Carnegie Mellon University
Software Engineering Institute

Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud

Timothy Morrow
Kelwyn Pender
Carrie Lee
Don Faatz

July 2019

TECHNICAL REPORT
CMU/SEI-2019-TR-004

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM18-0225

Table of Contents

List of Figures

List of Tables

Abstract

As organizations develop new applications in or migrate existing applications to cloud services, they face changes in securing their information and applications. This report examines the changes to risks, threats, and vulnerabilities when applications are deployed to cloud services. Five cloud-unique threats and risks are identified along with seven threats and risks that exist on-premises and in cloud computing. For each of these threats and risks, recommendations are made for managing and mitigating the threats and risks when using cloud services.

1 Introduction

The Software Engineering Institute (SEI) investigated cloud computing threats[1] and vulnerabilities[2] that organizations may face as they consider moving assets and capabilities to the cloud.

1.1 Purpose

The SEI assessed the unique characteristics associated with cloud computing in the context illustrated in Figure 1 to identify threats, vulnerabilities, and risks that organizations face when they convert from internal data centers and on-premises private clouds to a public-cloud deployment.

The threats and vulnerabilities presented here are not exhaustive. Organizations need to consider other challenges and risks[3] associated with cloud adoption specific to their mission, systems, and data. The National Institute of Standards and Technology (NIST) cloud model [Mell 2011] provides a definition of cloud computing and how it can be used and deployed.

---

[1] According to the Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009 from April 6, 2015, a *threat* is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

[2] According to the Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009 from April 6, 2015, a *vulnerability* is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

[3] According to the Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009 from April 6, 2015, a *risk* is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence.

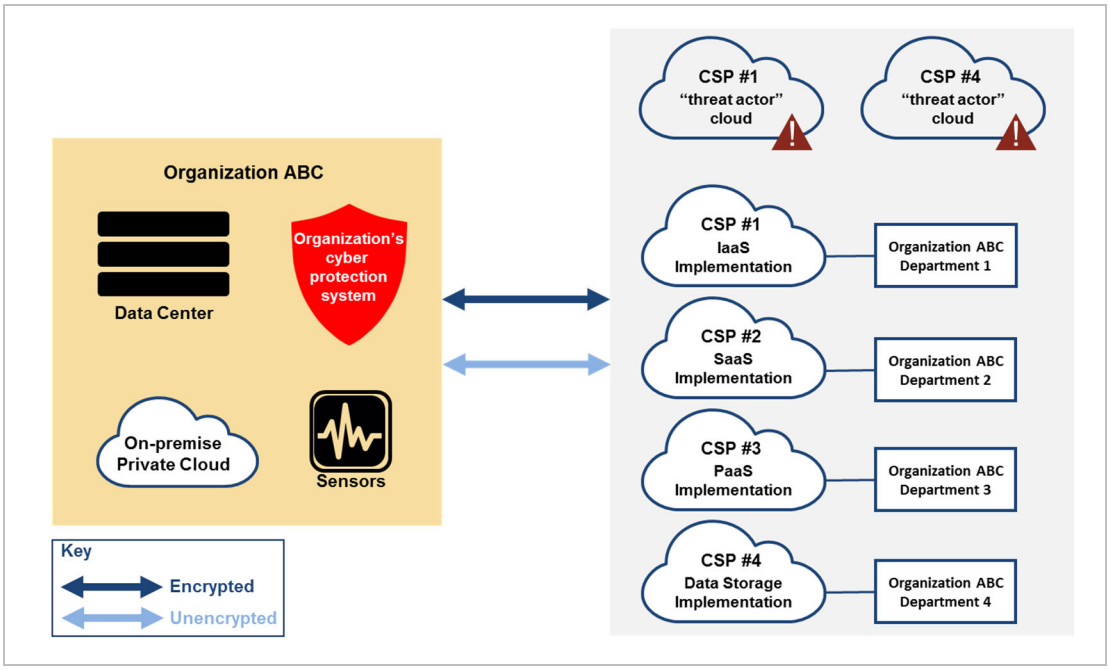

Figure 1: Potential Organization's Computing Environment

1.2 Scope

Cloud computing is defined by NIST as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST identifies the following characteristics and models for cloud computing:

- Essential Characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service[4]
- Service Models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)
- Deployment Models: private cloud, community cloud, public cloud, and hybrid cloud

Vulnerabilities and risks are considered using the Shared Responsibility Model (Figure 2), which is based on the three service models. The "Traditional IT" or "Classic IT" column represents internal data centers and/or on-premises private clouds. The "You manage" label refers to the cloud consumer (i.e., organizations). The cloud consumer's responsibilities lessen as you move from IaaS to PaaS to SaaS.

[4] These five characteristics are discussed in Appendix B.

It does not matter which service model(s) are used; identity and access management (IAM), configuration management, and monitoring and log analysis are key responsibilities that organizations must embrace to help secure their data and assets in the cloud [Yunghans 2017]. The community cloud deployment model is not considered in this report.

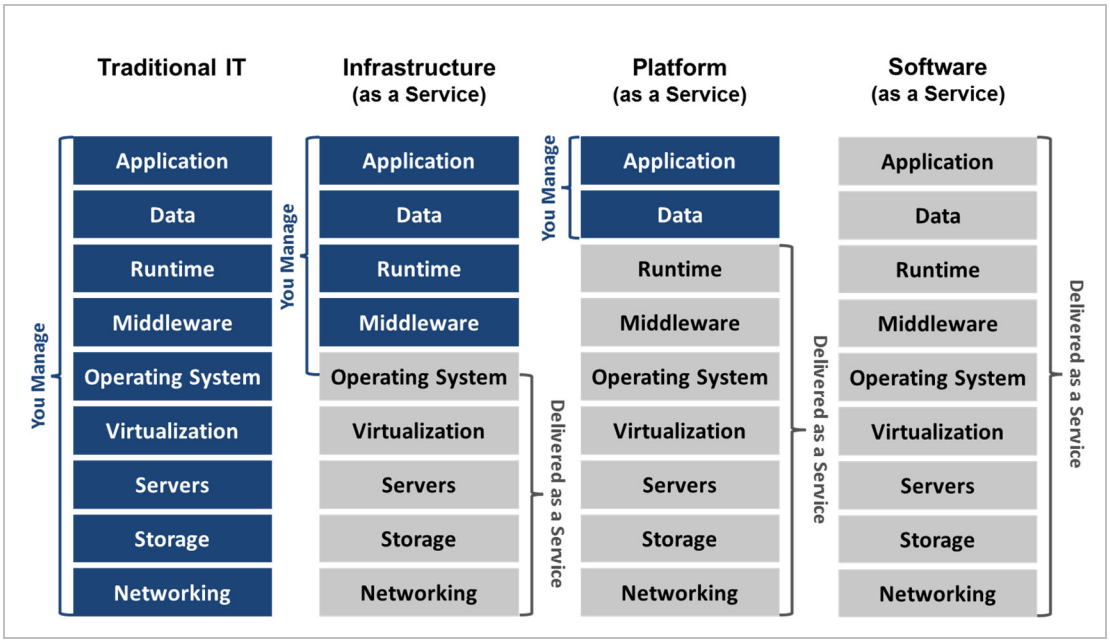

Figure 2: Shared Responsibility Model

Cloud environments experience—at a high level—the same threats as traditional data center environments; the threat picture is the same. That is, cloud computing runs software, software has vulnerabilities, and adversaries try to exploit those vulnerabilities. In the previous sentence, 'cloud computing' can be replaced with 'data center computing.' Figure 3 describes the threat picture for cloud computing platforms.

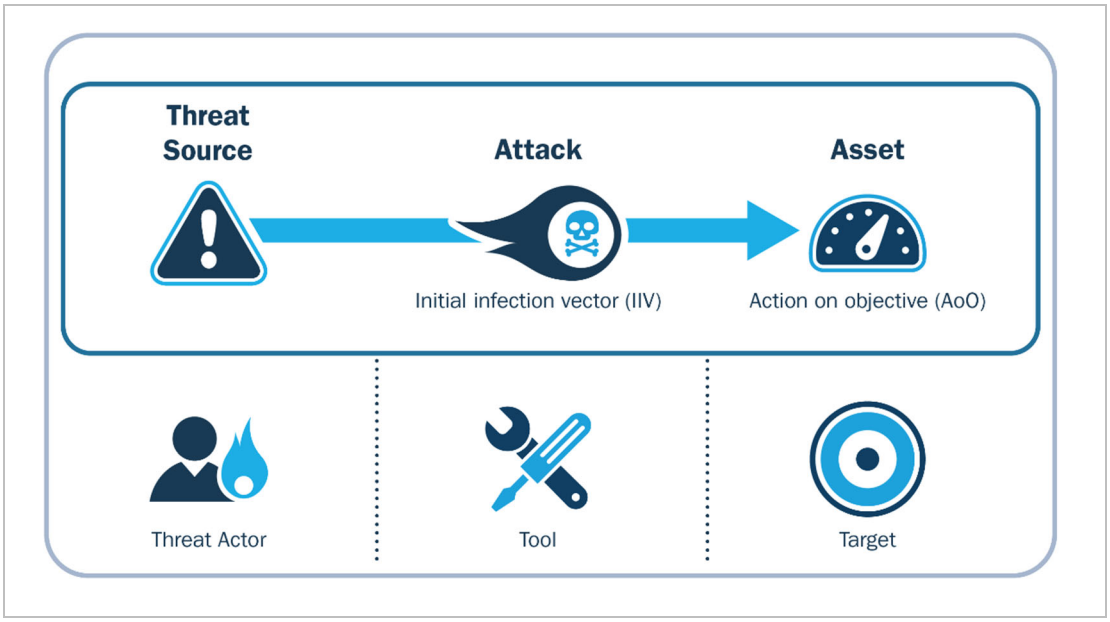

Figure 3: Threat Picture

While the threats for cloud computing and traditional data center computing are similar, the likelihood and/or impact of certain threats do change, affecting the risks an organization may face. Therefore, the increase in threat likelihood and impacts is a key focus of this report.

Organizations can choose from a number of cloud service providers (CSPs), offering various computing options to consider and trade off in determining the services that best meet their needs. In this report, we identify some important cloud computing threats and risks that need to be considered when an organization reasons about moving assets and capabilities to the cloud.

Three large CSPs, Amazon Web Service (AWS)[5], Microsoft Azure[6], and Google Cloud Platform,[7] were researched to learn what mitigation approaches and security controls were in place or suggested for the identified threats. Based on this and other researched information, recommendations were developed.

[5] https://aws.amazon.com/

[6] https://azure.microsoft.com/en-us/?v=18.05

[7] https://cloud.google.com/

2 Top Cloud Computing Threats and Risks

An organization that adopts cloud technologies and chooses CSPs and services or applications without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal, and compliance risks that jeopardize its success. In a paper addressing enterprises' moves to the cloud, Gartner identifies the following strategic planning assumption: "Through 2020, 95% of cloud security breaches will be the customer's fault" [Cancila 2016]. Also, due to their resource pooling characteristic, hackers can attack many organizations at once, thus reaping more benefits from a single successful attack.

This section identifies the vulnerabilities an organization needs to assess via its risk management process when considering moving assets to the cloud. The following information is provided for each vulnerability:

- a brief description
- threat probability and impact graphs
- example(s) of a threat based on the vulnerability
- recommendations for mitigation

This approach is based on the European Network and Information Security Agency's (ENISA) paper entitled "Cloud Computing: Benefits, Risks and Recommendations for Information Security" [ENISA 2012].

2.1 Cloud-Unique Threats and Risks

The following vulnerabilities are a result of a CSP's implementation of the five cloud computing characteristics. These vulnerabilities do not exist in classic IT data centers.

2.1.1 #1 Reduced Visibility and Control

Description

When transitioning assets/operations to the cloud, organizations lose some visibility and control over those assets/operations. When using external cloud services, the responsibility for some of the policies and infrastructure moves to the CSP.

The actual shift of responsibility depends on the cloud service model(s) used, leading to a paradigm shift for organizations in relation to security monitoring and logging. Organizations need to perform monitoring and log analysis on information about applications, services, data, and users, without using network-based monitoring and logging, which is available for on-premises IT.

As the CSP assumes more responsibilities, an organization's need increases for finding different ways to gather information to successfully monitor IT operations and satisfy security and compliance requirements. Organizations do not have the capability to levy their requirements on the CSP and are subject to the terms of the service level agreement (SLA), so an organization must work with the CSP via its SLA to ensure requirements are met.

Threat Probability and Impact

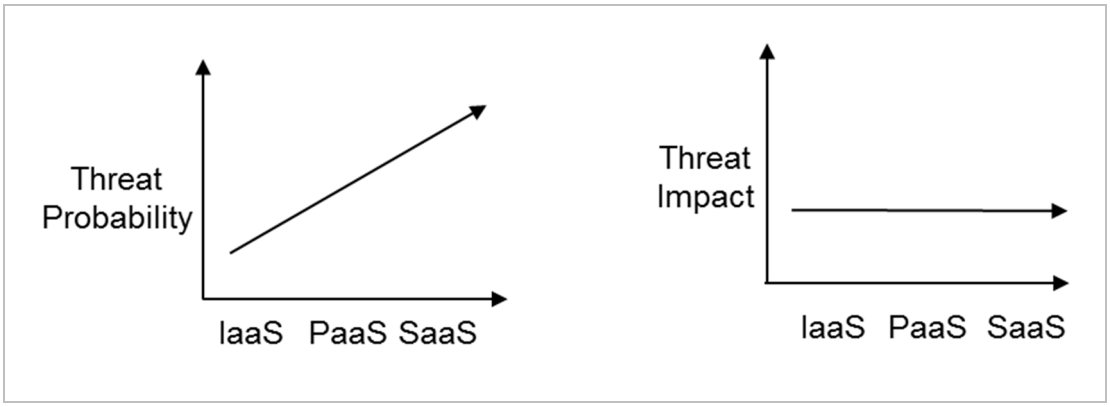

Figure 4: Reduced Visibility and Control Risk Graphs

Example

An organization has recently moved a website used to support a number of planned acquisitions from an on-premise data center to a CSP. The organization's IT staff had tools, network devices, and sensors in place to monitor and maintain the security of the website. The website is now implemented in the cloud, making use of the CSP's services to provide a front-end user interface, back-end connections to databases and storage, and a router that connects the website to the Internet. The organization selected the CSP partially based on its security record, but the IT staff would like more visibility into the interactions of the services used and the users accessing the site.

Recommendations

1. Use CSP services to log all user actions and actively monitor logs.
2. Use CSP services to log all data access and actively monitor logs.
3. Use CSP services to log application programming interface (API) calls and actively monitor the logs.
4. Treat the infrastructure as source code and enforce proper change control procedures [Sandage 2017]. Periodically check for changes.
5. Configuration manage the access controls to prevent or detect unauthorized changes [Morrato 2017].
6. Use security information and event management (SIEM) tools to monitor, analyze, and manage the logs.
7. Use CSP security monitoring capabilities.
8. Use CSP alerting capability for user actions, data access, and API calls.
9. Use bastion hosts[8] to enforce control and provide visibility [Centrify 2016].

[8] A description of a bastion host can be found on the SANS website: https://www.sans.org/security-resources/idfaq/what-is-a-bastion-host/2/11.

2.1.2 #2 On-Demand Self Service Simplifies Unauthorized Use

Description

CSPs make it very easy to provision new services. The on-demand self-service provisioning features[9] of the cloud enable organization personnel to provision additional services from the organization's CSP without IT consent using SaaS products (e.g., Dropbox, iCloud, OneDrive). The practice of using software in an organization that is not supported by the organization's IT department is commonly referred to as *shadow IT*.

Due to the lower costs and ease of implementing PaaS and SaaS products, the probability of unauthorized use of cloud services increases. Services provisioned or used without IT's knowledge present risks to an organization. The use of unauthorized cloud services could result in an increase in malware infections or data exfiltration since the organization is unable to protect resources it does not know about. The use of unauthorized cloud services also decreases an organization's visibility and control of its network and data.

Threat Probability and Impact

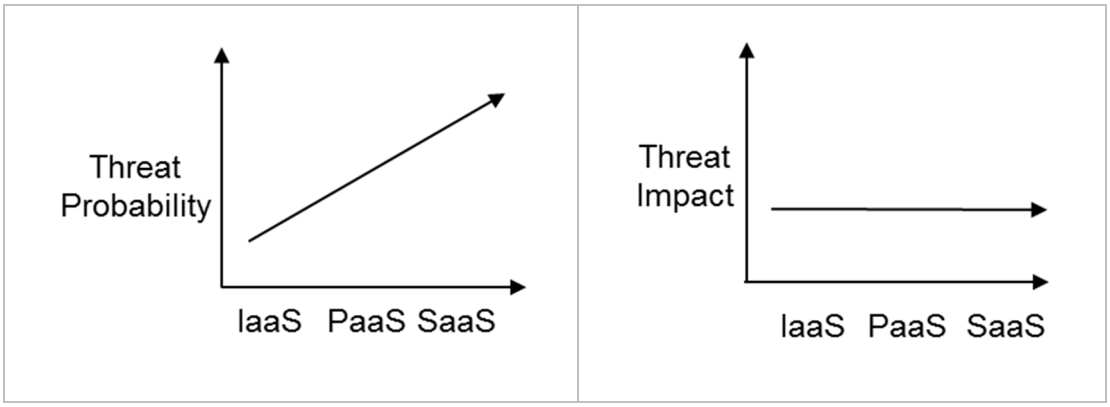

Figure 5: Ability to Self-Provision Resources and Services Risk Graphs

Example

An organization is using the IaaS service model. One of its programmers, who is a member of the DevOps team, is interested in trying out a new tool but is not sure of its value. The programmer wants to check it out prior to requesting approval to purchase and use the tool. Being a member of the DevOps team, the programmer can provision a work area and install the "30-day free trial" version of the tool. The programmer copies data and files from a development area and uses this information to evaluate the tool.

[9] The phrase "self-provisioning features" is defined in Appendix B.

Recommendations

1. Update the organization's security policy to prohibit self-provisioning unauthorized cloud services.
   - Set up alerts for access to cloud services that can be individually provisioned.
   - Require users to request access to cloud services; grant access on a case-by-case basis. This policy can be enforced by blocking access to common cloud services, such as Dropbox, and granting exceptions only when necessary.
2. Ensure the CSP service agreement does not allow users other than the designated IT representative to provision services.
3. Set up logging and alerting within the CSP console for new service provisioning.
4. Use role-based access control (RBAC) to control access to services. Periodically review the roles.
5. Treat infrastructure as source code and enforce proper change control procedures. Periodically check for changes.
6. Analyze enterprise firewall logs and proxy logs to identify enterprise access to and from CSPs provisioning resources not in the configuration baseline[MacDonald 2015].
7. Consider using a cloud access security broker application to help detect security policy violations such as self-provisioning and data exfiltration.
8. Use data loss prevention applications to provide technical and policy controls that help prevent data exfiltration to shadow IT.
9. In addition to protecting data, ensure the organization's security policy requires protection and configuration management for additional items, such as system configuration, architecture, and process flow, which combine in the cloud to form applications.

2.1.3 #3 Management API Compromise

Description

CSPs expose a set of APIs that customers use to manage and interact with cloud services (also known as the *management plane*). Organizations, via the Internet, use these APIs to provision, manage, orchestrate, and monitor their assets and users. These APIs can contain the same software vulnerabilities as an API for an operating system, library, etc. Unlike management APIs for on-premises computing, CSP APIs are accessible via the Internet exposing them more broadly to potential exploitation.

Threat actors look for vulnerabilities in management APIs. If discovered, these vulnerabilities can be turned into successful attacks and organization cloud assets can be compromised. From there, attackers can use organization cloud assets to perpetrate further attacks against other CSP customers.

Threat Probability and Impact

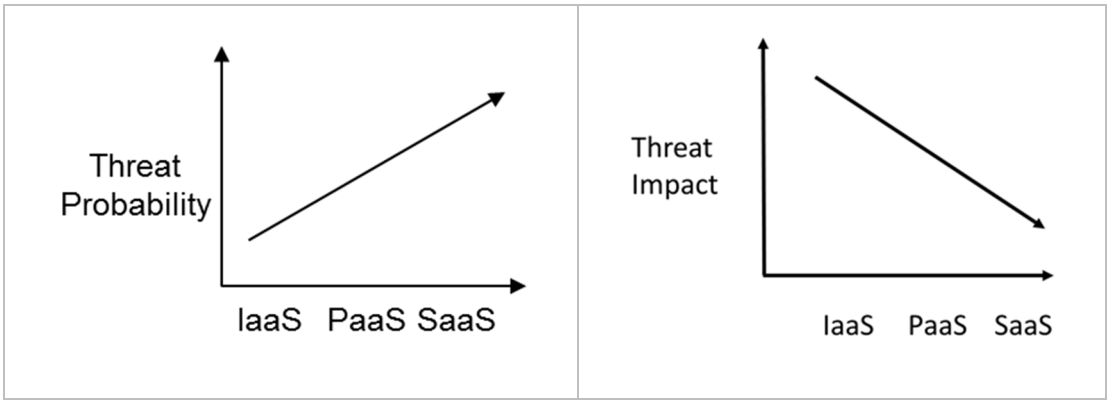

Figure 6: Management API Compromise Risk Graphs

Example

A threat actor uses a social media scheme to compromise the account of a user who has access rights to the management APIs used to provision CSP services. The threat actor uses this account to run an API vulnerability tool suite to identify possible vulnerabilities. The actor uses the information generated by the tool to develop attacks against the CSP's management APIs, which can be used against the CSP's customers.

Recommendations

1. Review the security practices of the CSP related to software development and vulnerability testing. Ensure that the CSP follows best practices, including performing code reviews and regular vulnerability testing.
2. Ensure that all accesses to and actions on the management API are logged and monitored, including logging and monitoring service, application, and user accesses and actions.
3. Implement the principle of least privilege when granting authorizations to services, applications, and users accessing the management API.
4. Use RBAC to control access to services, and periodically review the roles.
5. Ensure services and applications are configured with user-level permissions.
6. Move root capabilities to a role, and monitor, log, and profile its use to support behavioral analysis.
7. Check the billing of services to identify which services are being used.
8. Ensure that the credentials required to access the organization's network are different from those used to access the management APIs.
9. Develop a checks-and-balances process that provides protection that reflects and supports the size and skill level of the organization's IT staff. The process must ensure adequate separation of duties to prevent unilateral changes to production resources.

2.1.4 #4 Logical Separation Failure Among Multiple Tenants

Description

Exploitation of system and software vulnerabilities within a CSP's infrastructure, platforms, or applications that support multi-tenancy can lead to an isolation failure. This failure can be used by an attacker to gain access to another user's or organization's assets or data. Multi-tenancy increases the attack surface, leading to an increased chance of data leakage if the isolation controls fail [Gordon 2016].

This attack can be accomplished by exploiting vulnerabilities in the CSP's applications or hypervisor, subverting logical isolation controls or attacks on the CSP's management API. To date, there has not been a documented security failure of a CSP's SaaS platform that resulted in an external attacker gaining access to tenants' data [Heiser 2016].

No reports of an attack based on logical separation failure were identified, however, proof-of-concept exploits have been demonstrated. In 2009 researchers described an attack on AWS (Ristenpart 2009) that co-located a malicious virtual machine on the same physical hardware as a target virtual machine. The malicious virtual machine could observe characteristics of the shared hardware to infer information from the target virtual machine. More recently, on January 3, 2018, Google's Project Zero released information about vulnerabilities in Intel, AMD, and ARM processor designs (Horn 2018) that allow data access across logical separation boundaries. Project Zero developed four proof-of-concept exploits demonstrating the separation failure. These vulnerabilities enable logical separation failure attacks on all cloud service models, IaaS, PaaS, and SaaS.

Threat Probability and Impact

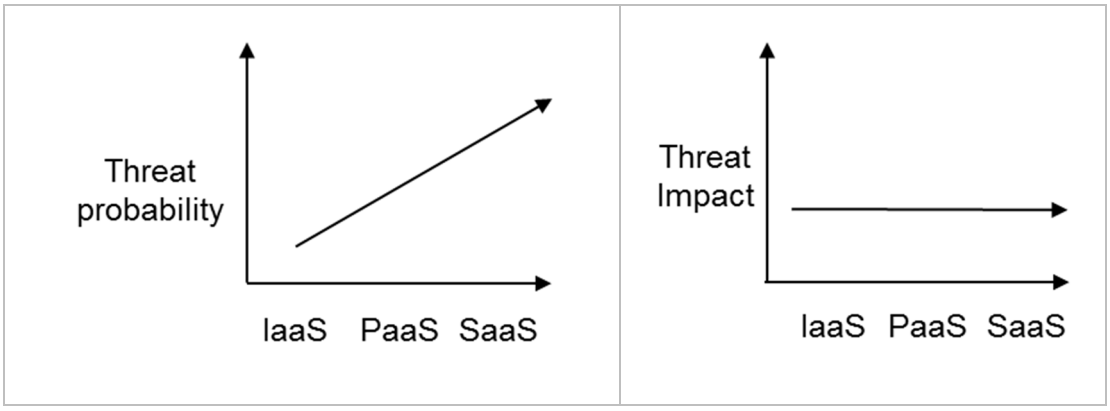

Figure 7: Multi-Tenancy Security Risk Graphs

Examples

An attacker uses stolen credentials to execute cache side-channel attacks to exfiltrate sensitive information from an organization via shared CPU caches.

A threat actor compromises the account of an organization user who has privileges to provision a virtual machine (VM). The actor loads a malicious version of Linux, which also contains tool suites that look for vulnerabilities in the VM's user area and in connections to the hypervisor. The

actor finds a vulnerability in the connections to the hypervisor code, which the actor later uses to compromise the software and view other VMs running on the same compute device.

An organization uses a CSP to build web applications supported by a backend SQL database. A threat actor identifies a vulnerability in one of the services supported by the CSP. The actor compromises an organization user's account. The threat actor uses this account to conduct an attack that places malicious code on the CSP's computing platform the organization is using. The threat actor now has access to the platform shared by other tenants using the CSP.

Recommendations

1. Review the CSP's implementation of customer resource and data isolation[10].
   - Ask the CSP how it prevents users from hopping virtual local area networks (VLANs).
   - Ensure that the CSP performs regular penetration testing and vulnerability analysis of processes, services, and APIs.
   - If the CSP uses a hypervisor, determine the methods used by the CSP to ensure it is regularly tested for vulnerabilities and updated when vulnerabilities are found.
2. Use CSP services to log all data access and actively monitor logs.
3. Ensure data is encrypted at rest and in transit.
4. Review available security reporting from the CSP. Configure advanced reporting features, such as behavior profiling, if available.
5. Use bastion hosts to limit access, enforce controls, and provide visibility.
6. Review the CSP's supply chain practices to ensure that suppliers are vetted and held to the same security practices as the CSP.

2.1.5 #5 Incomplete Data Deletion

Description

Threats associated with data deletion exist because the consumer has reduced visibility into where its data is physically stored in the cloud and a reduced ability to verify the secure deletion of its data. This risk is concerning because the data is spread over a number of different storage devices within the CSP's infrastructure in a multi-tenancy environment. In addition, deletion procedures may differ from provider to provider. Organizations may not be able to verify that their data was securely deleted and that remnants of the data are not available to attackers. This threat increases as an organization uses more CSP services.

---

[10] Data isolation controls must address issues such as ensuring that (1) packet sniffing by other tenants in the server is not possible in a hypervisor, (2) two VMs owned by the same customer and located on the same physical host cannot listen to each other's traffic, and (3) attacks like ARP cache poisoning will not work. The hypervisor must ensure that traffic is delivered to the specified destination VM(s), and cannot be seen or delivered to other VMs on the same physical host.

Threat Probability and Impact

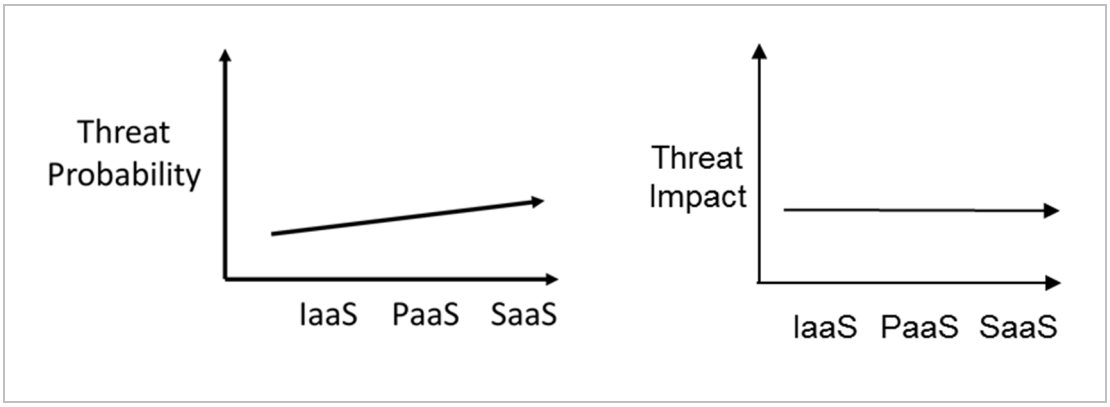

Figure 8: Data Deletion Risk Graphs

Example

An organization has been storing medical research files and data across two CSPs in compliance with its business continuity plan. The research is completed and the organization is archiving the information in on-premises data centers. After the archive is verified, the organization deletes its data at the two CSPs, but at one CSP, a bank of drives is offline due to a power supply problem. One of the offline drives holds some data to be deleted. Determining how the CSP ensures that the data is deleted from all physical devices—including backups—is a concern that must be addressed.

Recommendations

1. Review the CSP's policies and SLAs on data deletion to ensure it has a procedure that effectively deletes data.
2. Review the CSP's policies on data restoration.
3. Review the CSP's policies on data replication.
4. Review the CSP's policies and procedures on sanitizing disks.
5. Encrypt all stored data so that data remnants are unreadable (crypto erasure).
6. Understand your organization's data architecture, data implementation, data redundancy, data backup, and resilience planning processes to know all locations where your data is stored.
7. Review how the CSP's services use and store your data to determine from where data must be deleted.
8. Limit access to data backups (through use of roles) to know who has access to the data.

2.2 Cloud and On-Premise Threats and Risks

The following are risks that apply to both cloud and classic IT data centers that organizations need to address.

2.2.1 #6 Stolen Credentials

Description

If an attacker gains access to an organization user's cloud credentials, the attacker can have access to the CSP's services to provision additional resources (if credentials allowed access to provisioning), as well as target the organization's assets. The attacker could leverage cloud computing resources to target users, organizations using the same CSP, or other organizations. An attacker who gains access to a CSP administrator's cloud credentials may be able to use those credentials to access the organization's systems and data.

Administrator roles vary between a CSP and an organization. The CSP administrator has access to the CSP network, systems, and applications (depending on the service) of the CSP's infrastructure. Whereas the organization's administration has access only to the organization's cloud implementations. In essence, the CSP administrator has administration rights over more than one customer and supports multiple services.

Threat Probability and Impact

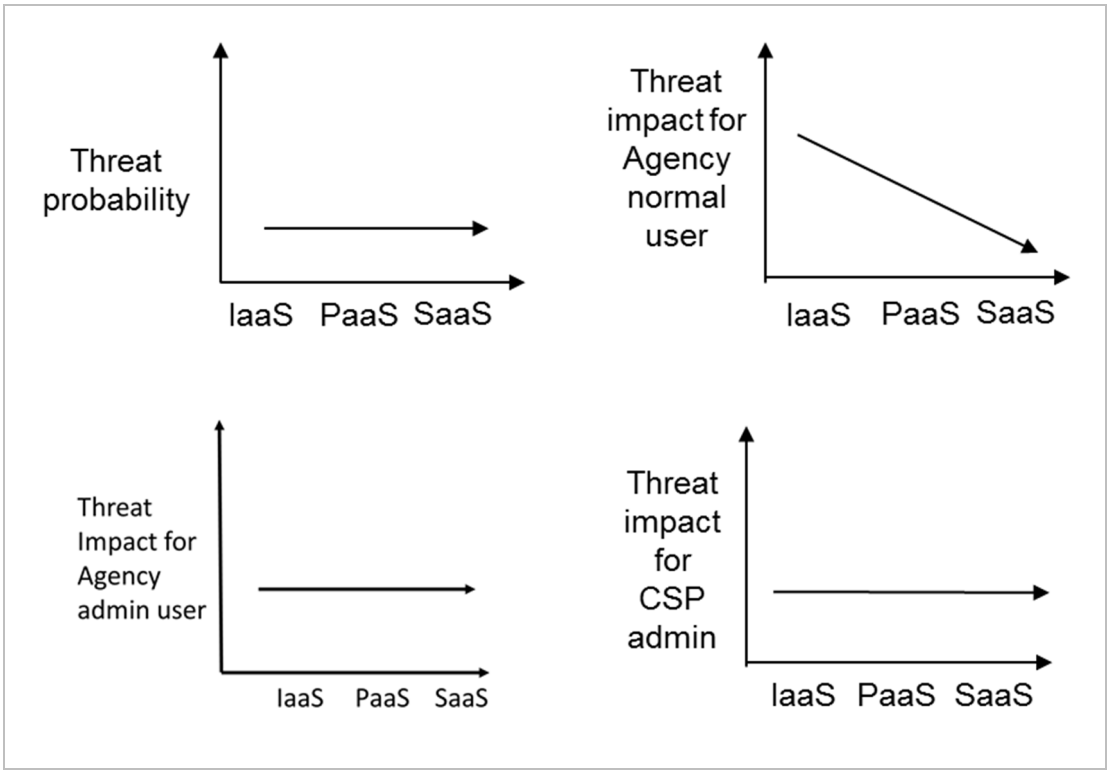

Figure 9: Credential Stealing Risk Graphs

Example

A threat actor learns that a particular organization is using XX CSP. The actor initiates a phishing email campaign attempting to target the organization's IT staff and support personnel. After compromising an organization's IT staff member's account, the actor begins reconnaissance of the staff's accounts to find one with the privilege to provision XX CSP's services. Once that account is found and compromised, the actor can severely impact the organization's operations.

Recommendations

1. Enable multi-factor authentication for cloud user accounts. (This may require purchasing additional services.)
2. Use access controls to implement the principle of least privilege and separation of duties.
3. Encrypt organization data at rest and in transit.
4. Use the CSP's services to log all user actions and actively monitor logs.
5. Use the CSP's services to log all data access and actively monitor logs.
6. Use a federated IAM approach for cloud and on-premises computing to minimize the attack surface [Centrify 2016].
7. Use secure key management processes.
8. Move root capabilities to a role and monitor/log/profile its use to support behavioral analysis.

2.2.2 #7 Vendor Lock-In Complicates Moving to Other CSPs

Description

Vendor lock-in becomes an issue when an organization considers moving its assets/operations from one CSP to another. The organization finds out that the cost/effort/schedule time necessary for the move is much higher that initially considered due to non-standard data formats, non-standard APIs, high charges to remove the presence on original CSP, inability to transfer large amounts of data out of a CSP in a timely manner, and reliance on one CSP's proprietary tools and unique APIs.

This issue increases in service models, such as SaaS, where the CSP takes more responsibility. As an organization uses more features, services, or APIs, the exposure to a CSP's unique implementations increases. These unique implementations require changes when a capability is moved to a different CSP. If a selected CSP goes out of business, it becomes a major problem since data can be lost or cannot be transferred to another CSP in a timely manner.

Threat Probability and Impact

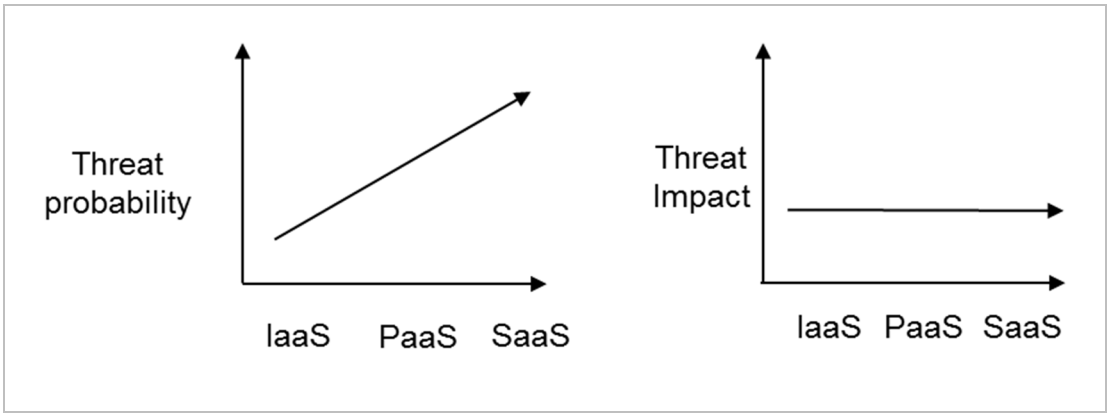

Figure 10: Vendor Lock-In Risk Graphs

Example

An organization contracts with a CSP for customer relationship management (CRM) services, and its data is stored in a proprietary format. The CSP declares bankruptcy, and the organization is given 60 days to retrieve its data. Due to the proprietary format, it is unable to port the data to its own systems or another CSP in the timeframe allotted. The organization incurs significant costs to recover the data.

Recommendations

1. Prior to selecting a CSP, check its ability to interface with other CSPs and use standard data formats.
2. Investigate the CSP's support for standard interfaces and open APIs. (Use standard data formats when possible.)
3. Understand how data can be imported into and exported from the service before choosing a CSP [Khnaser 2017].
4. When developing cloud-native applications, consider application lock-in due to use of the CSP's APIs.
5. Consider the impacts of possible vendor lock-in on the organization's business continuity planning (BCP) and disaster recovery planning (DRP) [Knipp 2016].

2.2.3 #8 Increased Complexity that Strains IT Staff

Description

Migrating to the cloud can introduce complexity into IT operations. Managing, integrating, and operating in the cloud may require that the organization's existing IT staff learn a new model. IT staff must have the capacity and skill level to manage, integrate, and maintain the migration of assets and data to the cloud in addition to their current responsibilities for on-premises IT.

Key management and encryption services become more complex in the cloud. The services, techniques, and tools available to log and monitor cloud services typically vary across CSPs, further increasing complexity. There may also be emergent threats/risks in hybrid cloud implementations due to technology, policies, and implementation methods, which add complexity. This added

complexity leads to an increased potential for security gaps in an organization's cloud and on-premises implementations.

Threat Probability and Impact

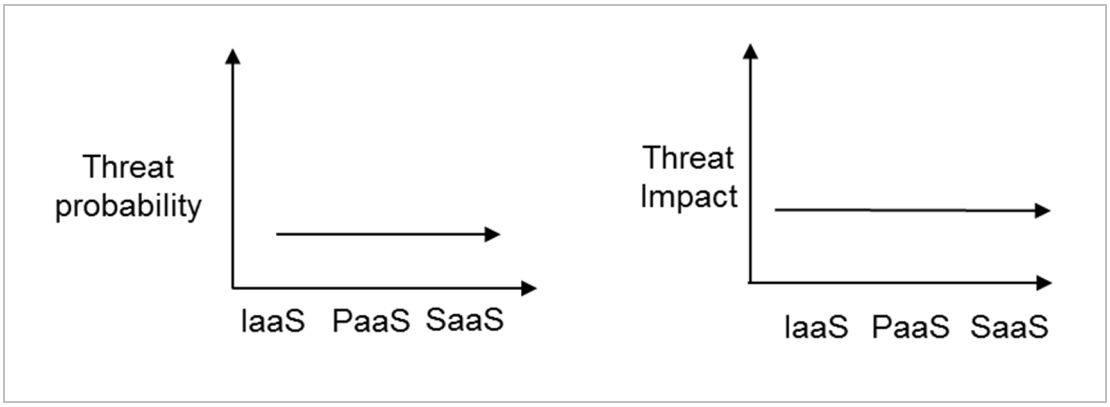

Figure 11: Increased Complexity that Strains IT Staff Risk Graphs

Example

An organization migrates some of its systems to a CSP's IaaS offering. The new infrastructure is not intuitive and requires extensive training to understand. In addition, several third-party tools are needed to implement proper monitoring and alerting for these systems. The IT department is consumed with the new infrastructure and does not have the resources to maintain the organization's current in-house infrastructure properly.

Recommendations

1. Review the features and documentation of configuration management tools prior to selecting a CSP to ensure management tools are sufficient for IT staff.
2. Include time in implementation schedules for training staff on CSP management tools and services.
3. Account for reconfiguring and maintaining systems and applications that require a considerable amount of expertise.
4. Map existing security policies and procedures to those available from the CSP [Gordon 2016].

2.2.4 #9 Insider Threat

Description

A malicious insider is defined as a current or former employee, contractor, or business partner who meets the following criteria:

- has or had authorized access to an organization's network, systems, or data
- has intentionally exceeded or intentionally used that access in a manner that negatively affects the confidentiality, integrity, or availability of the organization's information or information systems

This definition applies to staff and administrators for both organizations and CSPs.

The impact is most likely worse when using IaaS due to an insider's ability to provision resources or perform nefarious activities that require forensics for detection. These forensic capabilities may not be available with cloud resources.

A CSP user's threat impact depends on their organization's employee vetting process (background checks) and controls implementation.

Threat Probability and Impact

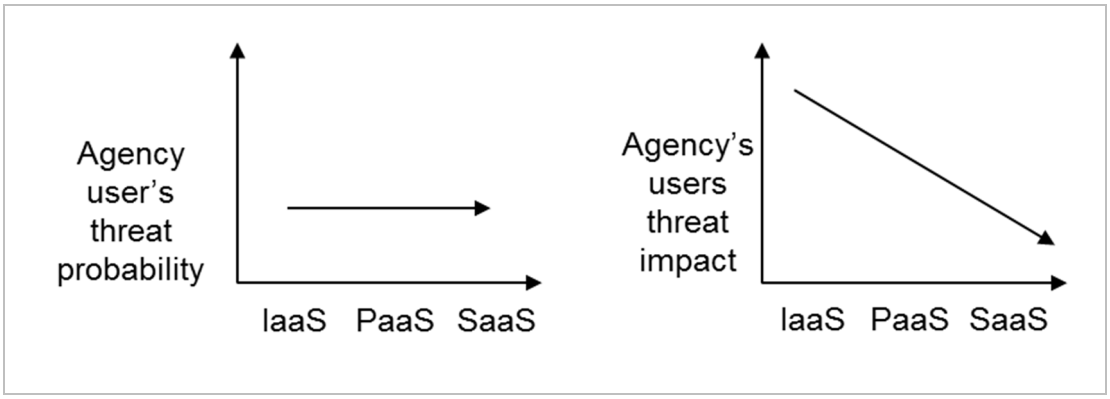

Figure 12: Insider Threat Risk Graphs

Example

A CSP administrator decides to make extra money by selling sensitive government information. They use their administrative credentials to steal data from multiple organization cloud instances. They also insert a backdoor onto the CSP's systems to gain future access without needing administrator credentials.

Recommendations

1. Enable multi-factor authentication for cloud user accounts.
2. Use access controls to implement the principles of least privilege and separation of duties.
3. Encrypt organization data at rest and in transit.
4. Use CSP services to log all user actions and actively monitor logs.
5. Use CSP services to log all data access and actively monitor logs.
6. Move root capabilities to a role and monitor/log its use.
7. Treat infrastructure as code and enforce proper configuration management procedures.
8. Be aware of the differences between vetting processes for becoming administrators for the CSP and for the organization; assess the impact of these differences.

2.2.5 #10 Data Loss

Description

As with data stored on-premises, data stored in the cloud can be lost for reasons other than malicious attacks. Accidental deletion of data by the cloud service provider or a physical catastrophe, such as a fire or earthquake, can lead to the permanent loss of customer data. The burden of avoiding data loss does not fall solely on the provider's shoulder. If a customer encrypts its data

before uploading it to the cloud but loses the encryption key, the data will be lost. In addition, inadequate understanding of a CSP's storage model may result in data loss. Organizations must consider data recovery and be prepared for the possibility of their CSP being acquired, changing service offerings, or going bankrupt [Gordon 2016].

This threat increases as an organization uses more CSP services. Recovering data stored at a CSP may be easier than recovering it at an organization because a SLA designates availability/uptime percentages. These percentages should be investigated when the organization selects a CSP.

Threat Probability and Impact

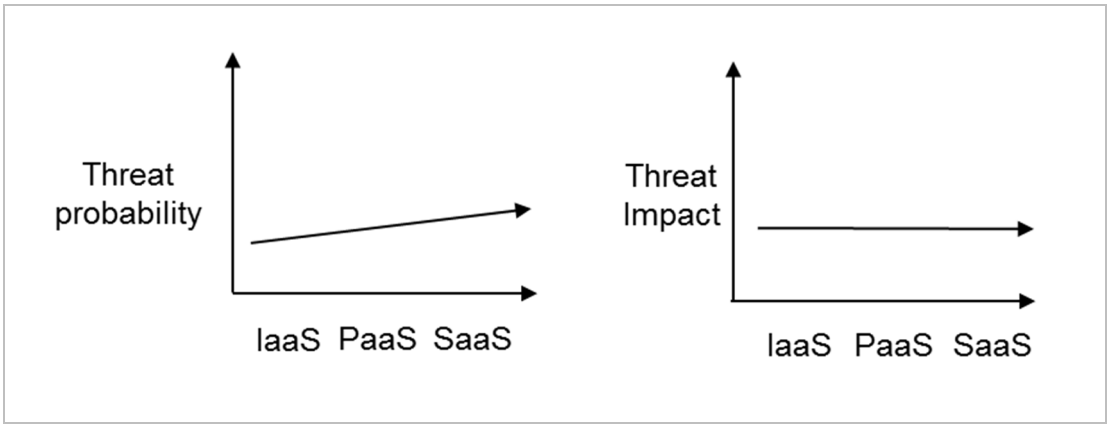

Figure 13: Data Recovery Risk Graphs

Example

A CSP suffers from widespread corruption of disks in their infrastructure. Some organization data is corrupted, and the backups are unreadable. The organization loses data.

Recommendations

1. Ensure that the CSP uses access permissions consistent with the principle of least privilege to protect against accidental or malicious deletion.
2. Review SLA documents for the CSP's availability and recovery time objectives (RTOs). Ensure it meets organization availability and RTO needs. Look at the history of the CSP's availability percentages before purchasing its services.
3. Review the data deletion and recovery processes of the CSP to ensure they meet organization needs. Ensure that the IT staff is familiar with the policies once cloud services are deployed.
4. Consider the recovery of data stored in the cloud when developing the organization BCP/DRP.

2.2.6 #11 Compromised Supply Chain

Description

If the CSP outsources parts of its infrastructure, operations, or maintenance, these third parties may not satisfy/support the requirements that the CSP is contracted to support with an organization. An organization needs to evaluate how the CSP enforces compliance and check to see if the

CSP flows its own requirements down to third parties. If the requirements are not being levied on the supply chain, then the threat to the organization increases.

This threat increases as an organization uses more CSP services and is dependent on individual CSPs and their supply chain policies.

Threat Probability and Impact

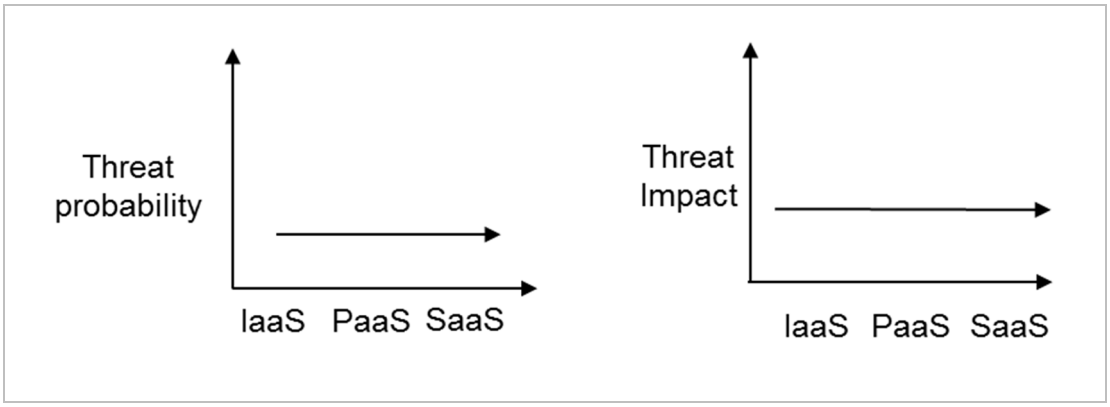

Figure 14: Supply Chain Risk Graphs

Example

A CSP uses network equipment that houses chips from a foreign country. The chips are outfitted with a hidden backdoor that allows foreign interests to monitor the CSP's network traffic. Due to this monitoring, the foreign interest is able to capture an organization's traffic.

Recommendations

1. Review the CSP's supply chain practices. Ensure that suppliers are vetted and held to the same security practices as the CSP.
2. If applicable, ensure the CSP has vetted its supply chain for compliance with FAR regulations, which require that government contractors and their supply chain are compliant with NIST SP 800-171 [Ross 2015] when storing controlled unclassified information (CUI).

2.2.7 #12 Insufficient Due Diligence Increases Cybersecurity Risk

Description

Organizations migrating to the cloud often perform insufficient due diligence. They move data to the cloud without understanding the full scope of doing so, the security measures used by the CSP, and their own responsibility to provide security measures. They make decisions to use cloud services without fully understanding how those services must be secured.

Threat Probability and Impact

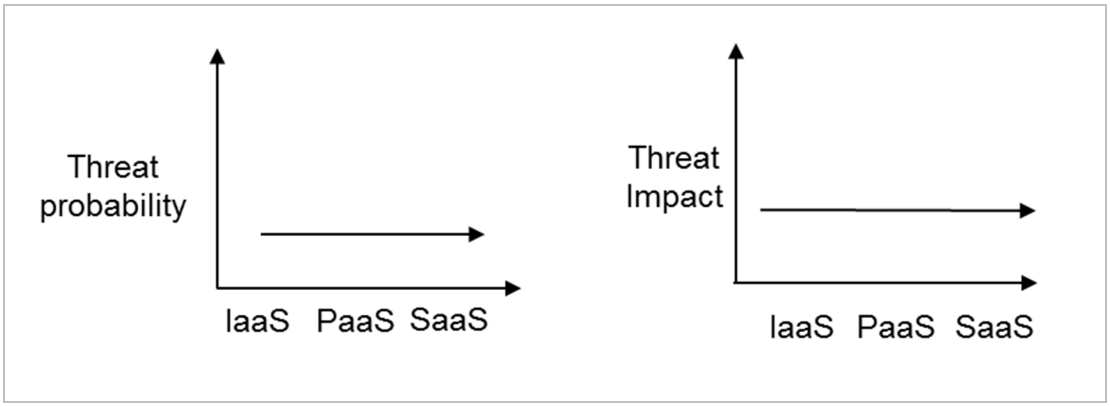

Figure 15: Insufficient Due Diligence Risk Graphs

Example

An organization decides to migrate to the cloud without accounting for security and changes in business processes required to support the move. Its cloud assets are exploited by a hacker, but the organization is not aware of the breach or data loss occurring from the breach because it did not implement proper logging and monitoring of application and data access.

Recommendations

1. Work with cloud experts to identify assets and capabilities that are both a good fit for cloud implementation and that can be effectively secured.
2. Perform a risk assessment on data migrating to the cloud. Implement security controls based on this assessment.
3. Work with CSPs to understand their SLAs, shared responsibility model, and pricing and support structure.

3 Summary and General Recommendations

In this report, we identified five cloud-unique and seven cloud and on-premises threats that organizations face as they consider migrating their data and assets to the cloud. For each threat, we covered probability and impacts based on the three service models (IaaS, PaaS, and SaaS), example(s) of the threat, and recommendations. The recommendations provided are suggestions for organizations to consider. A high-level summary of those recommendations is presented below.

1. Regardless of the platform (classic IT or cloud), apply (1) security architecture and design, (2) security engineering, (3) secure coding, (4) security policy, (5) governance, and (6) risk management.
2. Regardless of the CSP or service model used by an organization, accept ultimate responsibility for IAM, configuration management, monitoring and log analysis, and data security.
3. Develop/acquire expertise to log and monitor organization networks and data in the cloud based on cloud security guidance and best practices.
4. Perform due diligence assessments concerning migrating capabilities and assets to the cloud. Understand the division of responsibilities between the CSP and organization to provide security. Understand the security controls available from the CSP to protect organization assets.
5. Train your IT staff to support hybrid cloud implementations because organizations will be operating in a mixed classic IT/cloud environments for the foreseeable future.
6. Embrace a DevOps-like approach to security as organization IT staff improves their cloud skills to improve your organization's ability to address threats and handle incidents.
7. Carefully plan and prepare to use SIEM tools in monitoring and logging. First identify access monitoring requirements, configure CSP services to provide the desired audit and log data, determine if the format of the audit and log data is compatible with SIEM tools, and, if not, port the data to an acceptable format. Develop baselines for typical access behaviors for cloud data, and tune SIEM tools to alert only on possible anomalous behavior. As additional research is performed in the area of CSP operational security, new sources of audit and logging data may need to be configured for the SIEM tool.

Appendix A Recommendations Mapped to Security Control Categories (NIST SP 800-53, Rev. 4)

Table 1: Recommendations Mapped to Security Control Categories

Security Control Category	Recommendation
Access Control	Use role-based access control (RBAC) to control access to services. Periodically review the roles.
	Implement the principle of least privilege when granting authorizations to services, applications, and users accessing the management API.
	Use access controls to implement principle of least privilege and separation of duties.
	Move root capabilities to a role and monitor, log, and profile its use to support behavioral analysis.
	Use bastion hosts to limit access, enforce controls, and provide visibility.
	Limit access to data backups (through use of roles) to know who has access to the data.
	Ensure that the credentials required to access the organization's network are different from those used to access the management APIs.
	Ensure that the CSP uses access permissions consistent with the principle of least privilege to protect against accidental or malicious deletion.
Awareness and Training	Include time in implementation schedules for training staff on CSP management tools and services.
Audit and Accountability	Use CSP services to log all user actions and actively monitor logs.
	Use CSP services to log all data access and actively monitor logs.
	Use CSP services to log API calls and actively monitor the logs.
	Use security information and event management (SIEM) tools to monitor, analyze, and manage the logs.
	Use CSP security monitoring capabilities.
	Set up logging and alerting within the CSP console for new service provisioning.
	Use CSP alerting capability for user actions, data access, and API calls.
	Review available security reporting from the CSP. Configure advanced reporting features, such as behavior profiling, if available.
	Analyze enterprise firewall logs and proxy logs to identify enterprise access to and from CSPs provisioning resources not in the configuration baseline (MacDonald & Young, 2015).
	Check the billing of services to identify which services are being used.
Security Assessment and Authorization	Ensure that the CSP performs regular penetration testing and vulnerability analysis of processes, services, and APIs.
	If the CSP uses a hypervisor, determine the methods used by CSP to ensure it is regularly tested for vulnerabilities and updated when vulnerabilities are found.

Configuration Management	Treat the infrastructure as source code and enforce proper change control procedures. Periodically check for changes.
	Configuration manage the access controls to prevent or detect unauthorized changes.
	Review the features and documentation of configuration management tools prior to selecting a CSP to ensure management tools are sufficient for IT staff.
Contingency Planning	Review the data deletion and recovery processes of the CSP to ensure they meet organization needs. Ensure that the IT staff is familiar with the policies once cloud services are deployed.
	Consider the recovery of data stored in the cloud when developing the organization BCP/DRP.
	Consider the impacts of possible vendor lock-in on the organization's business continuity planning (BCP) and disaster recovery planning (DRP).
	Review SLA documents for the CSP's availability and recovery time objective (RTO). Ensure it meets organization availability and RTO needs. Look at the history of the CSP's availability percentages before purchasing its services.
Identification and Authentication	Enable multi-factor authentication for cloud user accounts. (This may require purchasing additional services.)
	Use a federated IAM approach for cloud and on-premises computing to minimize the attack surface [Centrify 2016].
Media Protection	Review the CSP's policies and SLAs on data deletion to ensure it has a procedure that effectively deletes data.
	Encrypt all stored data so that data remnants are unreadable (crypto erasure).
	Review the CSP's policies on data restoration.
	Review the CSP's policies on data replication.
	Review the CSP's policies and procedures on sanitizing disks.
	Use data loss prevention applications to provide technical and policy controls that help prevent data exfiltration to shadow IT.
Planning	Understand your organization's data architecture, data implementation, data redundancy, data backup, and resilience planning processes to know all locations where your data is stored.
	Understand how data can be imported into and exported from the service before choosing a CSP.
	When developing cloud-native applications, consider application lock-in due to use of the CSP's APIs.
	Account for reconfiguring and maintaining systems and applications that require a considerable amount of expertise.
	Map existing security policies and procedures to those available from the CSP [Gordon 2016].
	Work with cloud experts to identify assets and capabilities that are both a good fit for cloud implementation and that can be effectively secured.
	Prior to selecting a CSP, check its ability to interface with other CSPs and use standard data formats.

	Investigate the CSP's support for standard interfaces and open APIs. (Use standard data formats when possible.)
	Perform a risk management on data migrating to the cloud. Implement security controls based on this assessment.
	Review how the CSP's services use and store your data to determine from where data must be deleted.
	Develop a checks-and-balances process that provides protection that reflects and supports the size and skill level of the organization's IT staff. The process must ensure adequate separation of duties to prevent unilateral changes to production resources.
	In addition to protecting data, ensure the organization's security policy requires protection and configuration management for additional items, such as system configuration, architecture, and process flow, which combine in the cloud to form applications.
Personnel Security	Be aware of the differences between vetting processes for becoming administrators for the CSP and for the organization; assess the impact of these differences.
Systems and Services Acquisition	Ensure the CSP service agreement does not allow users other than the designated IT representative to provision services.
	Review the security practices of the CSP related to software development and vulnerability testing. Ensure that the CSP follows best practices, including code reviews and regular vulnerability testing.
	Prior to selecting a CSP, check its ability to interface with other CSPs and use standard data formats.
	Investigate the CSP's support for standard interfaces and open APIs.
	Be aware of the differences between vetting processes for becoming administrators for the CSP and for the agency organization, and assess the impact of these differences.
	Review the CSP's supply chain practices to ensure that suppliers are vetted and held to the same security practices as the CSP.
	Work with CSPs to understand their SLAs, shared responsibility model, and pricing and support structure.
	Update the agency organization's security policy to prohibit self-provisioning unauthorized cloud services.
	Ensure that all accesses to and actions on the management API are logged and monitored, including logging and monitoring service, application, and user accesses and actions.
	If applicable, ensure the CSP has vetted its supply chain for compliance with FAR regulations, which require that government contractors and their supply chain are compliant with NIST SP 800-171 [Ross 2015] when storing controlled unclassified information (CUI).
	Require users to request access to cloud services; grant access on a case-by-case basis. This policy can be enforced by blocking access to common cloud services, such as Dropbox, and granting exceptions only when necessary.
	Ensure services and applications are configured with user-level permissions.

System and Communications Protection	Ask the CSP how it prevents users from hopping virtual local area networks (VLANs).
	Use secure key management processes.
	Consider using a cloud access security broker application to help detect security policy violations such as self-provisioning and data exfiltration. Review the CSP's FedRamp CIS document for information about resource and data isolation controls.
	Ensure data is encrypted at rest and in transit. Consider using a cloud access security broker application to help detect security policy violations such as self-provisioning and data exfiltration.
	Ensure data is encrypted at rest and in transit.
System and Information Integrity	Ensure data is encrypted at rest and in transit.

Appendix B Five Essential Cloud Computing Characteristics

The five essential cloud computing characteristics are defined as follows:

1. **On-demand self-service** – A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
2. **Broad network access** – Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or think client platforms (e.g., mobile phones, tablets, laptops, and workstations).
3. **Resource pooling** – The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
4. **Rapid elasticity** – Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
5. **Measured service** – Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

References/Bibliography

URLs are valid as of the publication date of this document.

[Boyens 2015]
Boyens, Jon; Paulse, Celia; Moorthy, Rama; & Bartol, Nadya. NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST. April 2015.

[Cancila 2016]
Cancila, Mindy; Toombs, Douglas; Waite, Alan, & Khnaser, Elias. *2017 Planning Guide for Cloud Computing*. Gartner. 2016.

[Centrify 2016]
Centrify. *Six Best Practices for Securing Amazon Web Services*. 2016.

[ENISA 2012]
European Network and Information Security Agency (ENISA). *Cloud Computing: Benefits, risks and recommendations for information security*. 2012. https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

[Gordon 2016]
Gordon, Adam. *The Official (ISC)^2 Guide to the CCSP CBK, 2nd Edition*. John Wiley & Sons, Inc. 2016. https://www.wiley.com/WileyCDA/WileyTitle/productCd-1119276748,miniSiteCd-SYBEX.html

[Heiser 2016]
Heiser, Jay. *Everything You Know About SaaS Security Is Wrong*. Gartner. 2016. https://www.gartner.com/doc/3339317/everything-know-saas-security-wrong

[Horn 2018]
Horn, Jann, “Reading privileged memory with a side-channel,” Google Project Zero, January 2018. https://googleprojectzero.blogspot.co.uk/2018/01/reading-privileged-memory-with-side.html

[Khnaser 2017]
Khnaser, Elias. *Designing a Public Cloud Exit Strategy*. Gartner. 2017. https://www.gartner.com/doc/3564517/designing-public-cloud-exit-strategy

[Knipp 2016]
Knipp, Eric; Clayton, Traverse; & Watson, Richard. *A Guidance Framework for Architecting Portable Cloud and Multicloud Applications*. Gartner. 2016. https://www.gartner.com/binaries/.../a_guidance_framework_for_architecting.pdf

[Kundra 2011]
Kundra, Vivek. *Federal Cloud Computing Strategy*. 2011.

[McAfee 2016]
McAffe Labs. *2017 Threat Predictions.* 2016. https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

[MacDonald 2015]
MacDonald, Neil & Young, Greg. *Best Practices for Securing Workloads in Amazon Web Services*. Gartner. 2015. https://www.gartner.com/doc/3030318/best-practices-securing-workloads-amazon

[Mell 2011]
Mell, Peter & Grance, Timothy. *The NIST Definition of Cloud Computing*. NIST Special Publication 800-145. 2011. https://csrc.nist.gov/publications/detail/sp/800-145/final

[Morrato 2017]
Morato, Mike. *Assessing Cloud Security Monitoring and Compliance Capabilities in Amazon Web Services*. Gartner. 2017. https://www.gartner.com/doc/3606021/assessing-cloud-security-monitoring-compliance

[Ristenpart 2009]
Ristenpart, Thomas, Eran Tromer, Hovav Shacham, Stefan Savage "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds." Proceeding of Computing and Communications Security, ACM, November 2009.
https://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf

[Ross 2015]
Ross, Ron; Viscuso, Patrick; Guissane, Gary; Dempsey, Kelley, & Riddle, Mark. *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. NIST Special Publication 800-171. 2015. https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

[Sandage 2016]
Tim Sandage & Ted Staffan. *Automating Security in the Cloud: Modernizing Governance Through Secure Design*. O'Reilly. 2016. http://shop.oreilly.com/product/0636920051787.do

[Yunghans 2017]
Yunghans, Erik & Simkin, Scott. *Changing the Game in Public Cloud Security*. The SANS Institute. 2017. https://www.paloaltonetworks.com/resources/webcasts/changing-the-game-in-public-cloud-security

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	July 2019	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Overview of Risks, Threat, and Vulnerabilities Faced in Moving to the Cloud	FA8721-05-C-0003

6. AUTHOR(S)

Timothy Morrow, Kelwyn Pender, Carrie Lee, & Don Faatz

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2019-TR-004

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

As organizations develop new applications in or migrate existing applications to cloud services, they face changes in securing their information and applications. This report examines the changes to risks, threats, and vulnerabilities when applications are deployed to cloud services. Five cloud-unique threats and risks are identified along with seven threats and risks that exist on-premises and in cloud computing. For each of these threats and risks, recommendations are made for managing and mitigating the threats and risks when using cloud services.

14. SUBJECT TERMS	15. NUMBER OF PAGES
cloud services, app migration, risks, threats, vulnerabilities	27

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL