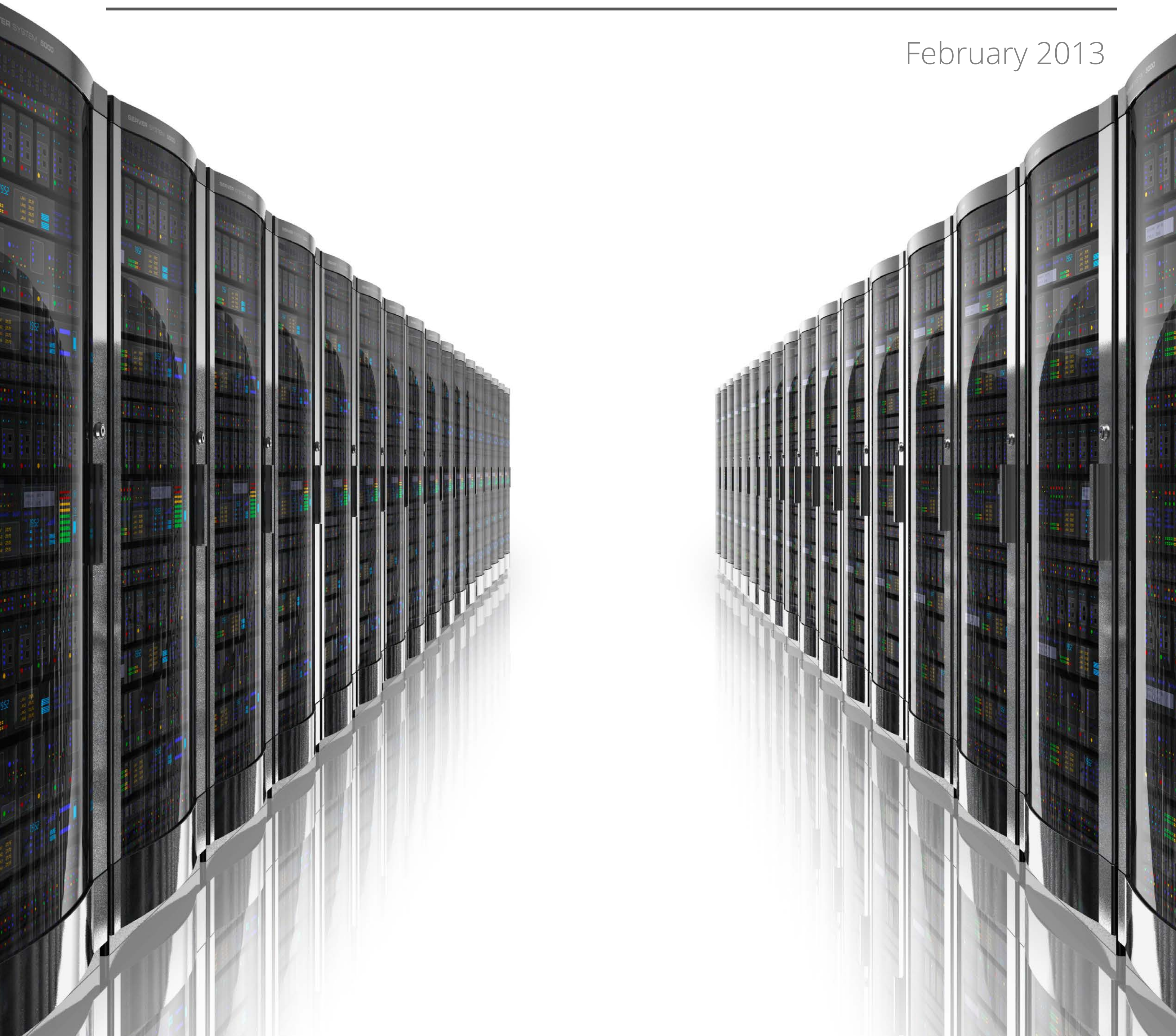
Top Threats Working Group

The Notorious Nine

Cloud Computing Top Threats in 2013

February 2013



The permanent and official location for Cloud Security Alliance Top Threats research is http://www.cloudsecurityalliance.org/topthreats.

Contents

Acknowledgments

Co-Chairs

Rafal Los, HP
Dave Shackleford, Voodoo Security
Bryan Sullivan, Microsoft

CSA Global Staff
Alex Ginsburg, Copywriter
Luciano JR Santos, Research Director
Evan Scoboria, Webmaster
Kendall Scoboria, Graphic Designer
John Yeoh, Research Analyst

The CSA Top Threats to Cloud Computing Survey in 2012 was assisted by the extended CSA Top Threats Working Group, led by committee members: Aaron Alva, Olivier Caleff, Greg Elkins, Allen Lum, Keith Pasley, Satheesh Sudarsan, Vinoth Sivasubramanian, and Rajeev Venkitaraman

Executive Summary

At an unprecedented pace, cloud computing has simultaneously transformed business and government, and created new security challenges. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from server to service-based thinking is transforming the way technology departments think about, design, and deliver computing technology and applications. Yet these advances have created new security vulnerabilities, including security issues whose full impact is still emerging.

Among the most significant security risks associated with cloud computing is the tendency to bypass information technology (IT) departments and information officers. Although shifting to cloud technologies exclusively is affordable and fast, doing so undermines important business-level security policies, processes, and best practices. In the absence of these standards, businesses are vulnerable to security breaches that can quickly erase any gains made by the switch to SaaS.

Recognizing both the promise of cloud computing, and the risks associated with it, the Cloud Security Alliance (CSA) has pioneered the creation of industry-wide standards for effective cloud security. In recent years, CSA released the "Security Guidance for Critical Areas in Cloud Computing" and the "Security as a Service Implementation Guidance." These documents have quickly become the industry-standard catalogue of best practices to secure cloud computing, comprehensively addressing this within the thirteen domains of CSA Guidance and ten categories of service associated with the SecaaS Implementation Guidance series. Already, many businesses, organizations, and governments have incorporated this guidance into their cloud strategies.

However, CSA recognizes that a central component of managing risks in cloud computing is to understand the nature of security threats. The purpose of the "The Notorious Nine: Cloud Computing Top Threats in 2013" report is to provide organizations with an up-to-date, expert-informed understanding of cloud security threats in order to make educated risk-management decisions regarding cloud adoption strategies.

The top threats report reflects the current consensus among experts about the most significant threats to cloud security. While there are many vulnerabilities to cloud security, this report focuses on threats specifically related to the shared, on-demand nature of cloud computing.

To identify the top threats, CSA conducted a survey of industry experts to compile professional opinion on the greatest vulnerabilities within cloud computing. The Top Threats working group used these survey results alongside their expertise to craft the final 2013 report. The survey methodology validated that the threat listing reflects the most current concerns of the industry. In this most recent edition of this report, experts identified the following nine critical threats to cloud security (ranked in order of severity):

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service

6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

With descriptions and analysis of these threats, this report serves as an up-to-date threat identification guide that will help cloud users and providers make informed decisions about risk mitigation within a cloud strategy. This threat research document should be utilized in conjunction with the best practices guides, "Security Guidance for Critical Areas in Cloud Computing V.3" and "Security as a Service Implementation Guidance." Together, these documents will offer valuable guidance during the formation of comprehensive, appropriate cloud security strategies.

1.0 Top Threat: Data Breaches

It's every CIO's worst nightmare: the organization's sensitive internal data falls into the hands of their competitors. While this scenario has kept executives awake at night long before the advent of computing, cloud computing introduces significant new avenues of attack. In November 2012, researchers from the University of North Carolina, the University of Wisconsin and RSA Corporation released a paper describing how a virtual machine could use side channel timing information to extract private cryptographic keys being used in other virtual machines on the same physical server. However, in many cases an attacker wouldn't even need to go to such lengths. If a multitenant cloud service database is not properly designed, a flaw in one client's application could allow an attacker access not only to that client's data, but every other client's data as well.

1.1 Implications

Unfortunately, while data loss and data leakage are both serious threats to cloud computing, the measures you put in place to mitigate one of these threats can exacerbate the other. You may be able to encrypt your data to reduce the impact of a data breach, but if you lose your encryption key, you'll lose your data as well. Conversely, you may decide to keep offline backups of your data to reduce the impact of a catastrophic data loss, but this increases your exposure to data breaches.

1.2 Controls

CCM DG-04: Data Governance - Retention Policy
CCM DG-05: Data Governance - Secure Disposal
CCM DG-06: Data Governance - Non-Production Data
CCM DG-07: Data Governance - Information Leakage
CCM DG-08: Data Governance - Risk Assessments
CCM IS-18: Information Security - Encryption
CCM IS-19: Information Security - Encryption Key Management
CCM SA-02: Security Architecture - User ID Credentials
CCM SA-03: Security Architecture - Data Security/Integrity
CCM SA-06: Security Architecture - Production/Non-Production Environments
CCM SA-07: Security Architecture - Remote User Multi-Factor Authentication

1.3 Links

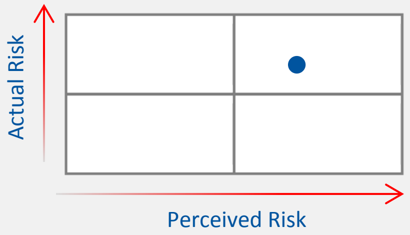
1. Cross-VM Side Channels and Their Use to Extract Private Keys
http://www.cs.unc.edu/~yinqian/papers/crossvm.pdf

2. Multi-Tenant Data Architecture
http://msdn.microsoft.com/en-us/library/Aa479086

SERVICE MODEL

IaaS PaaS SaaS

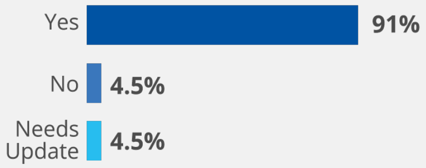
RISK MATRIX



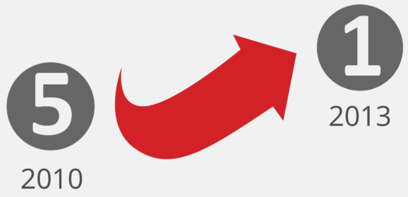
RISK ANALYSIS

CIANA: Confidentiality
STRIDE: Information Disclosure

IS THREAT STILL RELEVANT?



TOP THREAT RANKING



CSA REFERENCE

Domain 5: Information Management and Data Security
Domain 10: Application Security
Domain 12: Identity, Entitlement and Access Management
Domain 13: Virtualization

2.0 Top Threat: Data Loss

For both consumers and businesses, the prospect of permanently losing one's data is terrifying. Just ask Mat Honan, writer for Wired magazine: in the summer of 2012, attackers broke into Mat's Apple, Gmail and Twitter accounts. They then used that access to erase all of his personal data in those accounts, including all of the baby pictures Mat had taken of his 18-month-old daughter.

Of course, data stored in the cloud can be lost due to reasons other than malicious attackers. Any accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customers' data unless the provider takes adequate measures to backup data. Furthermore, the burden of avoiding data loss does not fall solely on the provider's shoulders. If a customer encrypts his or her data before uploading it to the cloud, but loses the encryption key, the data will be lost as well.

2.1 Implications

Under the new EU data protection rules, data destruction and corruption of personal data are considered forms of data breaches and would require appropriate notifications.

Additionally, many compliance policies require organizations to retain audit records or other documentation. If an organization stores this data in the cloud, loss of that data could jeopardize the organization's compliance status.

2.2 Controls

CCM DG-04: Data Governance - Retention Policy
CCM DG-08: Data Governance - Risk Assessments
CCM RS-05: Resiliency - Environmental Risks
CCM RS-06: Resiliency - Equipment Location

2.3 Links

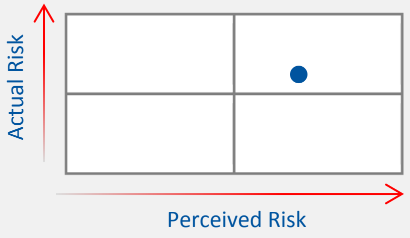
1. Cloud Computing Users Are Losing Data, Symantec Finds
http://news.investors.com/technology/011613-640851-cloud-computing-data-loss-high-in-symantec-study.htm

2. Kill the Password: Why a String of Characters Can't Protect Us Anymore
http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/

SERVICE MODEL

IaaS	PaaS	SaaS

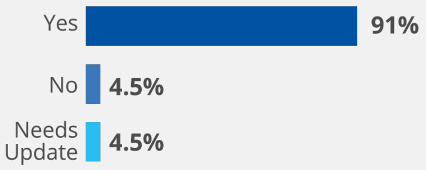
RISK MATRIX



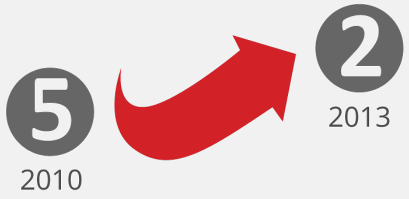
RISK ANALYSIS

CIANA: Availability, Non-Repudiation
STRIDE: Repudiation, Denial of Service

IS THREAT STILL RELEVANT?



TOP THREAT RANKING



CSA REFERENCE

Domain 5: Information Management and Data Security
Domain 10: Application Security
Domain 12: Identity, Entitlement and Access Management
Domain 13: Virtualization

3.0 Top Threat: Account or Service Traffic Hijacking

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

In April 2010, Amazon experienced a Cross-Site Scripting (XSS) bug that allowed attackers to hijack credentials from the site. In 2009, numerous Amazon systems were hijacked to run Zeus botnet nodes.

3.1 Implications

Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be aware of these techniques as well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach. Organizations should look to prohibit the sharing of account credentials between users and services, and leverage strong two-factor authentication techniques where possible.

3.2 Controls

CCM IS-07: Information Security - User Access Policy
CCM IS-08: Information Security - User Access Restriction/Authorization
CCM IS-09: Information Security - User Access Revocation
CCM IS-10: Information Security - User Access Reviews
CCM IS-22: Information Security - Incident Management
CCM SA-02: Security Architecture - User ID Credentials
CCM SA-07: Security Architecture - Remote User Multi-Factor Authentication
CCM SA-14: Security Architecture - Audit Logging / Intrusion Detection

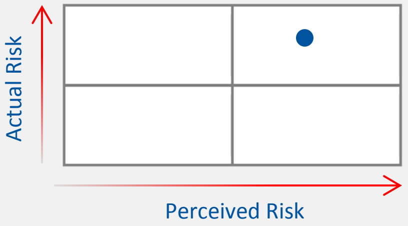
3.3 Links

1. Amazon purges account hijacking threat from site
http://www.theregister.co.uk/2010/04/20/amazon_website_treat/

SERVICE MODEL

IaaS | PaaS | SaaS

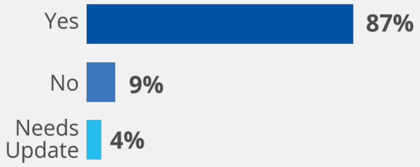
RISK MATRIX



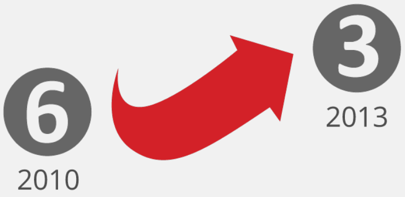
RISK ANALYSIS

CIANA: Authenticity, Integrity, Confidentiality, Non-repudiation, Availability
STRIDE: Tampering with Data, Repudiation, Information Disclosure, Elevation of Privilege, Spoofing Identity

IS THREAT STILL RELEVANT?



TOP THREAT RANKING



2. Zeus bot found using Amazon's EC2 as C&C Server
http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/

CSA REFERENCE

Domain 2: Governance and Enterprise Risk Management
Domain 5: Information Management and Data Security
Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
Domain 9: Incident Response
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management

4.0 Top Threat: Insecure Interfaces and APIs

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third-parties in order to enable their agency.

4.1 Implications

While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

4.2 Controls

CCM IS-08: Information Security - User Access Restriction/Authorization
CCM SA-03: Security Architecture - Data Security/Integrity
CCM SA-04: Security Architecture - Application Security

4.3 Links

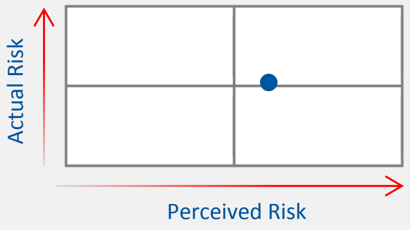
1. Insecure API Implementations Threaten Cloud
http://www.darkreading.com/cloud-security/167901092/security/application-security/232900809/insecure-api-implementations-threaten-cloud.html

2. Web Services Single Sign-On Contains Big Flaws
http://www.darkreading.com/authentication/167901072/security/news/232602844/web-services-single-sign-on-contain-big-flaws.html

SERVICE MODEL

IaaS PaaS SaaS

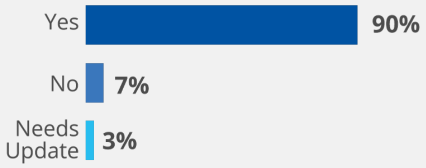
RISK MATRIX



RISK ANALYSIS

CIANA: Authenticity, Integrity, Confidentiality
STRIDE: Tampering with Data, Repudiation, Information Disclosure, Elevation of Privilege

IS THREAT STILL RELEVANT?



TOP THREAT RANKING

2
2010
4
2013

CSA REFERENCE

Domain 5: Information Management and Data Security
Domain 6: Interoperability and Portability
Domain 9: Incident Response
Domain 10: Application Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management

5.0 Top Threat: Denial of Service

Simply put, denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications. By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker (or attackers, as is the case in distributed denial-of-service (DDoS) attacks) causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding.

While DDoS attacks tend to generate a lot of fear and media attention (especially when the perpetrators are acting out of a sense of political "hactivism"), they are by no means the only form of DoS attack. Asymmetric application-level DoS attacks take advantage of vulnerabilities in web servers, databases, or other cloud resources, allowing a malicious individual to take out an application using a single extremely small attack payload – in some cases less than 100 bytes long.

5.1 Implications

Experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock: there's no way to get to your destination, and nothing you can do about it except sit and wait. As a consumer, service outages not only frustrate you, but also force you to reconsider whether moving your critical data to the cloud to reduce infrastructure costs was really worthwhile after all. Even worse, since cloud providers often bill clients based on the compute cycles and disk space they consume, there's the possibility that an attacker may not be able to completely knock your service off of the net, but may still cause it to consume so much processing time that it becomes too expensive for you to run and you'll be forced to take it down yourself.

5.2 Controls

CCM IS-04: Information Security - Baseline Requirements
CCM OP-03: Operations Management - Capacity/Resource Planning
CCM RS-07: Resiliency - Equipment Power Failures
CCM SA-04: Security Architecture - Application Security

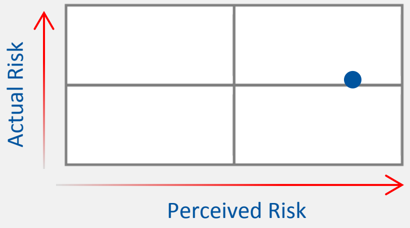
5.3 Links

1. As Cloud Use Grows, So Will Rate of DDoS Attacks
http://www.infoworld.com/d/cloud-computing/cloud-use-grows-so-will-rate-of-ddos-attacks-211876

SERVICE MODEL

IaaS | PaaS | SaaS

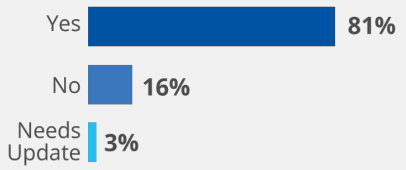
RISK MATRIX



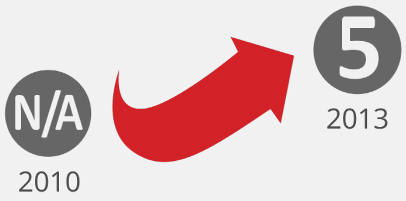
RISK ANALYSIS

CIANA: Availability
STRIDE: Denial of Service

IS THREAT STILL RELEVANT?



TOP THREAT RANKING



CSA REFERENCE

Domain 8: Data Center Operations
Domain 9: Incident Response
Domain 10: Application Security
Domain 13: Virtualization
Domain 14: Security as a Service

2. Computerworld: DDoS is Cloud's security Achilles heel (September 16, 2011)
http://www.computerworld.com.au/article/401127/ddos_cloud_security_achilles_heel/

3. OWASP: Application Denial of Service
https://www.owasp.org/index.php/Application_Denial_of_Service

4. Radware DDoSpedia
http://security.radware.com/knowledge-center/DDoSPedia/

6.0 Top Threat: Malicious Insiders

The risk of malicious insiders has been debated in the security industry. While the level of threat is left to debate, the fact that the insider threat is a real adversary is not.

CERN defines an insider threat as such:[1]

"A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

6.1 Implications

A malicious insider, such as a system administrator, in an improperly designed cloud scenario can have access to potentially sensitive information.

From IaaS to PaaS and SaaS, the malicious insider has increasing levels of access to more critical systems, and eventually to data. Systems that depend solely on the cloud service provider (CSP) for security are at great risk here. Even if encryption is implemented, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack.

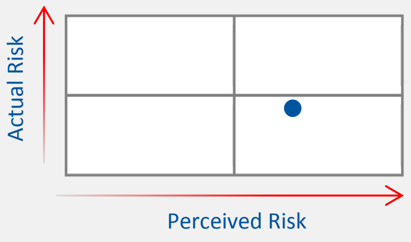
6.2 Controls

CCM CO-03: Compliance - Third Party Audits
CCM DG-01: Data Governance - Ownership / Stewardship
CCM DG-03: Data Governance - Handling / Labeling / Security Policy
CCM DG-07: Data Governance - Information Leakage
CCM FS-02: Facility Security - User Access
CCM FS-05: Facility Security - Unauthorized Persons Entry
CCM FS-06: Facility Security - Off-Site Authorization
CCM HR-01: Human Resources Security - Background Screening
CCM IS-06: Information Security - Policy Enforcement
CCM IS-08: Information Security - User Access Restriction / Authorization
CCM IS-10: Information Security - User Access Reviews
CCM IS-13: Information Security - Roles / Responsibilities
CCM IS-15: Information Security - Segregation of Duties
CCM IS-18: Information Security - Encryption

SERVICE MODEL

IaaS PaaS SaaS

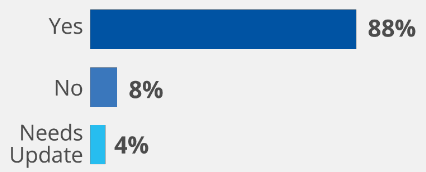
RISK MATRIX



RISK ANALYSIS

STRIDE: Spoofing, Tampering, Information Disclosure

IS THREAT STILL RELEVANT?



TOP THREAT RANKING

3
2010
6
2013

[1] http://www.cert.org/insider_threat/

CCM IS-19: Information Security - Encryption Key Management
CCM IS-29: Information Security - Audit Tools Access
CCM RI-02: Risk Management - Assessments
CCM SA-09: Security Architecture - Segmentation

6.3 Links

1. Insider threats to cloud computing
http://www.cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/

2. Cloud's privileged identity gap intensifies insider threats
http://www.darkreading.com/insider-threat/167801100/security/news/240146276/cloud-s-privileged-identity-gap-intensifies-insider-threats.html

CSA REFERENCE

Domain 2: Governance and Enterprise Risk Management
Domain 5: Information Management and Data Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement and Access Management

7.0 Top Threat: Abuse of Cloud Services

One of cloud computing's greatest benefits is that it allows even small organizations access to vast amounts of computing power. It would be difficult for most organizations to purchase and maintain tens of thousands of servers, but renting time on tens of thousands of servers from a cloud computing provider is much more affordable. However, not everyone wants to use this power for good. It might take an attacker years to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes. Alternately, he might use that array of cloud servers to stage a DDoS attack, serve malware or distribute pirated software.

7.1 Implications

This threat is more of an issue for cloud service providers than cloud consumers, but it does raise a number of serious implications for those providers. How will you detect people abusing your service? How will you define abuse? How will you prevent them from doing it again?

7.2 Controls

CCM IS-24: Information Security - Incident Response Legal Preparation
CCM IS-26: Information Security - Acceptable Use

7.3 Links

1. Cross-VM Side Channels and Their Use to Extract Private Keys
http://www.cs.unc.edu/~yinqian/papers/crossvm.pdf

2. Pirate Bay Ditches Servers and Switches to the Cloud
http://news.cnet.com/8301-1023_3-57534707-93/pirate-bay-ditches-servers-and-switches-to-the-cloud/

SERVICE MODEL

IaaS PaaS SaaS

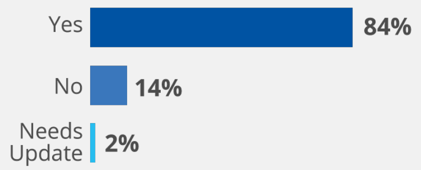
RISK MATRIX

N/A

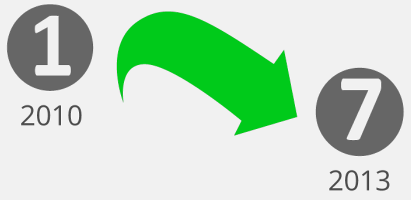
RISK ANALYSIS

CIANA: N/A
STRIDE: N/A

IS THREAT STILL RELEVANT?



TOP THREAT RANKING



CSA REFERENCE

Domain 2: Governance and Enterprise Risk Management
Domain 9: Incident Response

8.0 Top Threat: Insufficient Due Diligence

Cloud computing has brought with it a gold rush of sorts, with many organizations rushing into the promise of cost reductions, operational efficiencies and improved security. While these can be realistic goals for organizations that have the resources to adopt cloud technologies properly, too many enterprises jump into the cloud without understanding the full scope of the undertaking.

Without a complete understanding of the CSP environment, applications or services being pushed to the cloud, and operational responsibilities such as incident response, encryption, and security monitoring, organizations are taking on unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks.

8.1 Implications

An organization that rushes to adopt cloud technologies subjects itself to a number of issues. Contractual issues arise over obligations on liability, response, or transparency by creating mismatched expectations between the CSP and the customer. Pushing applications that are dependent on “internal” network-level security controls to the cloud is dangerous when those controls disappear or do not match the customer’s expectation. Unknown operational and architectural issues arise when designers and architects unfamiliar with cloud technologies are designing applications being pushed to the cloud.

The bottom line for enterprises and organizations moving to a cloud technology model is that they must have capable resources, and perform extensive internal and CSP due-diligence to understand the risks it assumes by adopting this new technology model.

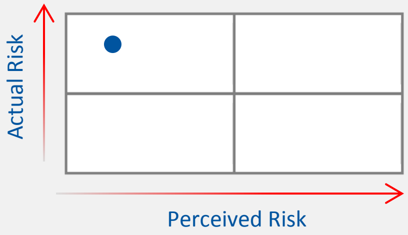
8.2 Controls

CCM DG-08: Data Governance - Risk Assessments
CCM IS-04: Information Security - Baseline Requirements
CCM IS-12: Information Security - Industry Knowledge / Benchmarking
CCM OP-03: Operations Management - Capacity / Resource Planning
CCM RI-01: Risk Management - Program
CCM RI-02: Risk Management - Assessments
CCM RS-01: Resiliency - Management Program
CCM RS-02: Resiliency - Impact Analysis
CCM RS -03: Resiliency - Business Continuity Planning
CCM SA-03: Security Architecture - Data Security / Integrity
CCM SA-04: Security Architecture - Application Security

SERVICE MODEL

IaaS PaaS SaaS

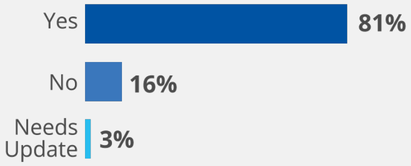
RISK MATRIX



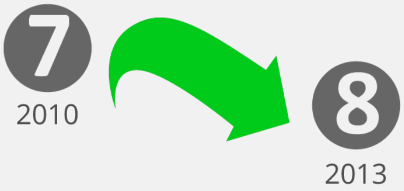
RISK ANALYSIS

STRIDE: All

IS THREAT STILL RELEVANT?



TOP THREAT RANKING



CSA REFERENCE

Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal and Electronic Discovery
Domain 8: Data Center Operations
Domain 9: Incident Response, Notification and Remediation

CCM SA-08: Security Architecture - Network Security

CCM SA-09: Security Architecture - Segmentation

8.3 Links

1. Perfecting the unknown: Cloud Computing
http://www.mysanantonio.com/business/article/Perfecting-the-Unknown-Cloud-Computing-4157844.php

9.0 Top Threat: Shared Technology Vulnerabilities

Cloud service providers deliver their services in a scalable way by sharing infrastructure, platforms, and applications. Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models. A defensive in-depth strategy is recommended and should include compute, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud.

9.1 Implications

A compromise of an integral piece of shared technology such as the hypervisor, a shared platform component, or an application in a SaaS environment exposes more than just the compromised customer; rather, it exposes the entire environment to a potential of compromise and breach. This vulnerability is dangerous because it potentially can affect an entire cloud at once.

9.2 Controls

CCM DG-03: Data Governance - Handling / Labeling / Security Policy
CCM IS-04: Information Security - Baseline Requirements
CCM IS-07: Information Security - User Access Policy
CCM IS-15: Information Security - Segregation of Duties
CCM IS-18: Information Security - Encryption
CCM IS-20: Information Security - Vulnerability / Patch Management
CCM SA-02: Security Architecture - User ID Credentials
CCM SA-09: Security Architecture - Segmentation
CCM SA-11: Security Architecture - Shared Networks
CCM SA-14: Security Architecture - Audit Logging / Intrusion Detection

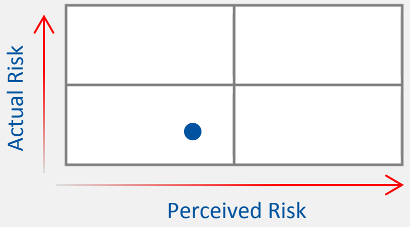
9.3 Links

1. New virtualization vulnerability allows escape to hypervisor attacks
http://www.informationweek.com/security/application-security/new-virtualization-vulnerability-allows/240001996

SERVICE MODEL

IaaS PaaS SaaS

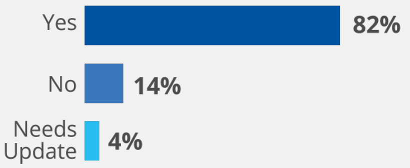
RISK MATRIX



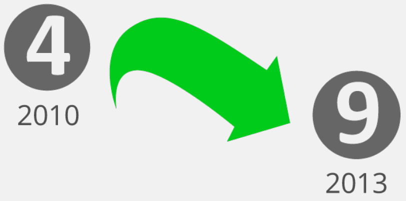
RISK ANALYSIS

STRIDE: Information Disclosure, Elevation of Privilege

IS THREAT STILL RELEVANT?



TOP THREAT RANKING



CSA REFERENCE

Domain 1: Cloud computing architectural framework
Domain 5: Information management and data security
Domain 11: Encryption and key management
Domain 12: Identity, entitlement, and access management
Domain 13: Virtualization