DATUMSEC

Vendors as a Vector

November 16, 2016

Harry Wan - Bio

- Symantec
- Arbor Network
- Datum Security
- CISSP since 2003
- 3rd place ISSA-LA Summit 2015 - Capture the flag

Vendor as a Vector - Agenda

- Recent Vendor / 3rd Party Breaches
- Deep Dive & Observations
- Conventional advice
- Implementing Internal vs External Controls
- Policy / Audit Example
- Additional Consideration

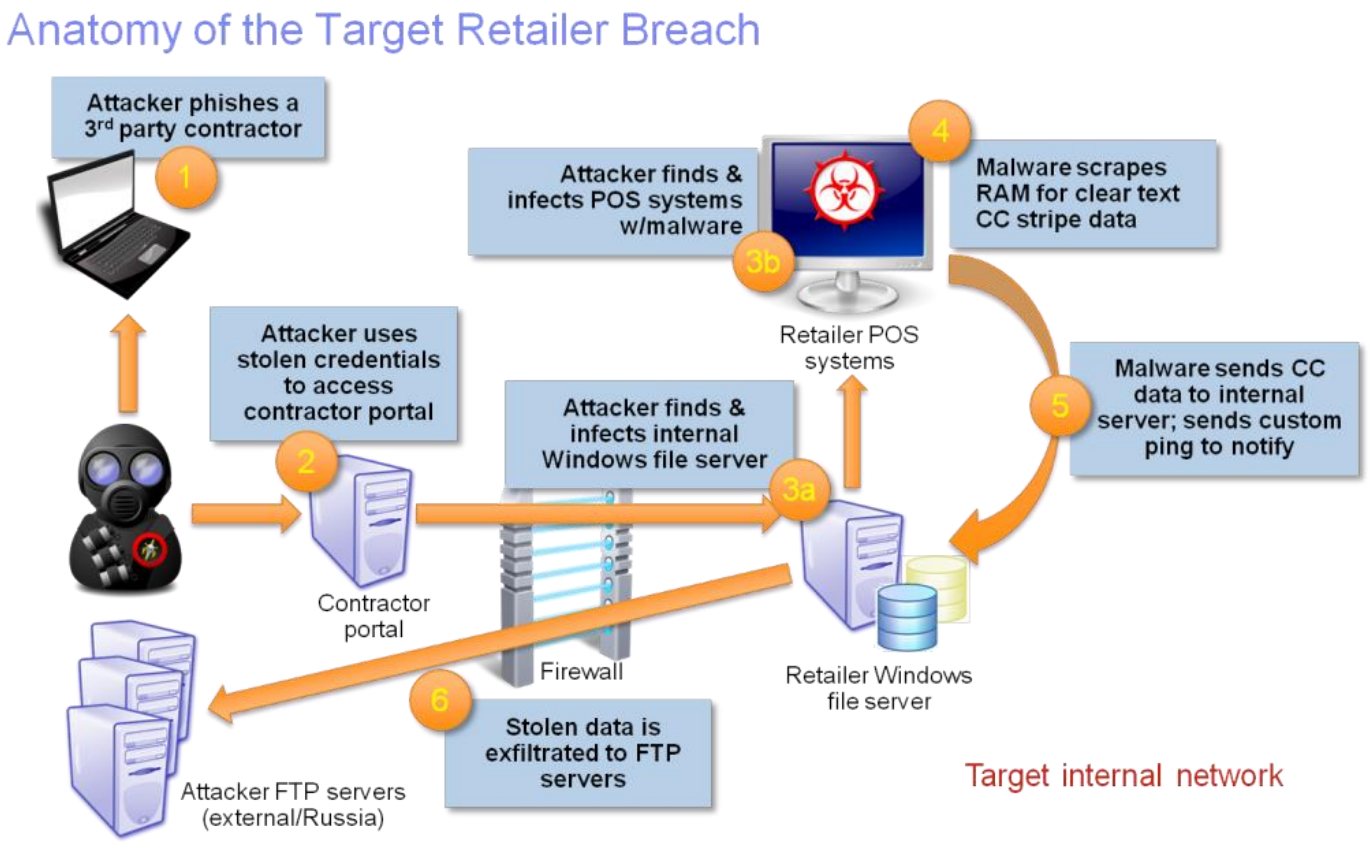
Recent Vendor / 3rd Party Breaches

First Party	Vendor	Loss	Cause	Source
U.S Bancorp	ADP(!)	Identity info for US Bancorp employees	Publicly avail info to create account	Krebs
Vincent Vein Center	Bizmatic (PronoCIS)	name, addr, SSN, DOB	Credential theft to install malware in Bizmatic	Healthcare Infomatics
Wendy POS	unnamed	POS info at 300 stores	Malware installed though use of compromised third party credentials	Kaspersky/Krebs
Multicolor (labels)	unnamed East Coast law firm	HR info of all firm employees	Law firm lost hard drive due to theft	scmagazine
California State University	We End Violence	Personal info of 79,000 students	Web site hack of "We End Violence"	sbsun (The Sun Education)
several wineries	Missing Link / eCellar	Customer names, credit card and other info. Unspecified number	"breach of web platform"	csoonline

Recent Vendor / 3rd Party Breaches

First Party	Vendor	Loss	Cause	Source
Home Depot	unnamed	56 million credit and debit card numbers	vendor logon credentials -> zero day lateral to corp then memory scrap	sans (and others)
Office of Personnel Management	KeyPoint Government Solutions	4.2 million employees info	Stolen credentials -> multiple internal pivots via "PlugX" malware	wired (and others)
Target	Fazio Mechanical	financial info on 100 million people and 11GB of data	3rd party contractor, pivot to windows file server, pivot to ram scarp POS then exfiltrate	security-intelligence (and others)

Target Retailer Breach Anatomy

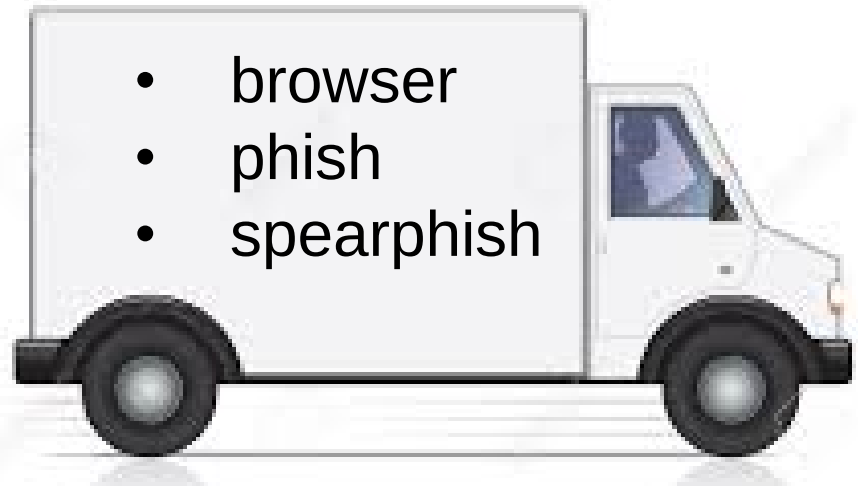


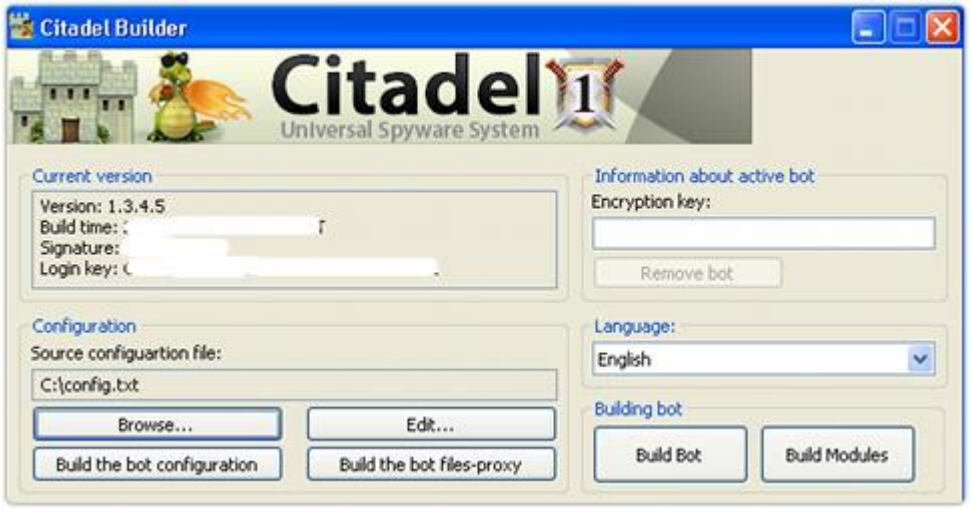
1. Citadel Malware infects Fazio
2. Target Partner or Property portal - likely unpatched vulnerability
3. Pivot via AD credentials
4. Compromise internal Windows File Server
5. Install memory scrapper on POS system

image credit - http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/#.VMA24UfF-So

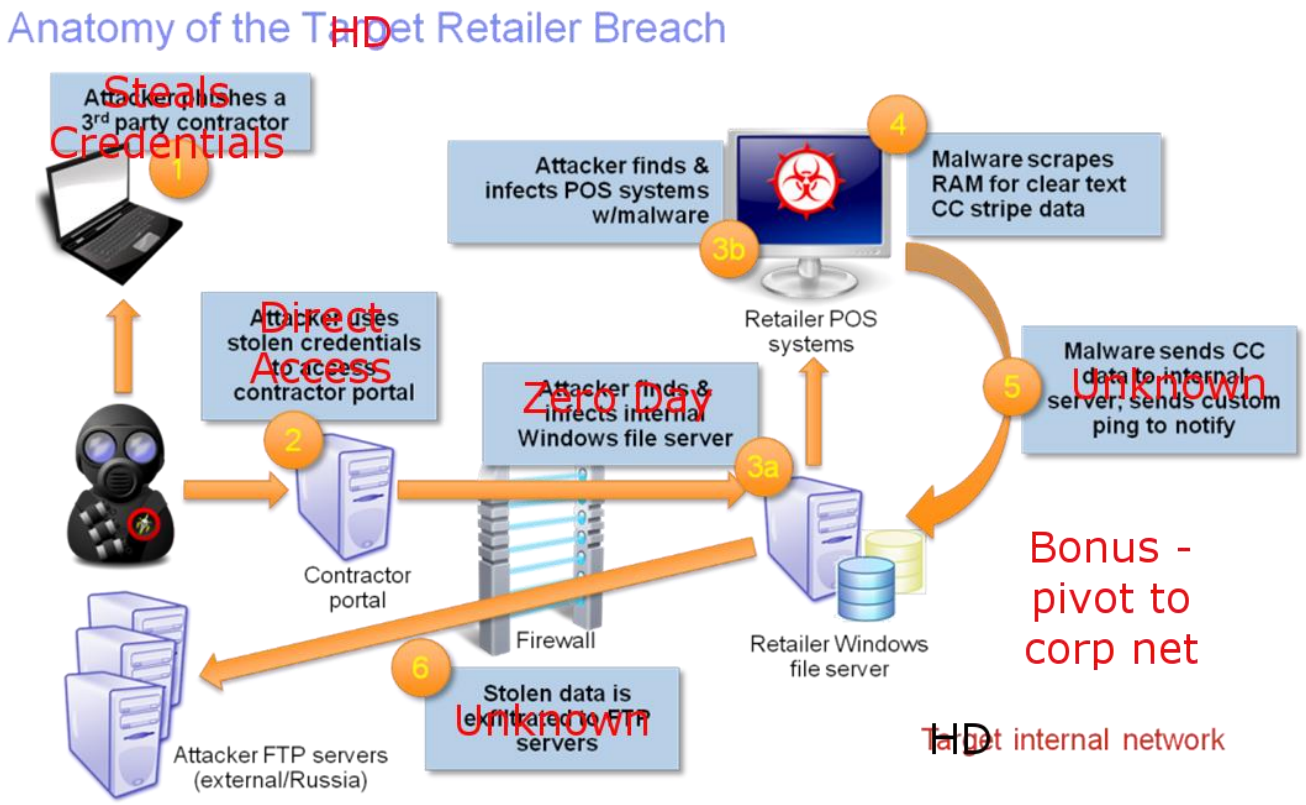
Malware - exploit vs payload

- Citadel
- Improvement on Zeus
- Mostly used to steal banking credentials
- Easily detected by all top up-to-date anti-virus products
- Target opportunistically targeted via Fazio?





~~Target~~ HD Retailer Breach Anatomy



1. Unnamed vendor logon credentials
2. Zero day windows to pivot to corporate
3. Install memory scrapper on POS system and steal 53 million emails

image credit - http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/#.VMA24UfF-So

Observations

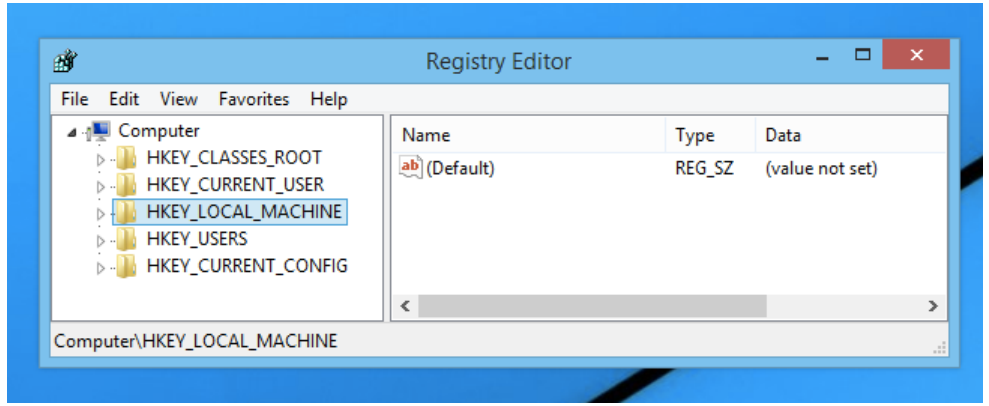
- Some vendor breaches results in direct loss
- For large attacks
  - Multiple defense layers failed
  - Smaller vendor is easy first vector
- Although HD zero-day, many attacks expose lack of basic controls

Conventional, boring, advice

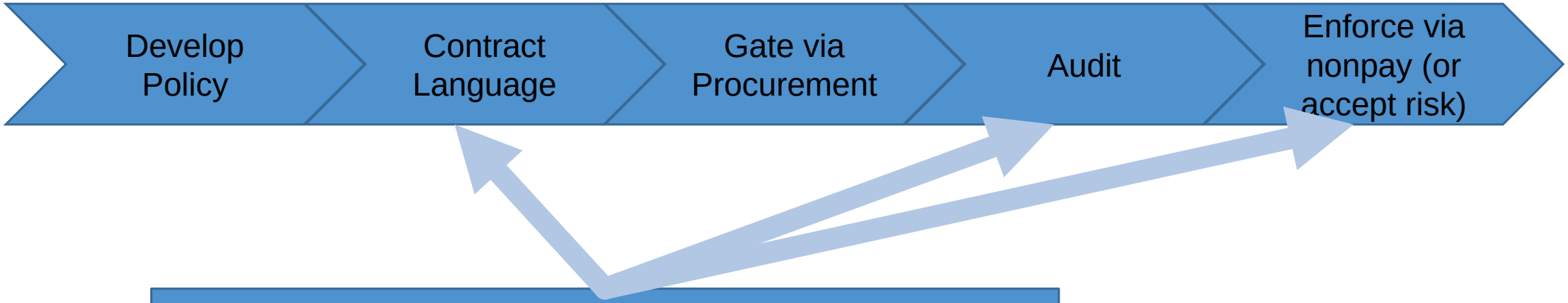
- Determine data important to corporation
- Develop security requirements (policy and controls) appropriate for each level of data importance
- Identify vendors handling each level of data
- Implement
- Win

Internal Controls

- Complexity here
- Mostly IT project
- Technical in nature



External Control



- Complexity here
- Involve General Counsel
- Need business to help determine data criticality

Vendor Security Requirement Example

6. Supplier Security Measures
   i. Information Security Policies
      Supplier will establish and maintain information security policies and controls for the facilities, network, and systems at each Service Location that support the delivery of the Secure Services.
   ii. Physical Security:
   iii. Access Controls:
   iv. Firewalls:
   v. Communicatio

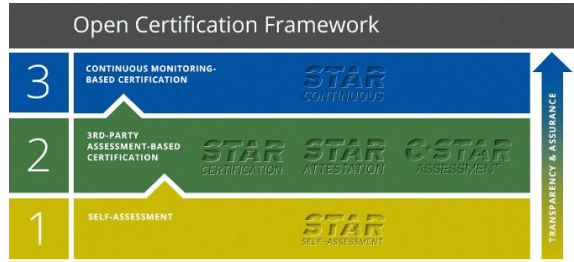
http://supplier.kp.org/formsreqs/Data_Security_Requirements.pdf

Certification / Audit best practice

Independent Certifications. If available, Supplier will provide Kaiser, on an ongoing basis each year, with copies of all independent, third-party certifications (each an "***Independent Certification***") of Supplier's applicable data security controls (e.g.; **SSAE16, ISO, SOC 1, SOC 2,** etc.) that address all or a portion of the subject matter of these Data Security Requirements (e.g., information security, internal controls, privacy). If Kaiser determines that one or more Independent Certifications provide an adequate assessment of the Supplier Security Measures, Kaiser may accept such **Independent Certifications in lieu** of all or a portion of the **Security Assessment** described in Section 7 above.

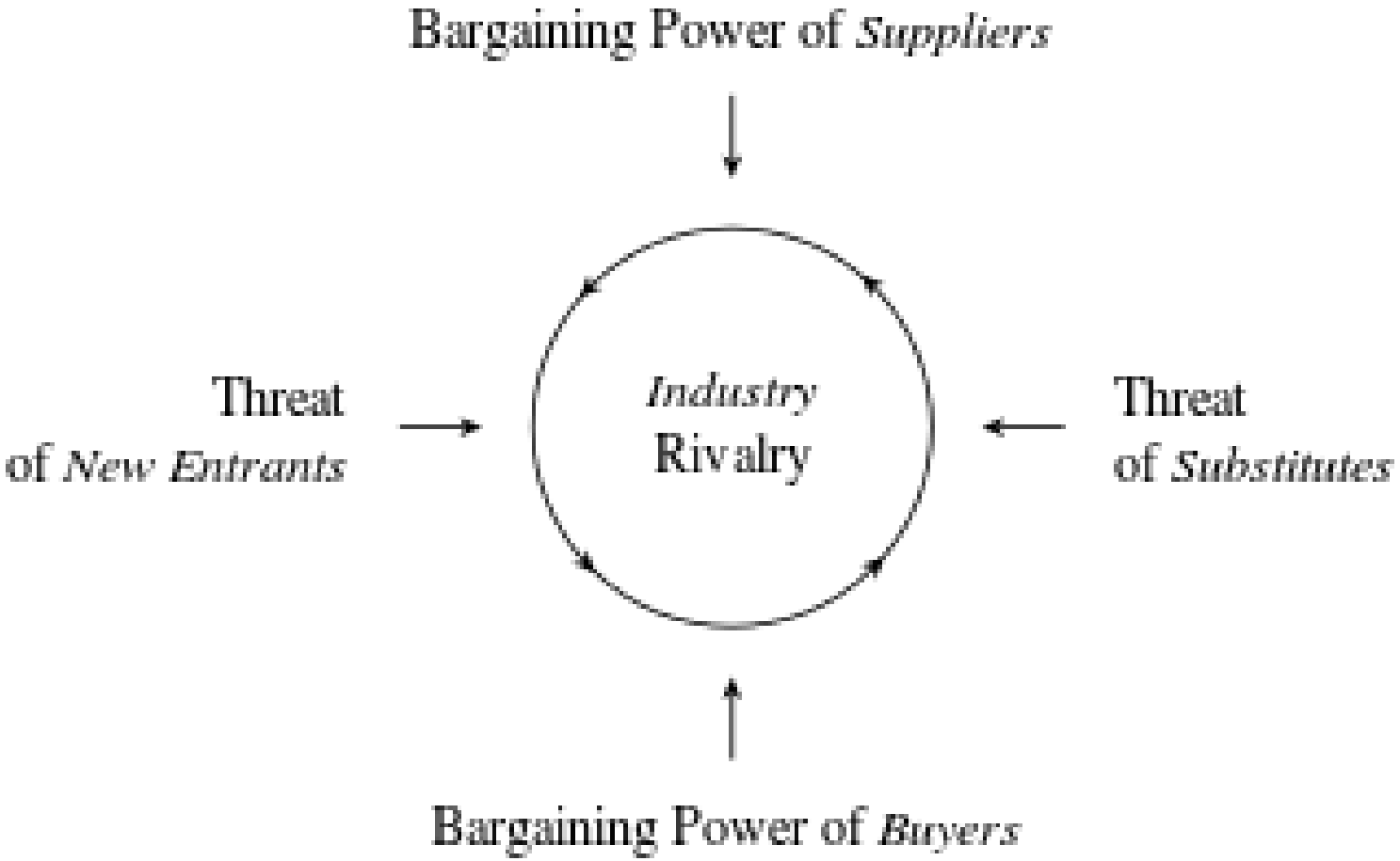
http://supplier.kp.org/formsreqs/Data_Security_Requirements.pdf

cloud security alliance®



DATUMSEC

Consideration - Michael Porter?



A "unnecessarily" expensive vendor program will have the unintended consequence of increasing the bargaining power of supplies

Conclusion

- Vendor breach causes direct loss
- Vendor breach is a vector of attack to larger targets
- Vendors attacked indiscriminately and continually
- Successful vendor program involve
  - Business input
  - Good contract language
  - Audit and Enforcement points
- A right sized vendor program balances cyber risk reduction with business competitiveness

Appendix - ISO27001

ISO/IEC 27001 - Information security management

The ISO 27000 family of standards helps organizations keep information assets secure.

Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

Appendix - SOC 2

The Service Organization Control **(SOC) 2** Report will be performed in accordance with AT 101 and based upon the Trust Services Principles, with the ability to test and report on the design (Type I) and operating (Type II) effectiveness of a service organization's controls (just like SOC 1 / SSAE 16). The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to SOC 1/SSAE 16 which is focused on the financial reporting controls.

Trust Service Principles

Security: The system is protected, both logically and physically, against unauthorized access.

Availability: The system is available for operation and use as committed or agreed to.

Processing Integrity: System processing is complete, accurate, timely, and authorized.

Confidentiality: Information that is designated "confidential" is protected as committed or agreed.

Privacy: Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with the privacy principles put forth by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

Appendix - CSA Star

STAR Self Assessment

About CSA STAR Self-Assessment

CSA STAR Self-Assessment is free and open to all cloud providers and allows them to submit self-assessment reports that document compliance to CSA-published best practices.

Cloud providers can submit two different types of reports to indicate their compliance with CSA best practices:

The Consensus Assessments Initiative Questionnaire (CAIQ), which provides industry-accepted ways to document what security controls exist in IaaS, PaaS and SaaS offerings. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. Providers may opt to submit a completed Consensus Assessments Initiative Questionnaire.

The Cloud Controls Matrix (CCM), which provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. Providers may choose to submit a report documenting compliance with Cloud Controls Matrix.