Technical assessment tools (they exist)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Controls specified by</th>
<th>Tests performed</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC2.3 Contd</td>
<td>Changes and updates to system policies and procedures are communicated to entity personnel through email communication and are placed on the intranet to be available to all entity personnel.</td>
<td>Inquired of management to determine whether employees were informed of policy and procedure changes and whether employees were notified through email communications, or through updates on the corporate intranet. Inspected email communication evidence to determine whether updates to policies and procedures were communicated to personnel. Inspected the intranet site to determine whether policies and procedures were available to personnel.</td>
</tr>
</tbody>
</table>

*Results of Testing: No deviations noted.*
QUESTIONNAIRES/GUIDED CONVERSATIONS/REFERENCES

- All the same issues of control reports, attestations, and certifications
- But you may get to talk to a CISO that you should absolutely not trust
- Good place to dive into the coding practices (OWASP top 10)
- Questionnaires have massive overhead, with very little to conclude
- Remember, people always tell the truth in detail, especially when there is no contractual obligation to do so and overhead is high [FALSE]

Plenty of hope, an infinite amount of hope—but not for us.

(Franz Kafka)
Me: How did you get so good at CTF?

Tom Pohl: I'm too stupid to give up.
At what point does the fear of data breach warrant keeping the solution in-house? In VRM there is a sentiment that if you have to go to certain degrees of scrutiny, maybe <>aaS is not your thing.

Really everything is funneled through this (risk management president trumps paranoia):

- Outside of costly technical audits, contracts are your friends
- Mitigate and transfer risk via contracts
- Demand better from vendors especially security vendors by transfer loss exposure to them
Maybe a big VRM program is too costly for your organization. But given the limits of traditional approaches, perhaps your VRM program focuses in on only a few elements that you know will really come back to bite you.
PRO TIPS—PUT VRM CHECKS IN CONTRACTS, GIVE YOURSELF AN OUT

10. SECURITY CONTROLS

10.1 FedRAMP Certification. After the Effective Date, [fill in the date] shall promptly commence and/or continue to undertake good-faith efforts to achieve FedRAMP certification. Such certification shall remain active and in good-standing throughout the term of this Agreement or any applicable SOW or Order Schedule (or as otherwise agreed-upon by the parties). If [fill in the entity not meeting the standard] has not achieved and provided written confirmation to Customer of such certification by November 30, 2017 (the "FedRAMP Deadline"), [fill in the entity not meeting the standard] shall provide Customer a detailed update as to its certification progress, shall make available to Customer, on the FedRAMP Deadline, its most current SOC 2 Type II report (if available), and shall allow a mutually agreed upon, third party auditor to perform a security control audit as set forth in section 10.2.

10.2 Security Control Audit. In the event [fill in the entity not meeting the standard] fails to meet the FedRAMP Deadline, to evaluate its security control environment, [fill in the entity not meeting the standard] shall, within 30 days of the FedRAMP deadline, permit a mutually agreed upon, third party on Customer’s behalf, to immediately perform an assessment, audit, examination or review of all internal security controls and related data in physical and/or technical environment (the “Audit”). [fill in the entity not meeting the standard] shall fully cooperate with the Audit by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, application software and related and reasonably necessary items. In addition, [fill in the entity not meeting the standard] shall complete and return Customer’s vendor security questionnaire, upon which [fill in the entity not meeting the standard] will represent and warrant that it is, and shall remain, in compliance with no less stringent standards than the controls set forth in its responses to the questionnaire throughout the term of the Agreement or any applicable SOW or Order Schedule.

10.3 Other Remedies. If [fill in the entity not meeting the standard] fails to meet the FedRAMP deadline, Customer is not provided or satisfied with [fill in the entity not meeting the standard] SOC 2 Type II report, and Customer is not timely provided access for or satisfied with the results of the Audit, or Customer is not provided, upon request, or satisfied with the results of the security questionnaire, Customer may, at its election, terminate this Agreement and/or any then-current SOWs and/or Order Schedules. In its assessment of [fill in the entity not meeting the standard] control environment, Customer will consider [fill in the entity not meeting the standard] management attestation, coverage period, scope of controls, type and quality of testing, control exceptions and the use of and controls for third (and fourth and beyond) parties to support the Services. If any are found to be deficient, Customer considers this unsatisfactory. Customer’s termination under this subsection shall not entitle it to a refund of used services fees.
PRO TIPS—RAISE THE LIMITATION OF LIABILITY

6.2. **Limitation of Liability** Except as may arise out of a breach of Section 4 (Confidentiality), the total liability of [name] to Customer for any and all claims and damages under this Agreement, whether arising by statute, contract tort or otherwise, will not exceed five times the cumulative amount paid by Customer to [name] under all SOWs or Order Schedules. This Agreement allocates risks between the parties and this section along with the pricing set forth in each SOW or Order Schedule reflects this allocation of risk and the limitation of liability specified herein.
Run a FAIR (Factor Analysis of Information Risk) analysis on the Vendor to quantify the loss exposure risk they pose to the environment in dollars. If they expose you to unreasonable risk, take it off the top.

Use VRM as a negotiation tool.
# AAS RISKS

## Data and Application Lock-in
- Data export and recovery—getting data out of a public cloud and back into your private cloud can be problematic.
- Data portability—compatibility of moving to another cloud solution can be problematic
- Indirect, hardware lock-in—hardware re-purchase if public cloud is migrated back in house can be problematic.

## Governance and Control
- Access, change, operational control considerations and accompanied <your company>’s risk and control matrix may be unmanaged or not considered in assessing vendors.
- Contracts may deny or not consider security assessments/attestations and limitation of liability amounts may not be properly set.
- Third party subservice providers may not be appropriately scrutinized or monitored.
- Regulatory or compliance policies that prohibit public cloud may bypass the procurement process.
- Customer User Entity Controls (CUECs) may not be appropriately applied and monitored by the cloud provider.
<table>
<thead>
<tr>
<th><strong>Reputation</strong></th>
<th>Activities of other tenants may affect &quot;electronic&quot; reputation (email, web filters, etc.) especially if utilizing a shared a subnet.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reputation of the business or cloud provider may suffer and company could be guilty by association.</td>
</tr>
<tr>
<td><strong>Cloud Business Failure or Acquisition</strong></td>
<td>Cloud provider failures, acquisitions, and mergers could come without warning and impact the application.</td>
</tr>
<tr>
<td></td>
<td>With zero warning of a cloud provider failure, controls to prevent data loss may not be appropriately considered.</td>
</tr>
<tr>
<td></td>
<td>Fully mitigating the risk of cloud provider failure means the benefits of a cloud computing model are pointless.</td>
</tr>
<tr>
<td></td>
<td>Mergers and acquisitions can affect business direction and roadmaps.</td>
</tr>
<tr>
<td><strong>Resource Exhaustion by other Tenants</strong></td>
<td>Vendors always oversubscribe and an oversubscribed SaaS offering can impact the quality of service to organizations.</td>
</tr>
<tr>
<td><strong>Isolation failure (VM or Network Escape)</strong></td>
<td>Configuration errors could lead to a situation of a VM or network escape.</td>
</tr>
<tr>
<td></td>
<td>Vendor mitigation of configuration errors may not be done timely because patching cost money and may cause downtime and downtown could cost the cloud providers money in unmet SLA dollars.</td>
</tr>
<tr>
<td></td>
<td>“Follow the money” — in general, what cost cloud providers money is often not done.</td>
</tr>
</tbody>
</table>
| **Malicious Insider** | Increased risk of malicious insider involvement in SaaS because of direct access to data at rest and transit plus the added benefit of anonymity.  
Malicious insider mitigation in contract of little help.  
Compromise may be undetected. |
|---|---|
| **Management Interface Compromise** | A common cloud management interface equates to an attack surface for an entire cloud.  
Poor code could lead to compromise.  
Poor updates could lead to compromise. |
| **Interception of Data in Transit** | Higher risk of interception of data in transit.  
Even with proper PKI people still click through cert warnings and other indicators of compromise.  
Migrating internal crypto technologies and process to external providers may not be possible.  
Sound key management is always critical and may not be performed. |
| **Deletion of Data** | Deleting data via a VM releases unzeroed sectors back into the pool.  
**Forensic recovery of that data is possible by other cloud tenants.**  
Disk wiping no longer under company control.  
Proper disposal cost money and may not happen by the cloud provider. |
<p>| Denial of Service | Denial of service could happen directly via cloud credential theft. |
| - | Denial of service could happen indirectly via co-tenant activity. |
| - | Cloud provider may not offer DDOS protection. |
| Economic Denial of Service | Attackers could target bandwidth constraints by the cloud provider. |
| - | Attackers could target payments per transaction by creating dummy transactions. |
| Encryption | Encryption may be weak. (Block or stream ciphers including modes need to be determined. Does the solution use libraries with known cryptographic vulnerabilities?) |
| - | Encryption may be broken. (Is it end to end? Protected against Chosen Plaintext Attacks or Chosen Ciphertext Attacks?) |
| - | Encryption may be downgraded. |
| Loss of Keys or Credentials (Key Management) | Loss of secret keys, TLS encryption or a compromise of credential database could lead to compromise. |
| - | Access to the key may be compromised. |
| - | Keys may be mismanaged or not rotated. |
| Larger Attack Surface | Public clouds are just bigger targets. |
| - | Public cloud should have a larger security program to account for economies of scale. |
| Conflicts in / over Hardening Procedures | Roles and responsibilities must be spelled out over who hardens the host. |
| - | Maintenance windows may not be established. |</p>
<table>
<thead>
<tr>
<th>Subpoena / Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process for handling subpoenas may not be defined.</td>
</tr>
<tr>
<td>Process for handling subpoenas of a co-tenant may not be defined.</td>
</tr>
<tr>
<td><strong>Process for handling seizures of a co-tenants hardware may not be defined.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Protection Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup media may be lost or stolen.</td>
</tr>
<tr>
<td>Data retention policy differences may occur.</td>
</tr>
<tr>
<td>Cloud provider may find itself hosting data illegally collected by customer or a transfer of data to a federated cloud could contravene legislation in the jurisdiction of the source or target cloud.</td>
</tr>
<tr>
<td>Data at rest may not be protected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Licensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ownership of the application and OS licenses may not be defined.</td>
</tr>
<tr>
<td>Tracks usage and methods for tracking may not be defined.</td>
</tr>
<tr>
<td>Licensing in general may be poorly defined and tracked.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>API Security Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and authorization mechanisms may be weak, basic, or too open per business requirements. May not utilize tokens.</td>
</tr>
<tr>
<td>Encryption keys may not be used as an access and authentication mechanism to call an API and may be not stored securely or be hardcoded.</td>
</tr>
<tr>
<td>Federation may not be used so that trust relationships cannot be revoked if necessary.</td>
</tr>
<tr>
<td>Principle of least privilege and least functions are not defined or adhered to.</td>
</tr>
<tr>
<td>Poorly written or implemented APIs.</td>
</tr>
</tbody>
</table>