Security as a Service (SecaaS)

John R. Robles CISA, CISM, CRISC
www.johnrrobles.com
jrobles@coqui.net
787-647-3961

Introduction

- What is Security as a Service (SecaaS)?
  - Security as a Service is a cloud computing model that
    - Delivers **Managed Security Services** over the Internet.

Cloud Characteristics of SecaaS

- **SecaaS, is a Cloud Service.** It is available:
  - On-demand, and
  - Over the Network.
- SecaaS-provider **resources are pooled** in order to be made available to many customers at the same time.
- SecaaS availability is provided **elastically**
  - Need more?, SecaaS provides more
  - Need less?, SecaaS provides less
- **SecaaS is provided as a measured Service**
  - Use more, Pay more
  - Use less, Pay less
- **The Cloud Provider**
  - Provides the Cloud Services

What Information Security Services Does SecaaS Provide?

- According to Cloud Security Alliance (CSA) SecaaS services include:
  - Identity and Access Management (IAM)
  - Data Loss Prevention
  - Web Security
  - Email Security
  - Security Assessments
  - Intrusion Management
  - Security Information and Event Management (SIEM)
  - Encryption
  - Business Continuity and Disaster Recovery
  - Network Security

Impact of SecaaS on the Enterprise

- Information Security is a **critical function** in today's computer environments (in private enterprises, as well as, government, and NGOs-Non Government Organizations).
- Information Security is complex.
- Not having adequate & appropriate security can be devastating to organizations
  - Loss of organizational money
  - Loss of organizational credibility
  - Loss of critical information to competitors and national enemies
  - Loss of personal identity and the abuse of stolen identities
  - Loss of compliance with government regulations and contractual obligations

Impact of SecaaS on the Enterprise

- When using SecaaS, organizations should constantly ask their Cloud Security Service Provider:
  - Who is responsible for securing what?
  - Who has access to what data?
  - Where are important security data (audit logs, user credentials, etc.) stored and can they be accessed when needed?
  - What are the destruction and archival procedures?
  - What legal and jurisdictional issues do cross-border SecaaS offerings raise?
  - What new data privacy and access management issues are raised by SecaaS?
  - As SecaaS grows in popularity will more regulations be created to deal specifically with some of these potential issues?
- An organization can outsource Security Responsibility but not Security Accountability

Organizational Benefits of SecaaS

- Organizational Benefits of SecaaS include:
  - Cost
  - Ease of management and operations
    - Provider is responsible
  - Focus on core competencies
    - No log management
    - Eliminate or reduce Help Desk calls
  - Scalability
  - Fast provisioning
  - Best of breed
  - Expertise
    - Access to specialized security expertise
  - Continuous updates
  - Cost–effective compliance

What are the Risks of Using SecaaS?

- Service Model
  - SaaS: the organization pushes almost all security concerns to the Cloud
  - PaaS: the organizations have some control over the security pushed to the Cloud
  - IaaS: the organizations has even greater control over security pushed to the Cloud
- Confidential Data
  - Data Classification: High Risk, Medium Risk, Low Risk
  - Ensure security is appropriate for the classified data
- Data Protection
  - Is SecaaS security in line with organizational requirements?
  - Is access granted based on least privilege?
  - Are there country-specific regulations that restrict locations for transfer, processing, or storage of data?

What are the Risks of Using SecaaS?

- Contract
  - High risk! Must be strictly scrutinized.
  - Contracted security services, settings and options must meet organization's needs and regulator compliance.
  - The enterprise is ultimately responsible for the security of its assets
- Gaps
  - High risk! How to determine that contracted security services, settings and options are provided as contracted (Gaps).
  - Must get attestations via SSAE-16, ISAE 3402, ISO 27001, or PCI DSS reviews.
  - Identified gaps must be managed as risks.

Strategies for Addressing SecaaS Risk

- Risk Management Strategies
  - **Acceptance**
    - Accept rather than mitigate because of high implementation costs
  - **Mitigation**
    - Establish physical, administrative and/or technical controls or systems the potential for problems
  - **Avoidance**
    - Make changes to avoid the risk
  - **Transfer**
    - Transfer the risk to another party
      - Buy insurance to cover consequences of risk occurrence.
  - **Governance and Risk Management**
    - Constantly Detect, Manage, and Review Risk
    - Establish Risk appetite

Governance

- COBIT 5 from ISACA
  - Provides a comprehensive framework
  - Assists organizations in achieving their objectives in using SecaaS
- Governance considerations for SecaaS
  - For whom are the benefits?
  - Who bears the Risk?
  - What resources are required?
- Management:
  - Knows & understands the benefits of SecaaS
  - Evaluates and monitors benefits realization
  - Understands cloud computing risk
  - Can quickly respond to changing risks
  - Seeks periodic assurance to ensure SecaaS effectiveness
  - Has established acquisition, deployment and operations roles and responsibilities

Assurance Consideration for SecaaS

- Ensure that the SecaaS provided by the Cloud Service Provider has:
  - **Availability**
    - 24/7 operations must have 24/7 security
  - **Privacy**
    - Ensure that provider has effective controls to ensure privacy of data
  - **Data security**
    - Security Information and Event Management
    - Protect CIA (Confidentiality, Integrity, and Availability) of information.
  - **Location**
    - Locations requirements for jurisdiction and legal obligations that must be ensured.
  - **Compliance**
    - Ensure provider complies with all relevant information security laws and regulations

Assurance Consideration for SecaaS

- Monitoring Controls
  - Appropriate use of SLAs to monitor and assess performance
- Reporting Controls
  - Independent security reviews or certification reports issued by 3rd parties
- Compensatory Controls
  - Implement if
    - If Gaps arise
    - New risks are introduced
  - Governance Controls
  - Physical Controls
  - Logical Controls

Conclusion

- SecaaS may be an appropriate IT Solution
  - Increase security while reducing costs and resources
- The organization is always responsible for information security assurance
- Use Cobit 5 as a assurance framework to test controls that protect information assets
- Maintain partnership with SecaaS provider
  - Transparency of security controls

Questions?

- And Answers!

John R. Robles CISA, CISM, CRISC
www.johnrrobles.com
jrobles@coqui.net
787-647-3961