Cloud Security Toolkit

Top 10 Cloud Security Concerns Introduction and Overview

Introduction

This component of the HIMSS Cloud Security Toolkit provides a set of questions to ask cloud service providers about the information security aspects of their cloud service offerings. The questions are intended for evaluating cloud services as a business strategy and for evaluating cloud service providers during the early stages of an acquisition process. The questions should allow an organization to understand how using a cloud service provider affects security risk posture, providing a more secure or less secure solution, and help an organization understand the relationships between security risks and business benefits.

The questions are divided into ten areas of security concern, based closely on the Open Web Application Security Project's (OWASP) Cloud Top 10 Security Risks. While there are no right or wrong answers to the questions, a cloud service provider's responses to the questions should inform an organization's discussions internally and with cloud service vendors, and they should allow an organization to gauge the comparative suitability of cloud providers for particular business problems.

What constitutes an "acceptable" answer to a question depends on an organization's specific use cases for cloud services. In some cases, there may be a lower "bar" for what constitutes an acceptable answer. For example, cloud services providing online learning material for ICD10 transition will probably have different security consideration than cloud services providing electronic medical records.

A healthcare organization may choose to use all of the questions in the list or select a subset of questions for its use. Questions may be modified or augmented for specific situations as needed.

The questions are not intended to replace industry standard control sets for healthcare information technology operations and cloud providers, such as the Health Information Trust Alliance's (HITRUST's) Common Security Framework (CSF) and the Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM).

This component of the toolkit is primarily oriented towards public cloud, software-as-a-service solutions, although many of the concepts and questions are applicable to community clouds, hybrid clouds, private clouds, and infrastructure-as-a-service and platform-as-a-service solutions.

Overview of the Top 10 Security Concerns

1. Data Ownership and Protection

The traditional approach to business software applications is to run the software applications in-house on an infrastructure built and maintained by the organization using the applications. Therefore, all data resides within the organization and the organization has complete control over the data and how it is protected. Larger organizations typically have data centers where network equipment, servers, and data storage is centrally managed and secured. Smaller organizations may have all of their servers and data storage within their offices.

When an organization uses the cloud, the data resides on the cloud provider's resources, where the organization has no direct control over the data. This creates critical security risks an organization must carefully understand and mitigate. At the same time, it creates the potential for security benefits an organization should endeavor to identify and understand.

An organization using cloud services must consider where its data is geographically located, how reliably the data will be available when it is needed, how the data is backed up and protected from loss or destruction or fabrication, how the data is kept private, and how the data can be recovered or moved to another system if the contract with cloud provider is terminated, the cloud provider goes out of business, or the cloud provider gets acquired by another company.

An organization using cloud services must understand to what extent the cloud provider's personnel have access to the organization's data. Some cloud providers may offer cloud-enabled business services to their customers in addition to software applications. When an organization uses these cloud-enabled services, the organization is outsourcing business processes to the cloud provider and the cloud provider therefore requires access to the organization's data to perform these services. In this case, the cloud provider may be considered a HIPAA Business Associate, which has regulatory and contract implications.

2. User Identity Management and Federation

Organizations must understand how cloud providers identify users and manage user accounts for accessing data in the cloud. If the cloud provider requires the organization to use the cloud provider's logon accounts (usernames and passwords), then user satisfaction and productivity may be diminished. Users would be forced to remember another username and password and explicitly login to the cloud provider's system.

Organizations must understand the risks associated with logon accounts and how the cloud provider mitigates these risks. These risks include password guessing, password theft, password reset, hijacking of user login sessions, and revocation of access. Revocation of access must be understood in terms of how quickly access to the cloud provider's system will be removed when the organization terminates an employee. When there is a separate “island” of usernames and passwords within a cloud service provider, there is a higher risk that a terminated employee could improperly retain access to the cloud.

As an alternative to creating a separate island of usernames and passwords, some cloud providers may offer integration with an organization's in-house authentication systems. Through integration, existing in-house logon accounts managed by the organization can be used to access data in the cloud. Typically, this integration is achieved through Lightweight Directory Access Protocol (LDAP) mechanisms or using single-sign (SSO) technologies such as the Security Assertion Markup Language (SAML). While integration provides a substantially better user experience and avoids many of the risks associated with separate islands of credentials, integration approaches carry risks as well. These risks and the associated mitigations need to be understood carefully. Integration risks include, for example, exposing organization's authentication systems and spoofing of SSO assertions using stolen private keys.

A final consideration is how the organization's user identities are mapped to cloud provider user identities. The organization may identify users with one particular username convention while a cloud service provider may use a different convention. An organization needs to understand the mapping between the two conventions to ensure accountability for audit and investigation purposes.

3. Regulatory Compliance

Organizations using cloud providers face different challenges with respect to regulatory compliance for data stored in the cloud. Organizations must consider whether data entrusted to a cloud provider carries legal/regulatory protection and breach notification requirements, such as protected health information (PHI) governed by HIPAA and HITECH, personally-identifiable information (PII) governed by state privacy laws, and payment card information regulated by the Payment Card Industry's (PCI's) Data Security Standard (DSS).

Even though protected information may be entrusted to a cloud provider, the organization utilizing the services of the cloud provider retains the ultimate responsibility for compliance with applicable laws and regulations. The organization's compliance responsibility encompasses its own internal business operations as well as ensuring compliant operations within the cloud service provider. For PHI, depending on the nature of the services offered by the cloud provider, the cloud provider may be considered a covered entity and/or a business associate. A cloud provider which is a covered entity should be able to offer evidence of compliance with HIPAA security and privacy rules. A cloud provider that is a business associate should be willing to put in place a business associate agreement with its customer, and is also covered by HIPAA.

Cloud providers may need to comply with HIPAA minimum necessary use and de-identification requirements. Cloud providers that are public companies have to comply with the Sarbanes-Oxley Act of 2002 (SOX) and can be expected to have at least a Statement on Standards for Attestation Engagements No. 16/ Service Organization Control 1 (SSAE 16/SOC 1) report prepared by a third-party auditor. Organizations using a cloud provider must consider the possibility that a cloud provider may make changes to the cloud provider's underlying technology infrastructure or business operations which may affect the organization's compliance status. Organizations should ensure that compliance expectations are defined in contracts/service agreements with their cloud providers. The end result is that an organization must perform essentially the same security due diligence for cloud-based solutions as for non-cloud solutions.

4. Business Continuity and Resiliency

Business continuity and resiliency refer to the ability of an organization to conduct business operations in adverse situations. Adverse situations include disruptions not only to information technology infrastructure, but also any disruptions affecting the ability of the cloud service provider to deliver its services at defined service levels, including, for example, the loss of key personnel or the loss of access to business offices.

When an organization uses a cloud provider, the organization cedes control of business continuity planning for the data and services entrusted to the cloud provider. As a result, the organization must consider carefully the ability of the cloud provider to provide continuity of services when adverse situations affect the cloud provider. Cloud providers may rely on other cloud/infrastructure providers for critical business operations, so this consideration must extend to the cloud provider's service providers.

While it is impossible to provide business continuity for all conceivable situations, organizations considering cloud providers should understand the types of adverse situations for which the cloud provider has planned. The cloud provider should have a business continuity plan describing the scope of the cloud provider's business continuity capabilities, its procedures for handling adverse situations, and the extent of regular testing performed to ensure restoration of service.

Organizations must also consider the quality of service received from a cloud provider in an adverse situation. A degraded service level may pose risks such as longer response times for access to data or services. Service agreements with cloud providers should specify recovery objectives for business functions. These recovery objectives should be based on the time sensitivity of business functions to loss of service.

5. User Privacy and Secondary Uses of Data

For the purposes of this toolkit, there are two broad categories of users for which privacy and secondary uses of data are a concern: users of the cloud service provider's system, who are typically employees of the healthcare organization, and users who have information stored about them in the cloud provider's system, who are typically patients of the healthcare provider and who themselves may access the cloud provider's system.

Organizations considering the use of cloud services must understand how a cloud provider protects and uses information about both types of users. Organizations should consider to what extent a cloud provider can disclose information about its employees, its customers, or its business. This information includes specific information or aggregate statistics. It includes information collected from an individual's use of the cloud provider's information systems, such as characteristics of user behavior (such as links clicked, options selected) and productivity measurements.

Secondary uses of data refer to uses of information collected by a cloud provider about a cloud subscriber for purposes other than the provision of services to the cloud subscriber. The concern with secondary uses of data is the sale or disclosure of the information to third parties for the benefit of the cloud provider, such as for marketing purposes. However, there may be secondary uses of data which deliver value to cloud subscribers through a "network effect" whereby the sharing of information allows improved operational efficiencies, for example the elimination of the need for manual paper-based intake and reduced faxing of clinical data.

Information about patients is governed by the HIPAA Privacy Rule, but organizations should consider to what extent a cloud provider may disclose PHI to third parties or use information about an organization's patients for purposes other than the provision of services to the cloud subscriber.

6. Service and Data Integration

Organizations must understand how their users will access the data and services of a cloud provider. Typically this access will be over the Internet or a virtual private network (VPN) using a web browser or a software application downloaded from the cloud provider. If the organization will be interfacing any of its systems with the cloud providers systems, for example to implement "back-end" or batch processing of Health Level 7 (HL7) or Electronic Data Interchange (EDI) transactions, the organization must understand the technical aspects of how the interface will work. In both cases (user access and system interfaces), organizations must understand the risks associated with electronic communication across the Internet or wide area networks (WANs), including interception of data in transit, falsification or corruption of data, and verification of client and server endpoints.

Many of these risks are mitigated by the proper use of standard encrypted communication technologies for wide area networks, such as https web sites with strong Secure Sockets Layer / Transport Layer Security (SSL/TLS) ciphers, Internet Security Protocol (IPSec) Virtual Private Networks (VPNs) and SSL VPNs, and properly implemented Public Key Infrastructure (PKI). For safe harbor from breach notification requirements under the HITECH Interim Final Rule, encryption for data in transit must comply with NIST

800-52 “Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations”, NIST 800-77 “Guide to IPSec VPNs”, NIST 800-113 “Guide to SSL VPNs”, or the Federal Information Processing Standards Publication Series (FIPS) 140-2.

Organizations must be sure to consider all possible avenues of data exchange with cloud providers. Email and instant messaging, for example, may not be encrypted by default and extra steps may be necessary to bring such avenues of electronic communication up to par with protection requirements for data in transit.

7. Multi-tenancy

In a cloud computing environment, multi-tenancy refers to the sharing of information technology infrastructure among multiple clients (different customers of a single cloud service provider). This infrastructure includes telecommunications circuits, network equipment, servers, storage, and application software. Multi-tenancy allows cloud providers to achieve economies of scale which would be impossible for an individual organization to attain, allowing organizations to obtain higher levels of service at lower costs.

Risks with multi-tenancy include one client accessing the data of another client, unintentional mixing of one client’s data with another client’s data, one client affecting the quality of service provided to another client, and cloud provider application software upgrades affecting client business operations. While cloud providers can be expected to have adequately mitigated these risks given that multi-tenancy is core to the cloud business model, an organization should understand how the cloud provider achieves isolation between clients. Isolation approaches include use of virtualization technologies such as virtual machines, application-level isolation through processes, threads, or application-managed contexts, and database-level isolation through the use of separate database instances, tablespaces, or record identifiers.

8. Incident Response and Forensic Analysis

Incident response and forensic analysis refer to activities conducted by an organization when there is a security incident requiring immediate response and subsequent investigation. These incidents include malicious acts or mistakes by the organization’s employees or former employees resulting in data breaches. When an organization uses a cloud provider, it does not have access to the underlying log files and other low-level system-level information typically used for forensic examination.

The risk to the organization is that the data necessary to respond to an incident and construct a detailed timeline of a user’s activities may not be available when it is needed, or the organization may require time-consuming and expensive manual assistance from a cloud provider. An organization should understand the types of possible security incidents within their organization which may involve the cloud provider and understand what the cloud provider offers to help the organization respond to such incidents, such as user activity reports, log files, and audit trails.

In addition to understanding their capabilities for reconstructing user activity, organizations must also understand their capabilities for reconstructing a history of specific data records. For example, it may be important to be able to see the history of accesses and modifications for a specific patient’s medical records. Identity management and multi-tenancy create challenges for forensics because users may be identified in the cloud provider’s system differently than the organization’s systems, and sharing of infrastructure at the cloud provider may make it difficult to separate activity of one cloud subscriber from another. Organizations must carefully evaluate the tools available from the cloud provider for conducting investigations as security incidents may require the prompt collection of evidence for possible civil or criminal proceedings.

9. Infrastructure and Application Security

When an organization uses a cloud service provider, it trusts the cloud service provider to properly secure its applications and infrastructure. Securing applications and infrastructure is a highly complex activity requiring an extensive array of personnel with advanced technical skill sets and threat knowledge.

An organization using the cloud must carefully understand the risk that a cloud service provider is not adequately securing its infrastructure and applications. At the same time, an organization should consider to what extent the cloud provider offers enhanced security through economies of scale with dedicated security personnel which could be difficult for an organization to staff on its own. The amount of risk that can be tolerated, and the potential security benefit of using a cloud provider, depends on the sensitivity of the data and services located within the cloud provider.

A cloud provider should follow industry best practices for information security, including configuring and hardening computer systems and networks, secure infrastructure architecture and design, and access control. A cloud provider should be using standard control sets to guide hardening activities and evaluate security posture, such as the HITRUST Common Security Framework (CSF) , the Cloud Security Alliance's (CSA's) Common Control Matrix (CCM), the Center for Internet Security's (CIS's) benchmarks, and the National Security Agency's (NSA's) configuration guides.

For web-based applications, the Open Web Application Security Project (OWASP) publishes a list of the Top 10 web application vulnerabilities. Cloud service providers offering access through web applications should eliminate these vulnerabilities through the architecture and design of their applications and through their software development lifecycle process, including quality assurance checks to ensure web applications are not vulnerable to attacks.

Cloud providers should employ third party experts to audit the security of their infrastructure and applications. These audits may include formal reviews of security and privacy controls (such as SOC 2) and third party penetration testing of infrastructure and applications. The National Institute of Standards and Technology's (NIST's) HIPAA Security Rule Toolkit may provide valuable guidance for HIPAA security audits.

Cloud providers should also have a vulnerability and risk management programs in place, based on established frameworks such as the NIST Risk Management Framework and International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) (ISO/IEC) 27001.

10. Non-production Environment Exposure

A cloud provider typically operates multiple environments where cloud data and services exist. These environments include what is normally referred to as a "production" environment, which is where cloud subscribers have the primary copy of their data and where they conduct their business operations.

Cloud providers also typically operate other environments for purposes such as software development, testing, training, and demonstrations to potential customers. These other environments may be populated with copies of data from the production environment. In other words, an organization's data may be copied into several places to support the necessary business operations of the cloud provider. The data contained in these copies may or may not be de-identified, a process whereby individual patient information is rendered untraceable to a specific patient and individual business information is made untraceable to an organization.

Risks with these non-production copies of data include non-production environments not being as secure as production environments, with lower standards for hardening and with accessibility to the data by larger numbers of people. While integrity and availability may not be a concern in these non-production environments, if the data is protected by HIPAA or state privacy laws, confidentiality may be a concern as well as having an audit trail of access. To the extent required by the nature of the data, a cloud provider must properly protect data and audit access in these non-production environments. HIPAA defines standards for de-identification of PHI which may be applied by a cloud provider to reduce disclosure risk. Depending on the sensitivity of the data stored in the cloud and the organization's liability or concern over disclosure of the data, the organization may want to understand the circumstances around when copies of its data are made, who has access to the copies, and audit capabilities for these copies.