Top Threats to Cloud Computing

The Egregious 11

cloud security alliance®

Table of Contents

Acknowledgments

Co-Chairs

Jon-Michael C. Brook

Contributors

Jon-Michael Brook
Alexander Getsin
Greg Jensen
Laurie Jameson
Michael Roza
Neha Thethi
Ashish Kurmi
Shachaf Levy
Shira Shamban
Vic Hargrave
Victor Chin
Zoran Lalic
Randall Brooks

Cloud Security Alliance Global Staff

Victor Chin
Stephen Lumpe (Cover Art)
AnnMarie Ulskey (Design)

Executive Summary

The *Top Threats* reports have traditionally aimed to raise awareness of threats, risks and vulnerabilities in the cloud. Such issues are often the result of the shared, on-demand nature of cloud computing. In this fourth installment, we again surveyed 241 industry experts on security issues in the cloud industry. This year our respondents rated 11 salient threats, risks and vulnerabilities in their cloud environments. The *Top Threats Working Group* used the survey results along with its expertise to create the final 2019 report.

The latest report highlights the *Egregious Eleven* (ranked in order of significance per survey results with applicable previous rankings):

1. Data Breaches
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking
6. Insider Threat
7. Insecure Interfaces and APIs
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services

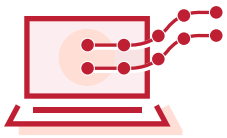
Observations and Rationale

After analyzing the responses in this survey, we noticed a drop in ranking of traditional cloud security issues under the responsibility of cloud service providers (CSPs). Concerns such as denial of service, shared technology vulnerabilities, and CSP data loss and system vulnerabilities—which all featured in the previous *Treacherous 12*—were now rated so low they have been excluded in this report. These omissions suggest that traditional security issues under the responsibility of the CSP seem to be less of a concern. Instead, we're seeing more of a need to address security issues that are situated higher up the technology stack that are the result of senior management decisions.

New, highly rated items in the survey are more nuanced and suggest a maturation of the consumer's understanding of the cloud. These issues are inherently specific to the cloud and thus indicate a technology landscape where consumers are actively considering cloud migration. Such topics refer to potential control plane weaknesses, metastructure and applistructure failures, and limited cloud visibility. This new emphasis is markedly different from more generic threats, risks and vulnerabilities (i.e. data loss, denial of service) that featured more strongly in previous *Top Threats* reports.

We hope this document raises organizational awareness of the top security issues and their mitigations —and ensures that they are taken into consideration when budgeting for cloud migration and security. The report provides controls recommendations and reference examples that are meant to be of use to compliance, risk, and technology staff. Executive management will also benefit from exposition technology trends and overviews in the report.

Security Issue: Data Breaches



A data breach is a cybersecurity incident where sensitive, protected or confidential information is released, viewed, stolen or used by an unauthorized individual. A data breach may be the primary objective of a targeted attack or merely the result of human error, application vulnerabilities or inadequate security practices. A data breach involves any kind of information that was not intended for public release, including—but not limited to—personal health information, financial information, personally identifiable information (PII), trade secrets and intellectual property.

SECURITY RESPONSIBILITY

- ☒ Customer
- ☒ Cloud Service Provider
- ☑ Both

ARCHITECTURE

- ☑ Infra
- ☑ Meta
- ☑ Info
- ☑ Appli

CLOUD SERVICE MODEL

- ☑ Software as a service (SaaS)
- ☑ Platform as a service (PaaS)
- ☑ Infrastructure as a service (IaaS)

Business Impact

Negative consequences of a data breach may include:

1. Impact to reputation and trust of customers or partners
2. Loss ofintellectual property (IP) to competitors, which may impact products release
3. Regulatory implications that may result in monetary loss
4. Brand impact which may cause a market value decrease due to (due to previously listed reasons)
5. Legal and contractual liabilities
6. Financial expenses incurred due to incident response and forensics

There are cases of data breaches being undetected until months after the compromise. In such incidents, the implications might not be immediately apparent (e.g., IP theft). For example, the United States Office of Personnel Management (OPM) and Sony Pictures breach both had a dwell time of approximately one year[1].

Key Takeaways

1. Data is becoming the main target of cyber attacks. Defining the business value of data and the impact of its loss is essential important for organizations that own or process data.
2. Protecting data is evolving into a question of who has access to it
3. Data is accessible via the internet is the most vulnerable asset to mis-configuration or exploitation.
4. Encryption techniques can help protect data, but negatively impacts system performance while making applications less user-friendly
5. A robust and well tested incident response plan that considers the CSP and data privacy laws will help data breach victims recover.

[1] Improving Cyber Resiliency https://cloudsecurityalliance.org/artifacts/improving-metrics-in-cyber-resiliency/

Anecdotes and Examples

- Timehop had a data breach that affected 21 million users because of a cloud computing environment compromise. Social media access tokens were also compromised.
- Uber disclosed that its Amazon Web Services (AWS) account was hacked in late 2016, compromising the personal information of 57 million users worldwide.
- In 2019, Voipo, a telecoms company that provides Voice over Internet Protocol (VoIP) services, exposed millions of customer call logs, short message service (SMS) logs and credentials. The database was exposed on June 2018 and contained call and message logs dating back to May 2015. Many of the files contained detailed call records (i.e., who called whom, time of call, etc.). In total, Voipo exposed "7 million call logs, 6 million text messages and other internal documents containing unencrypted passwords that— if used—could allow an attacker to gain deep access to the company's systems.

CSA Security Guidance

Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal Issues, Contracts and Electronic Discovery
Domain 4: Compliance and Audit Management
Domain 5: Information Governance
Domain 6: Management Plane and Business Continuity
Domain 9: Incident Response
Domain 11: Data Security and Encryption
Domain 12: Identity Entitlement and Access Management
Domain 14: Related Technologies

CCM Controls

AIS Application and Interface Security
AIS-01: Application Security
AIS-02: Customer Access Requirements
AIS-03: Data Integrity
AIS-04: Data Security / Integrity

CCC Change Control and Configuration Management
CCC-05: Production Changes

DSI Data Security and Information Lifecycle Management
DSI-01: Classification
DSI-02: Data Inventory / Flows
DSI-03: Ecommerce Transactions
DSI-04: Handling / Labeling / Security Policy
DSI-05: Non-Production Data
DSI-07: Secure Disposal

EKM Encryption and Key Management
EKM-01: Entitlement
EKM-02: Key Generation
EKM-03: Sensitive Data Protection
EKM-04: Storage and Access

GRM Governance and Risk Management
GRM-02: Data Focus Risk Assessments
GRM-06: Policy
GRM-10: Risk Assessments

IAM Identity and Access Management
IAM-01: Audit Tools Access
IAM-04: Policies and Procedures

THREAT ANALYSIS

- ☒ Spoofing Identity
- ☒ Tampering with Data
- ☒ Repudiation
- ☑ Information Disclosure
- ☒ Denial of Service
- ☒ Elevation of Privilege

LINKS AND REFERENCES

1. *Timehop Security Incident, July 4, 2018:* https://www.timehop.com/security/
2. *Uber Discloses Year-Old AWS Data Breach, Exposing Millions of Users:* https://awsinsider.net/articles/2017/11/21/uber-aws-data-breach.aspx
3. *Amazon hit with major data breach days before Black Friday:* https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-data-breach-days-before-black-friday
4. *VOIPO database exposed millions of call and SMS logs, system data:* https://www.zdnet.com/article/voipo-database-exposed-millions-of-call-and-sms-logs-system-data/

Security Issue: Misconfiguration and Inadequate Change Control

Misconfiguration occurs when computing assets are set up incorrectly, often leaving them vulnerable to malicious activity. Some common examples include unsecured data storage elements or containers; excessive permissions; default credentials and configuration settings left unchanged; standard security controls disabled; unpatched systems and logging or monitoring disabled and unrestricted access to ports and services. Misconfiguration of cloud resources is a leading cause of data breaches and could allow deletion or modification of resources and service interruption.

SECURITY RESPONSIBILITY

- ☑ Customer
- ☒ Cloud Service Provider
- ☒ Both

ARCHITECTURE

- ☑ Infra
- ☑ Meta
- ☑ Info
- ☑ Appli

CLOUD SERVICE MODEL

- ☑ Software as a Service (SaaS)
- ☑ Platform as a Service (PaaS)
- ☑ Infrastructure as a Service (IaaS)

An absence of effective change control is a common cause of misconfiguration in a cloud environment. Cloud environments and cloud computing methodologies differ from traditional information technology (IT) in ways that make changes more difficult to control. Traditional change processes involved multiple roles and approvals and could take days or weeks to reach production. Infrastructure elements that were static in the corporate data center are now abstracted to software in the cloud, and their entire lifecycle may only be a matter of minutes or seconds. Cloud computing techniques rely on automation, expansion of roles and access to support rapid change. Using multiple cloud providers adds complexity, as each provider has unique capabilities which are enhanced and expanded almost daily. This dynamic environment requires an agile and proactive approach to change control and remediation that many companies have not yet mastered.

Business Impact

The business impact of a misconfigured item can be severe depending on the nature of the misconfiguration and how quickly it is detected and mitigated. The most commonly reported effect is the exposure of data stored in cloud repositories.

Key Takeaways

1. Cloud-based resources are highly complex and dynamic, making themit challenging to configure.
2. Traditional controls and change management approaches are not effective in the cloud.
3. Companies should embrace automation and employ technologies that scan continuously for misconfigured resources and remediate problems in real time.

Anecdotes and Examples

Recent examples of issues related to misconfiguration and inadequate change control include:

1. A misconfigured AWS Simple Storage Service (S3) cloud storage bucket exposed detailed and private data of 123 million American households. The data set belonged to Experian, a credit bureau, which sold the data to an online marketing and data analytics company called Alteryx. It was Alteryx that exposed the file.
2. An unsecured Elasticsearch database owned by Exactis resulted in another massive breach containing highly personal data of 230 million U.S. consumers. The database server was configured to be publicly accessible.
3. Level One Robotics, an engineering company specializing in automation process and assembly, exposed highly sensitive proprietary information belonging to more than 100 manufacturing companies, including Volkswagen, Chrysler, Ford, Toyota, General Motors, Tesla and ThyssenKrupp. In this case, the misconfigured asset was an rsync (backup) server that allowed unauthenticated data transfer to any rsync client.

CSA Security Guidance

Domain 4: Compliance and Audit Management
Domain 5: Information Governance
Domain 6: Management Plane and Business Continuity
Domain 7: Infrastructure Security
Domain 8: Virtualization and Containers
Domain 10: Application Security
Domain 11: Data Security and Encryption
Domain 12: Identity, Entitlement, and Access Management

CCM Controls

AIS Application and Interface Security
AIS-01: Application Security
AIS-04: Data Security / Integrity

CCC Change Control and Configuration Management
CCC-02: Outsourced Development
CCC-03: Quality Testing
CCC-05: Production Changes

DSI Data Security and Information Lifecycle Management
DSI-01: Classification
DSI-04: Handling / Labeling / Security Policy

EKM Encryption and Key Management
EKM-03: Sensitive Data Protection
EKM-04: Storage and Access

GRM Governance and Risk Management
GRM-01: Baseline Requirements
GRM-02: Data Focus Risk Assessments

HRS Human Resources
HRS-09: Training / Awareness

IAM Identity and Access Management
IAM-02: Credential Lifecycle / Provision Management
IAM-05: Segregation of Duties

IVS Infrastructure and Virtualization Security

IVS-02: Change Detection
IVS-06: Network Security
IVS-07: OS Hardening and Base Controls
IVS-06: Network Security
IVS-07: OS Hardening and Base Controls

THREAT ANALYSIS	LINKS AND REFERENCES
☒ Spoofing Identity ☑ Tampering with Data ☑ Repudiation ☑ Information Disclosure ☑ Denial of Service ☒ Elevation of Privilege	1. *120 Million American Households Exposed in 'Massive' ConsumerView Database Leak:* https://www.forbes.com/sites/thomasbrewster/2017/12/19/120m-american-households-exposed-in-massive-consumerview-database-leak/#37bb94d27961 2. *Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records:* https://www.wired.com/story/exactis-database-leak-340-million-records/ 3. *Short Circuit: How a Robotics Vendor Exposed Confidential Data for Major Manufacturing Companies:* https://www.upguard.com/breaches/short-circuit-how-a-robotics-vendor-exposed-confidential-data-for-major-manufacturing-companies

Security Issue: Lack of Cloud Security Architecture and Strategy

Worldwide, organizations are migrating portions— of their IT infrastructure to public clouds. One of the biggest challenges during this transition is the implementation of appropriate security architecture to withstand cyber attacks. Unfortunately, this process is still a mystery for many organizations. Data is exposed to different threats when organizations assume that cloud migration is a "lift-and-shift" endeavor of simply porting their existing IT stack and security controls to a cloud environment. A lack of understanding of a shared security responsibility model is also another contributing factor.

Furthermore, the functionality and speed of migration often take precedence over security. These factors lead to a lack of security architecture and strategy in the cloud—leaving organizations vulnerable to successful cyber-attacks. Implementing security architecture and developing a robust security strategy will provide organizations with a strong foundation to operate and conduct business activities in the cloud. Leveraging cloud native tools to increase visibility in cloud environments will also minimize risk and cost. Such precautions, if taken, will significantly reduce the risk of compromise.

SECURITY RESPONSIBILITY

- ☑ Customer
- ☒ Cloud Service Provider
- ☒ Both

ARCHITECTURE

- ☑ Infra
- ☒ Meta
- ☒ Info
- ☒ Appli

CLOUD SERVICE MODEL

- ☒ Software as a Service (SaaS)
- ☑ Platform as a Service (PaaS)
- ☑ Infrastructure as a Service (IaaS)

Business Impact

No matter how big or small the enterprise, proper security architecture and strategy are required elements for securely moving, deploying, and operating in the cloud. Successful cyberattacks can have a severe impact on businesses, including financial loss, reputational damage, legal repercussions, and fines.

Key Takeaways

1. Ensure security architecture aligns with business goals and objectives.
2. Develop and implement a security architecture framework
3. Ensure the threat model is continuously kept up to date.
4. Bring continuous visibility into the actual security posture

Anecdotes and Examples

Recent examples of issues related to a lack of cloud security architecture and strategy include:

- Technology and cloud giant Accenture recently confirmed it inadvertently left a massive store of private data across four unsecured cloud servers, exposing highly sensitive passwords and secret decryption keys that could have inflicted considerable damage on the company and its customers. The servers, hosted on Amazon's S3 storage service, contained hundreds of gigabytes of data for the company's enterprise cloud offering, which the company said provides support to the majority of the *Fortune 100* companies. The data could be downloaded without a password by anyone who knew the servers' web addresses.
- Researchers at Kromtech Security Center discovered a trove of data belonging to the Honda Connect App, which was exposed online. The data was stored on two unsecured, publicly accessible and unprotected Amazon AWS S3 Buckets.

CSA Security Guidance

Domain 1: Cloud Computing Concepts and Architectures
Domain 6: Management Plane and Business Continuity
Domain 7: Infrastructure Security

CCM Controls

AIS Application and Interface Security
AIS-04: Data Security / Integrity

GRM Governance and Risk Management
GRM-01: Baseline Requirements
GRM-02: Data Focused Risk Assessments
GRM-05: Management Support/Involvement
GRM-08: Management Policy

IAM Identity and Access Management
IAM-02: Credential Lifecycle / Provision Management

IVS Infrastructure and Virtualization Security
IVS-06: Network Security
IVS-08: Production / Non-Production Environments
IVS-09: Segmentation
IVS-13: Network Architecture

STA Supply Chain Management, Transparency, and Accountability
STA-03: Network / Infrastructure Services
STA-05: Supply Chain Agreements

THREAT ANALYSIS

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

LINKS AND REFERENCES

1. *Introduction to Cloud Security Architecture from a Cloud Consumer's Perspective:* https://www.infoq.com/articles/cloud-security-architecture-intro
2. *The New Shared Responsibility Model For Cloud Security:* https://www.forbes.com/sites/forbestechcouncil/2018/10/15/the-new-shared-responsibility-model-for-cloud-security/#508d0f422490
3. *The Importance of a Defined Cloud Strategy:* https://www.expedient.com/blog/the-importance-of-a-defined-cloud-strategy/
4. *Accenture left a huge trove of highly sensitive data on exposed servers:* https://www.zdnet.com/article/accenture-left-a-huge-trove-of-client-passwords-on-exposed-servers/
5. *The Consequences of a Cyber Security Breach:* https://www.sungardas.com/en/about/resources/articles/the-consequences-of-a-cyber-security-breach/
6. *Why Enterprise Architecture Deserves a Seat at the Security Table:* https://erwin.com/blog/enterprise-architecture-seat-security-table/
7. *Personal data of over 50,000 Honda Connect App leaked:* https://www.hackread.com/personal-data-of-over-50000-honda-connect-app-leaked/

Security Issue: Insufficient Identity, Credential, Access and Key Management

SECURITY RESPONSIBILITY
☑ Customer
☒ Cloud Service Provider
☒ Both

ARCHITECTURE
☑ Infra
☒ Meta
☒ Info
☒ Appli

CLOUD SERVICE MODEL
☒ Software as a Service (SaaS)
☑ Platform as a Service (PaaS)
☑ Infrastructure as a Service (IaaS)

Identity, credential, access management systems include tools and policies that allow organizations to manage, monitor, and secure access to valuable resources. Examples may consist of electronic files, computer systems, and physical resources, such as server rooms and buildings.

Cloud computing introduces multiple changes to traditional internal system management practices related to identity and access management (IAM). It isn't that these are necessarily new issues. Rather, they are more significant issues when dealing with the cloud because cloud computing profoundly impacts identity, credential, and access management. In both public and private cloud settings, CSPs and cloud consumers are required to manage IAM without compromising security.

Security incidents and data breaches can occur due to inadequate protection of credentials; a lack of regular automated rotation of cryptographic keys, passwords and certificates; a lack of scalable identity, credential, and access management systems; a failure to use multifactor authentication; and failure to use strong passwords.

Credentials and cryptographic keys must not be embedded in source code or distributed in public-facing repositories (such as GitHub) because there is a high risk of discovery and misuse. Keys need to be appropriately secured, and a well-secured public key infrastructure (PKI) is required to ensure key-management activities are carried out.

Identity management systems must scale to handle lifecycle management for millions of users as well as CSPs. Identity management systems must support immediate de-provisioning of access to resources with personnel changes, such as job termination or role transitions. Such identity management lifecycle processes should be integrated and automated within cloud environments and accomplished a timely manner.

Identity systems are becoming increasingly interconnected, and federating identity with a cloud provider (e.g., Security Assertion Markup Language (SAML)) is becoming more prevalent to ease the burden of user maintenance. Organizations planning to federate identity with a cloud provider must understand the security around the cloud provider's identity solution, including processes, infrastructure, and segmentation between customers (in the case of a shared identity solution).

Multifactor authentication systems—smartcard, one-time password (OTP), and phone authentication, for example—should be required for users and operators of a cloud service (i.e., the cloud customer).

These Forms of authentication helps address password theft, where stolen passwords enable access to resources without user consent. Password theft can manifest in common network lateral movement attacks, such as "pass the hash."

In cases where legacy systems require the use of passwords alone, the authentication system must support policy enforcement, such as the verification of strong passwords and organizational-defined rotation period policies.

The management of cryptographic keys used to protect data at rest must occur throughout their lifecycles, including creation, distribution, storage, replacement, and deletion. Doing so helps address attacks that feature unauthorized access to keys. Stolen cryptographic keys—coupled with a lack of key rotation policy–may dramatically increase effective elapsed breach time and scope.

Any centralized storage mechanism containing data secrets (e.g., passwords, private keys, or confidential customer contact databases) is an extremely high-value target for attackers. Choosing to centralize passwords and keys is a compromise that an organization must consider carefully: the convenience of centralized key management against the threat of grouping these keys. As with any high-value asset, monitoring, and protection of identity and key management systems should be a high priority.

Business Impact

Malicious actors masquerading as legitimate users, operators or developers can read/exfiltrate, modify and delete data; issue control plane and management functions; snoop on data in transit; or release malicious software that appears to originate from a legitimate source. As a result, insufficient identity, credential, or key management can enable unauthorized access to data and potentially catastrophic damage to organizations or end-users.

Key Takeaways

1. Secure accounts, inclusive to two-factor authentication and limited use of root accounts.
2. Practice the strictest identity and access controls for cloud users and identities.
3. Segregate and segment accounts, virtual private clouds (VPCs) and identity groups based on business needs and the principle of least privilege.
4. Rotate keys, remove unused credentials and privileges, employ central and programmatic key management.

Anecdotes and Examples

Recent examples of issues related to insufficient identity, credential, access, and key management include:

- In December 2018, a German student hacked data protected by weak passwords and shared the information using a cloud platform. The 20-year-old utilized passwords such as "Iloveyou" and "1234" to hack into online accounts of hundreds of lawmakers and personalities whose political stances he disliked. German cybersecurity officials revealed

that phone numbers, text messages, photographs, credit card numbers and other data connected to 1,000 members of parliament, journalists and other public figures had been stolen, collated and spread via Twitter and other online platforms.

- Accountancy firm Deloitte experienced a major data breach due to weak identity, credential, and access management on Sept. 25, 2017, when the company announced it had detected a breach of its global email server due to a poorly secured administrator email account. The compromise occurred in March 2017, and supposedly gave attackers privileged, unrestricted access "to all areas." The administrator account required only a single password and did not employ a two-step verification process. The attackers allegedly controlled the server since October/November of 2016. Deloitte's 244,000 staff utilized the Azure cloud service provided by Microsoft to store incoming and outgoing emails. In addition to emails, the hackers may have had potential access to usernames, passwords, Internet Protocol (IP) addresses, architectural diagrams for businesses, and health information. Some emails had attachments with sensitive security and design details. Furthermore, hackers may have accessed usernames, passwords, and personal data of the organization's blue-chip clients.
- On May 31, 2017, a threat actor used OneLogin's AWS keys to gain access to the company's AWS platform via application programming interface (API) from an intermediate host with another, smaller service provider in the U.S. OneLogin, which provides identity and password management services, detected the intrusion and shut down the affected systems (and compromised AWS keys) to stop the intrusion within minutes. They also confirmed there were no other active threats.
- Attackers recently scraped GitHub for cloud service credentials and , hijacked an account to mine virtual currency. – "Cloud service provider credentials included in a GitHub project were discovered and misused within 36 hours of the project going live.
- Praetorian, an Austin, Texas-based provider of information security solutions, launched a new cloud-based platform that leverages the computing power of Amazon AWS To crack password hashes in a simple fashion.

CSA Security Guidance

Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management

CCM Controls

EKM Encryption and Key Management
EKM-01: Entitlement
EKM-02: Key Generation
EKM-03: Sensitive Data Protection
EKM-04: Storage and Access

HRS Human Resources
HRS-01: Asset Returns
HRS-03: Employment Agreements
HRS-04: Employment Termination
HRS-08: Technology Acceptable Use
HRS-09: Training / Awareness
HRS-10: User Responsibility

IAM Identity and Access Management

IAM-01: Audit Tools Access
IAM-02: Credential Lifecycle / Provision Management
IAM-03: Diagnostic / Configuration Ports Access
IAM-04: Policies and Procedures
IAM-05: Segregation of Duties
IAM-06: Source Code Access Restriction
IAM-07: Third Party Access
IAM-08: Trusted Sources
IAM-09: User Access Authorization
IAM-10: User Access Reviews
IAM-11: User Access Revocation
IAM-12: User ID Credentials
IAM-13: Utility Programs Access

THREAT ANALYSIS	LINKS AND REFERENCES
☑ Spoofing Identity ☑ Tampering with Data ☑ Repudiation ☑ Information Disclosure ☑ Denial of Service ☑ Elevation of Privilege	1. *German Man Confesses to Hacking Politicians' Data, Officials Say:* https://www.nytimes.com/2019/01/08/world/europe/germany-hacking-arrest.html 2. *German data hacker says he was 'annoyed' by politicians:* https://www.irishtimes.com/news/world/europe/german-data-hacker-says-he-was-annoyed-by-politicians-1.3751332 3. *Deloitte hit by cyber-attack revealing clients' secret emails:* https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails 4. *Deloitte breached by hackers for months:* https://blog.malwarebytes.com/security-world/2017/09/deloitte-breached-by-hackers-for-months/ 5. *Major identity manager breach exposes sensitive user info:* https://www.engadget.com/2017/06/03/major-identity-manager-breach-stole-sensitive-user-info/?guccounter=1 6. *OneLogin, May 31, 2017 Security Incident:* https://www.onelogin.com/blog/may-31-2017-security-incident 7. *System Shock: How A Cloud Leak Exposed Accenture's Business:* https://www.upguard.com/breaches/cloud-leak-accenture 8. *Quora breach leaks data on over 100 million users:* https://www.engadget.com/2018/12/03/quora-breach/ 9. *Attackers Scrape GitHub for Cloud Service Credentials, Hijack Account to Mine Virtual Currency:* http://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/ 10. *Dell Releases Fix for Root Certificate Fail:* http://www.bankinfosecurity.com/dell-releases-fix-for-root-certificate-fail-a-8701/op-1

Security Issue: Account Hijacking

Account hijacking is a threat in which malicious attackers gain access to and abuse accounts that are highly privileged or sensitive. In cloud environments, the accounts with the highest risks are cloud service accounts or subscriptions. Phishing attacks, exploitation of cloud-based systems, or stolen credentials can compromise these accounts. These threats—unique and potentially powerful—can cause significant disruption of the cloud environment, such as data and asset loss and compromised operations. These risks stem from the delivery model of cloud services, as well as that of its organization and governance: data and applications reside in cloud services, which reside in a cloud account or subscription. Subscriptions, in particular, are accessible online to anyone with privilege and credentials.

Organizations should vigorously promote an awareness of these threats and defense-in-depth protection strategies to contain breach damage.

SECURITY RESPONSIBILITY

- ☑ Customer
- ☑ Cloud Service Provider
- ☑ Both

ARCHITECTURE

- ☒ Infra
- ☑ Meta
- ☒ Info
- ☑ Appli

CLOUD SERVICE MODEL

- ☑ Software as a Service (SaaS)
- ☑ Platform as a Service (PaaS)
- ☑ Infrastructure as a Service (IaaS)

Business Impact

Account and service hijacking implies full compromise: control of the account, its services, and data within. In such a scenario, business logic, function, data, and applications reliant on the account services are at-risk.

The fallout from such compromises has been severe at times. In recent breach cases, there were significant operational and business disruptions—including examples of the complete elimination of organization assets, data, and capabilities.

Account hijacking consequences include data leaks that lead to reputational damage, brand value degradation, legal liability exposure, and sensitive personal and business information disclosures.

Key Takeaways

1. Account Hijacking is a threat that must be taken seriously
2. Defence-in-depth and IAM controls are key in mitigating account hijacking

Anecdotes and Examples

Recent examples of issues related to account hijacking include:

- In June 2014, the AWS account of Code Spaces—a former code-hosting service company—was compromised when it failed to protect its administrative console with multi-factor authentication. The business was forced to close after the destruction of its assets.
- In 2018, consumer cloud services hijacked and sold data in darknet marketplaces at commercial scale.
- 2017 marked the rise of cloud account-targeted campaigns, in particular for Microsoft Office 365.
- In April 2010, an Amazon cross-site scripting (XSS) bug enabled credentials theft, and in 2009, numerous Amazon systems were hijacked to run Zeus botnet nodes.

CSA Security Guidance

Domain 2: Governance and Enterprise Risk Management
Domain 6: Management Plane and Business Continuity
Domain 9: Incident Response
Domain 12: Identity, Entitlement, and Access Management

CCM Controls

BCR Business Continuity Management and Operational Resilience
BCR-01: Business Continuity Planning

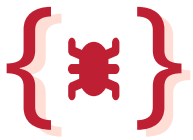
IAM Identity and Access Management
IAM-02: Credential Lifecycle / Provision Management
IAM-05: Segregation of Duties
IAM-08: Trusted Sources
IAM-10: User Access Reviews
IAM-11: User Access Revocation

IVS Infrastructure and Virtualization Security
IVS-01: Audit Logging/Intrusion Detection
IVS-08: Production / Non-Production Environments

SEF Security Incident Management, E-Discovery, and Cloud Forensics
SEF-01: CSP points of contact for IR escalation and support

THREAT ANALYSIS	LINKS AND REFERENCES
☑ Spoofing Identity ☑ Tampering with Data ☑ Repudiation ☑ Information Disclosure ☑ Denial of Service ☑ Elevation of Privilege	1. *Murder in the Amazon cloud:* https://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html 2. *Alleged hacker tried to sell details of 319 million iCloud users for bitcoin:* https://www.cultofmac.com/583836/alleged-hacker-tried-to-sell-details-of-319-million-icloud-for-bitcoin/ 3. *PoC Exploit Compromises Microsoft Live Accounts via Subdomain Hijacking:* https://threatpost.com/poc-exploit-compromises-microsoft-live-accounts-via-subdomain-hijacking/138719/ 4. *How can Office 365 phishing threats be addressed?:* https://www.helpnetsecurity.com/2018/05/18/office-365-phishing-threats/

Security Issue: Insider Threat



CERT defines an insider threat as, "the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization." Insiders can be current or former employees, contractors, or other trusted business partners. Unlike external threat actors, insiders do not have to penetrate firewalls, virtual private networks (VPNs), and other perimeter security defenses. Insiders operate within a company's security circle of trust where they have direct access to networks, computer systems, and sensitive company data.

SECURITY RESPONSIBILITY
☑ Customer
☒ Cloud Service Provider
☒ Both

ARCHITECTURE
☑ Infra
☒ Meta
☒ Info
☒ Appli

CLOUD SERVICE MODEL
☑ Software as a Service (SaaS)
☑ Platform as a Service (PaaS)
☑ Infrastructure as a Service (IaaS)

Insider threats are more prevalent than you may think. The Netwrix 2018 Cloud Security Report indicates that 58 percent of companies attribute security breaches to insiders. Insider negligence is the cause of most security incidences.

Employee or contractor negligence was the root cause of 64 percent of the reported insider incidents, whereas 23 percent were related to criminal insiders and 13 percent to credential theft, according to the Ponemon Institute's 2018 Cost of Insider Threats study. Some common scenarios cited included misconfigured cloud servers, employees storing sensitive company data on their own insecure personal devices and systems, and employees or other insiders falling prey to phishing emails that lead to malicious attacks on company assets.

Business Impact

Insider threats can result in the loss of proprietary information and intellectual property. System downtime associated with attacks can negatively impact company productivity. Additionally, data loss or other customer harm can reduce confidence in company services.

Dealing with insider security incidents involves containment, remediation, incident response, investigation, post-incidence analysis, escalation, monitoring, and surveillance. These activities can add significantly to a company's workload and security budget. The Ponemon Institute reported that—of the companies interviewed—the average cost of insider incidents in 2017 (per company) was more than $8.7 million, with the maximum cost running as high as $26.5 million.

Key Takeaways

1. Taking measures to minimize insider negligence can help mitigate the consequences of insider threats. Actions outlined below can help resolve the security problems introduced by negligent users and administrators.
2. Security employee training and education: Provide training to your security teams to properly install, configure, and monitor your computer systems, networks, mobile devices, and backup devices.
3. Regular employee training awareness: Provide training to your regular employees to inform them how to handle security risks, such as phishing and protecting corporate data they carry outside the company on laptops and mobile devices. Require usage of strong passwords and frequent password updates. Inform employees of repercussions related to engaging in malicious activity.
4. Fixing misconfigured cloud servers: Routinely audit servers in the cloud and on-premises, then correct any deviation from the secure baseline set across the organization.
5. Restrict access to critical systems: Make sure that privileged access security systems and central servers are limited to a minimum number of employees, and that these individuals only include those with the training to handle the administration of mission-critical computer servers. Monitor access to all computer servers at any privilege level.

Anecdotes and Examples

Recent examples of insider threat-related issues include:

- In June 2018, Tesla CEO Elon Musk sent an e-mail to Tesla employees alleging there was a saboteur within his company's ranks. The saboteur, a disgruntled employee, allegedly used false usernames to make changes to the code used in the Tesla Manufacturing Operation System. The employee also exported "large amounts of highly sensitive Tesla data to unknown third parties."
- Also in 2018, an employee at the Punjab National Bank in India gained unauthorized access to a sensitive password in the SWIFT interbank transaction system to release funds in a fraudulent transactional chain. A diamond merchant created the scheme to buy rough stones from suppliers. The total price tag for the bank: $1.8 billion.
- According to the IBM X-Force Threat Intelligence Index 2018: "Misconfigured cloud servers, networked backup incidents, and other improperly configured systems were responsible for the exposure of more than 2 billion records, or nearly 70 percent of the total number of compromised records tracked by X-Force in 2017."

CSA Security Guidance

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

CCM Controls

DCS Datacenter Security
DCS-04: Off-Site Authorization
DCS-08: Unauthorized Persons Entry
DCS-09: User Access

DSI Data Security and Information Lifecycle Management
DSI-04: Handling / Labeling / Security Policy
DSI-06: Ownership / Stewardship

EKM Encryption and Key Management
EKM-02: Key Generation
EKM-03: Sensitive Data Protection

GRM Governance and Risk Management
GRM-03: Management Oversight
GRM-04: Management Program
GRM-06: Policy
GRM-07: Policy Enforcement
GRM-10: Risk Assessments

HRS Human Resources
HRS-02: Background Screening
HRS-03: Employment Agreements
HRS-07: Roles / Responsibilities

IAM Identity and Access Management
IAM-01: Audit Tools Access
IAM-05: Segregation of Duties
IAM-08: Trusted Sources
IAM-09: User Access Authorization
IAM-10: User Access Reviews
IAM-11: User Access Revocation

IVS Infrastructure and Virtualization Security
IVS-09: Segmentation

STA Supply Chain Management, Transparency and Accountability
STA-09: Third Party Audits

THREAT ANALYSIS	LINKS AND REFERENCES
☑ Spoofing Identity ☑ Tampering with Data ☒ Repudiation ☑ Information Disclosure ☒ Denial of Service ☑ Elevation of Privilege	1. *CERT Definition of an 'Insider Threat' - Updated:* https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html 2. *Cloud Security Risks and Concerns in 2018:* https://blog.netwrix.com/2018/01/23/cloud-security-risks-and-concerns-in-2018/ 3. *IBM X-Force Threat Intelligence Index 2018:* https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN 4. *Insider Threat – 2018 Statistics:* https://www.uscybersecurity.net/insider-threats-2018-statistics//2018_Global_Cost_of_a_Data_Breach_Report.pdf 5. *Examining the 2018 Cost of a Data Breach:* https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf 6. *Tesla's Tough Lesson on Malicious Insider Threats:* https://www.infosecurity-magazine.com/news/teslas-tough-lesson-on-malicious/ 7. *The 6 Worst Insider Attacks of 2018 – So Far:* https://www.darkreading.com/the-6-worst-insider-attacks-of-2018---so-far/d/d-id/1332183

Security Issue: Insecure Interfaces and APIs

Cloud computing providers expose a set of software user interfaces (UIs) and APIs to allow customers to manage and interact with cloud services. The security and availability of general cloud services are dependent on the security of these 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 the security policy. Poorly designed APIs could lead to misuse or—even worse—a data breach. Broken, exposed, or hacked APIs have caused some major data breaches. Organizations must understand the security requirements around designing and presenting these interfaces on the internet.

APIs and UIs are generally the most exposed parts of a system, perhaps the only asset with a public IP address available outside the trusted organizational boundary. As the "front door," they are very likely to be attacked continuously; therefore, security by design and adequate controls protecting them from the attacks are required.

SECURITY RESPONSIBILITY

- ☒ Customer
- ☒ Cloud Service Provider
- ☑ Both

ARCHITECTURE

- ☑ Infra
- ☑ Meta
- ☒ Info
- ☑ Appli

CLOUD SERVICE MODEL

- ☑ Software as a Service (SaaS)
- ☑ Platform as a Service (PaaS)
- ☑ Infrastructure as a Service (IaaS)

Business Impact

While most providers strive to ensure that security is well-integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the use, 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. Additionally, regulatory and financial impacts could be very significant.

Key Takeaways

1. Practice good API hygiene. Good practice includes diligent oversight of items such as inventory, testing, auditing, and abnormal activity protections.
2. Ensure proper protection of API keys and avoid reuse.
3. Consider using standard and open API frameworks (e.g., Open Cloud Computing Interface (OCCI) and Cloud Infrastructure Management Interface (CIMI)).

Anecdotes and Examples

Recent examples of issues related to insecure interfaces and APIs include:

- Facebook announced a significant data breach affecting more than 50 million accounts on Sept. 28, 2018. Reportedly, credential theft vulnerability was introduced into Facebook code in July of 2017, more than a year earlier. The company admitted it didn't know what information was stolen, nor how many other user accounts were compromised as a result of the breach.

CSA Security Guidance

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

CCM Controls

AIS Application and Interface Security
AIS-01: Application Security
AIS-03: Data Integrity
AIS-04: Data Security / Integrity

IAM Identity and Access Management
IAM-01: Audit Tools Access
IAM-07: Third Party Access
IAM-08: Trusted Sources
IAM-09: User Access Authorization
IAM-10: User Access Reviews
IAM-11: User Access Revocation
IAM-12: User ID Credentials
IAM-13: Utility Programs Access

THREAT ANALYSIS

- ☒ Spoofing Identity
- ☑ Tampering with Data
- ☑ Repudiation
- ☑ Information Disclosure
- ☒ Denial of Service
- ☑ Elevation of Privilege

LINKS AND REFERENCES

1. *The Treacherous 12: Top Threats to Cloud Computing + Industry Insights:* https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf
2. Cloud API security risks: How to assess cloud service provider APIs: https://searchcloudsecurity.techtarget.com/tip/Cloud-API-security-risks-How-to-assess-cloud-service-provider-APIs
3. *Insecure API Implementations Threaten Cloud:* https://www.darkreading.com/cloud/insecure-api-implementations-threaten-cloud/d/d-id/1137550
4. *Facebook data breach highlights API vulnerabilities:* https://www.pingidentity.com/en/company/blog/posts/2018/facebook-data-breach-highlights-api-vulnerabilities.html
5. *Facebook says at least 50 million users affected by security breach:* https://techcrunch.com/2018/09/28/facebook-says-50-million-accounts-affected-by-account-takeover-bug/
6. *Cloud Security Threats - Insecure APIs:* https://community.hpe.com/t5/Shifting-to-Software-Defined/Cloud-Security-Threats-Insecure-APIs/ba-p/6871684#.XBkCEGhKiUl

Security Issue: Weak Control Plane

Moving from the data center to the cloud poses some challenges for creating a sufficient data storage and protection program. The user must now develop new processes for data duplication, migration, and storage and—if using multicloud—it gets even more complicated. A control plane should be the solution for these problems, as it enables the security and integrity that would complement the data plane that provides stability and runtime of the data. A weak control plane means the person in charge—either a system architect or a DevOps engineer—is not in full control of the data infrastructure's logic, security, and verification. In this scenario, controlling stakeholders don't know the security configuration, how data flows, and the where architectural blind spots and weak points exist. These limitations could result in data corruption, unavailability, or leakage.

SECURITY RESPONSIBILITY

- ☑ Customer
- ☒ Cloud Service Provider
- ☒ Both

ARCHITECTURE

- ☑ Infra
- ☒ Meta
- ☒ Info
- ☒ Appli

CLOUD SERVICE MODEL

- ☑ Software as a Service (SaaS)
- ☑ Platform as a Service (PaaS)
- ☑ Infrastructure as a Service (IaaS)

Business Impact

A weak control plane could result in data loss, either by theft or corruption. This could lead to a massive business impact, particularly if data loss includes private user data. Regulatory punishment for data loss may be incurred as well. For example, under General Data Protection Regulation (GDPR) regulations, incurred penalties can reach €20M— or four percent— of global revenue.

With a weak control plane, users may also be unable to protect their cloud-based business data and applications, which can lead to frustration and a loss of confidence in the service or the product provided. Ultimately, this may translate to a revenue decrease.

Key Takeaways

1. Adequate security controls provided through a CSP are necessary so that cloud customers can fulfill their legal and statutory obligations.
2. The cloud customer should perform due diligence and determine if the cloud service they intend to use possesses an adequate control plane.

Anecdotes and Examples

Recent examples of issues related to weak control plane include:

- The management plane of a cloud service is very critical and needs to be adequately protected by identity and access controls. Two-factor authentication should be part of the standard suite of controls provided to a cloud customer by the CSP. Unfortunately, many CSPs only make two-factor authentication available to their customers as a premium service. Such practices weaken the security posture of cloud customers—particularly those who do not or cannot utilize this premium service.

CSA Security Guidance

Domain 1: Cloud Computing Concepts and Architectures
Domain 5: Information Governance
Domain 7: Infrastructure Security
Domain 8: Virtualization and Containers
Domain 12: Identity, Entitlement and Access Management

CCM Controls

AIS Application and Interface Security
AIS-03: Data Integrity
AIS-04: Data Security / Integrity

AAC Audit Assurance and Compliance
AAC-03: Information System Regulatory Mapping

BCR Business Continuity Management and Operational Resilience
BCR-04: Documentation

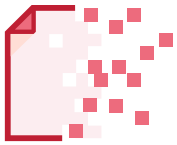
DSI Data Security and Information Lifecycle Management
DSI-04: Handling / Labeling / Security Policy

GRM Governance and Risk Management
GRM-01: Baseline Requirements
GRM-02: Data Focus Risk Assessments
GRM-06: Policy
GRM-07: Policy Enforcement
GRM-08: Policy Impact on Risk Assessments
GRM-09: Policy Reviews
GRM-10: Risk Assessments
GRM-11: Risk Management Framework

IVS Infrastructure and Virtualization Security
IVS-01: Audit Logging / Intrusion Detection
IVS-04: Information System Documentation
IVS-06: Network Security
IVS-09: Segmentation
IVS-13: Network Architecture

THREAT ANALYSIS	LINKS AND REFERENCES
☒ Spoofing Identity ☑ Tampering with Data ☒ Repudiation ☑ Information Disclosure ☒ Denial of Service ☑ Elevation of Privilege	1. *Uber fined $148m for failing to notify drivers they had been hacked:* https://www.theguardian.com/technology/2018/sep/26/uber-hack-fine-driver-data-breach 2. *Exposed S3 bucket compromises 120 million Brazilian citizens:* https://www.scmagazine.com/home/security-news/exposed-s3-bucket-compromises-120-million-brazilian-citizens/

Security Issue: Metastructure and Applistructure Failures



Cloud service providers routinely reveal operations and security protections that are necessary to implement and protect their systems successfully. Typically, API calls disclose this information, and the protections are incorporated in the metastructure layer for the CSP. The metastructure is considered the CSP/customer line of demarcation—also known as the waterline.

SECURITY RESPONSIBILITY
☒ Customer
☒ Cloud Service Provider
☑ Both
ARCHITECTURE
☒ Infra
☑ Meta
☒ Info
☑ Appli
CLOUD SERVICE MODEL
☑ Software as a Service (SaaS)
☑ Platform as a Service (PaaS)
☑ Infrastructure as a Service (IaaS)

Failure possibilities exist at multiple levels in this model. For example, poor API implementation by the CSP offers attackers an opportunity to disrupt cloud customers by interrupting confidentiality, integrity, or availability of the service.

To increase cloud visibility to customers, CSPs have often revealed or allowed API interaction with security processes at the waterline. Immature CSPs are often unsure of how to make APIs available to their customers—and to what extent. For example, APIs that allow customers to retrieve logs or audit system access may include highly sensitive information. However, this process is also necessary for tenants to detect unauthorized access.

Above the waterline, cloud consumers must understand how to properly implement cloud applications to fully utilize the cloud platform. For example, applications that are not designed for cloud environments will not be able to fully interact and use available cloud resources and capabilities. Merely taking a "lift-and-shift" approach does not suffice when migrating business operations and applications to the cloud.

Business Impact

Metastructure and applistructure are critical components of a cloud service. Failures involving these features at the CSP level can severely impact all service consumers. At the same time, misconfigurations by the tenant could disrupt the user financially and operationally.

Key Takeaways

1. Cloud service providers must offer visibility and expose mitigations to counteract the cloud's inherent lack of transparency for tenants.
2. Cloud tenants should implement appropriate features and controls in cloud native designs.
3. All CSPs should conduct penetration testing and provide findings to customers.

Anecdotes and Examples

Recent examples of issues related to metastructure and applistructure failure include:

- The most consistent examples of meta/applistructure failures on the customer side surround identity and access management issues. Many organizations still solely rely on usernames and passwords, ignoring updated security capabilities such as single sign-on (SSO), identity federation and multi-factor authentication (MFA), which are offered—and easily implemented—within the cloud. For example, Deloitte spilled the contents of their Office 365 email service after relying on a single password for their administrator account (despite Microsoft offering an MFA option). As a result, hackers breached that account, exposing large amounts of client information.
- Netflix, one of the heaviest users of AWS, understands how vital metastructure access is and provides credential compromise detection steps used in their security operations processes. Attackers see value in metastructure credentials: Microsoft warns that their cloud credential targeting continues to increase year-to-year. According to the *2017 Microsoft Security Intelligence Report*, these targets tripled in frequency from the year prior. The 2018 Microsoft Security Intelligence Report findings also document that "79 percent of SaaS storage apps and 86 percent of SaaS collaboration apps do not encrypt data both at rest and in transit."
- An early SecureWorks study of the AWS Community Marketplace found more than half of the images had some flaw embedded in the Amazon Machine Image (AMI). Deficiencies cited include files in temporary directories, embedded keys left on systems, and additional runlevel run control (rc) scripts left on the snapshots. Without knowing image origins, images might be doing more than promised. Infrastructure as a service (IaaS) providers have since published instructions and requirements for sharing in the various marketplaces. Additionally, applistructure implementations have similar problems, with Apple restricting iOS app providers in 2019 due to screen recording code for customer analytics.

CSA Security Guidance

Domain 1: Cloud Computing Concepts and Architectures
Domain 2: Governance and Enterprise Risk Management
Domain 4: Compliance and Audit Management
Domain 5: Information Governance
Domain 6: Management Plane and Business Continuity
Domain 7: Infrastructure Security
Domain 8: Virtualization and Containers
Domain 9: Incident Response
Domain 10: Application Security
Domain 11: Data Security and Encryption
Domain 12: Identity Entitlement and Access Management

CCM Controls

AIS Application and Interface Security
AIS-01: Application Security
AIS-03: Data Integrity
AIS-04: Data Security / Integrity

AAC Audit Assurance and Compliance
AAC-01: Audit Planning

BCR Business Continuity Management and Operational Resilience
BCR-02: Business Continuity Testing
BCR-04: Operational Resilience Documentation

CCC Change Control and Configuration Management
CCC-01: New Development / Acquisition
CCC-05: Production Changes

DSI Data Security and Information Lifecycle
DSI-02: Data Inventory / Flows
DSI-03: Ecommerce Transactions
DSI-04: Handling / Labeling / Security Policy
DSI-07: Secure Disposal

EKM Encryption and Key Management
EKM-02: Key Generation
EKM-03 - Sensitive Data Protection

HRS Human Resources
HRS-08: Human Resources: Technology Acceptable Use

IAM Identity and Access Management
IAM-01: Audit Tools Access
IAM-02: Credential Lifecycle / Provision Management
IAM-04: Policies and Procedures
IAM-05: Segregation of Duties
IAM-07: Third Party Access
IAM-08: Trusted Sources
IAM-09: User Access Authorization
IAM-10: User Access Reviews
IAM-11: User Access Revocation
IAM-12: User ID Credentials
IAM-13: Utility Programs Access

IVS Infrastructure and Virtualization Security
IVS-09: Segmentation

IPY Interoperability and Portability
IPY-01: APIs

SEF Security Incident, E-Discovery &and Cloud Forensics
SEF-04: Incident Reporting

STA Supply Chain Management, Transparency and Accountability
STA-03: Network / Infrastructure Services

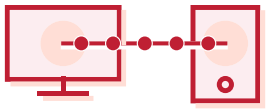
THREAT ANALYSIS

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

LINKS AND REFERENCES

1. *Why Cloud Security Is Everyone's Business:* https://www.gartner.com/smarterwithgartner/why-cloud-security-is-everyones-business/
2. *Source: Deloitte Breach Affected All Company Email, Admin Accounts:* https://krebsonsecurity.com/2017/09/source-deloitte-breach-affected-all-company-email-admin-accounts/
3. *Deloitte hack hit server containing emails from across US government:* https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government
4. *Deloitte Gets Hacked: What We Know So Far:* http://fortune.com/2017/09/25/deloitte-hack
5. *"Get Off of My Cloud": Cloud Credential Compromise and Exposure:* https://www.defcon.org/images/defcon-19/dc-19-presentations/Feinstein-Jarmoc/DEFCON-19-Feinstein-Jarmoc-Get-Off-of-My-Cloud.pdf
6. *Netflix Cloud Security: Detecting Credential Compromise in AWS:* https://medium.com/netflix-techblog/netflix-cloud-security-detecting-credential-compromise-in-aws-9493d6fd373a
7. *Microsoft Security Intelligence Report:* https://download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security_Intelligence_Report_Volume_22.pdf
8. *Microsoft warns that hackers are increasingly targeting cloud accounts:* https://www.theinquirer.net/inquirer/news/3016031/microsoft-warns-that-hackers-are-increasingly-targeting-cloud-accounts
9. *Microsoft Security Intelligence Report volume 23 is now availablePoorly secured Cloud Apps:* https://cloudblogs.microsoft.com/microsoftsecure/2018/03/15/microsoft-security-intelligence-report-volume-23-is-now-available/
10. *Understand top trends in the threat landscape:* https://www.microsoft.com/sir
11. *What Is Amazon EC2?:* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/building-shared-amis.htm
12. *Virtual machine prerequisites:* https://docs.microsoft.com/en-us/azure/marketplace/cloud-partner-portal/virtual-machine/cpp-prerequisites
13. *How to Log a Security Event Support Ticket:* https://docs.microsoft.com/en-us/azure/security/azure-security-event-support-ticket
14. *Apple tells app developers to disclose or remove screen recording code:* https://techcrunch.com/2019/02/07/apple-glassbox-apps/
15. *Announcing AWS CloudTrail:* https://aws.amazon.com/about-aws/whats-new/2013/11/13/announcing-aws-cloudtrail/
16. *AWS Discussion Forums - AWS CloudTrail Feature Additions:* https://forums.aws.amazon.com/forum.jspa?forumID=168
17. *AWS Discussion Forums - AWS CloudWatch Feature Aadditions:* https://forums.aws.amazon.com/forum.jspa?forumID=138
18. *Announcing the public preview of Azure Monitor:* https://azure.microsoft.com/en-us/blog/announcing-the-public-preview-of-azure-monitor/
19. *Azure AD Activity Logs in Azure Monitor Diagnostics now in public preview:* https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Activity-Logs-in-Azure-Monitor-Diagnostics-now-in/ba-p/245435

Security Issue: Limited Cloud Usage Visibility



Limited cloud usage visibility occurs when an organization does not possess the ability to visualize and analyze whether cloud service use within the organization is safe or malicious. This concept is broken down into two key challenges.

SECURITY RESPONSIBILITY
☒ Customer
☒ Cloud Service Provider
☑ Both
ARCHITECTURE
☑ Infra
☑ Meta
☑ Info
☑ Appli
CLOUD SERVICE MODEL
☑ Software as a Service (SaaS)
☑ Platform as a Service (PaaS)
☑ Infrastructure as a Service (IaaS)

Un-sanctioned app use: This occurs when employees are using cloud applications and resources without the specific permission and support of corporate IT and security. This scenario results in a self-support model called Shadow IT. When insecure cloud services activity does not meet corporate guidelines, this behavior is risky— especially when paired with sensitive corporate data. Gartner predicts that by 2020, one-third of all successful security attacks on companies will come through shadow IT systems and resources.

Sanctioned app misuse: Organizations are often unable to analyze how their approved applications are being leveraged by insiders who use a sanctioned app. Frequently, this use occurs without the explicit permission of the company, or by external threat actors who target the service using methods such as credential theft, Structured Query Language (SQL) injection, Domain Name System (DNS) attacks and more.

In most cases, it comes down to discerning valid and invalid users from one another; if their behaviors are out of the norm; and if they abide by corporate policies.

Business Impact

The risks are widespread but can be summed up with the following points:

- Lack of governance: When employees are unfamiliar with proper access and governance controls, it is common to see sensitive corporate data placed in public access locations vs. private access locations.
- Lack of awareness: When data and services are in use without the knowledge of the company, they are, in essence, unable to control their IP. The employee has the data, not the company.
- Lack of security: When an employee incorrectly sets up a cloud service, it can become exploitable not only for the data that resides on it but for future data.Malware, botnets, cryptocurrency mining malware, and more can compromise cloud containers—which puts organizational data, services, and finances at risk.

When asked about the impact of unsanctioned cloud use in their respective environments, 50 percent of the respondents cited in the Oracle and KPMG Cloud Threat Report 2019 indicated this unsanctioned use has led to "unauthorized access to data," and another 48 percent cited the "introduction of malware" as a result.

Key Takeaways

1. Mitigating these risks starts with the development of a complete cloud visibility effort from the top down. This process usually originates with tasking an organization's cloud security architect with the creation of a comprehensive solution that ties into people, process, and technology. Actions outlined below can help jumpstart this process.
2. Mandate companywide training on accepted cloud usage policies and enforcement thereof.
3. All non-approved cloud services must be reviewed and approved by the cloud security architect or third-party risk management.
4. Invest in solutions like cloud access security brokers (CASB) or software defined gateway (SDG) to analyze outbound activities and help discover cloud usage, at-risk users, and to follow behavior usage of credentialed employees to identify anomalies.
5. Invest in a web application firewall (WAF) to analyze all inbound connections to your cloud services for suspicious trends, malware, distributed denial-of-service (DdoS), and Botnet risks.
6. Select solutions that are specifically designed to monitor and control all of your key enterprise cloud applications (enterprise resource planning, human capital management, commerce experience, and supply chain management) and ensure suspicious behaviors can be mitigated.
7. Implement a zero-trust model across your organization.

Anecdotes and Examples

Recent examples of issues related to limited cloud usage visibility include:

- According to 2018 research conducted by cloud security firm Lacework: "More than 22,000 container orchestration and API management systems are unprotected or publicly available on the internet – highlighting the reality of the risks of operating workloads in the cloud."
- The "Skyhigh Networks Cloud Adoption & Risk Report Q2 2015 reported that "the average enterprise now uses 1,083 cloud services. That astounding figure is almost 50 percent higher than this time last year, and up to 100 percent from two years ago."
- Of those 1,000-plus cloud services in use today, the Skyhigh Networks Cloud Adoption & Risk Report Q2 2015 stated that many might fall into the category of Shadow IT. Simply put: the IT department had no role in helping to select and deploy the services of these Shadow IT services, and might not even know they are being used."

CSA Security Guidance

Domain 5: Information Governance
Domain 11: Data Security and Encryption

CCM Controls

DSI Data Security and Information Lifecycle Management
DSI-01: Classification
DSI-02: Data Inventory / Flows
DSI-04: Handling / Labeling / Security Policy
DSI-06: Ownership / Stewardship

EKM Encryption and Key Management
EKM-03: Sensitive Data Protection

GRM Governance and Risk Management
GRM-02: Data Focus Risk Assessments

HRS Human Resources
HRS-03: Employment Agreements
HRS-07: Roles / Responsibilities
HRS-08: Technology Acceptable Use
HRS-09: Training / Awareness
HRS-10: User Responsibility

THREAT ANALYSIS	LINKS AND REFERENCES
☑ Spoofing Identity ☑ Tampering with Data ☑ Repudiation ☑ Information Disclosure ☑ Denial of Service ☑ Elevation of Privilege	1. *22K Open, Vulnerable Containers Found Exposed on the Net:* https://threatpost.com/22k-open-vulnerable-containers-found-exposed-on-the-net/132898/ 2. *Five Ways Shadow IT in the cloud hurts your enterprise:* https://www.networkworld.com/article/2997152/cloud-computing/five-ways-shadow-it-in-the-cloud-hurts-your-enterprise.html 3. *Cloud Adoption and Risk Report:* https://info.skyhighnetworks.com/WP-CARR-Q2-2015_Download_White.html?Source=website&LSource=website

Security Issue: Abuse and Nefarious Use of Cloud Services

Malicious actors may leverage cloud computing resources to target users, organizations, or other cloud providers. Malicious attackers can also host malware on cloud services. Cloud services that host malware can seem more legitimate because the malware uses the CSP's domain. Furthermore, cloud-hosted malware can use cloud-sharing tools as an attack vector to further propagate itself. Other examples of misuse of cloud resources include:

- launching DDoS attacks
- email spam and phishing campaigns
- "mining" for digital currency
- large-scale automated click fraud
- brute-force attacks of stolen credential databases
- hosting of malicious or pirated content

SECURITY RESPONSIBILITY
☒ Customer
☒ Cloud Service Provider
☑ Both
ARCHITECTURE
☑ Infra
☑ Meta
☑ Info
☑ Appli
CLOUD SERVICE MODEL
☑ Software as a Service (SaaS)
☑ Platform as a Service (PaaS)
☑ Infrastructure as a Service (IaaS)

The mitigations for misuse of cloud services include CSP detection of payment instrument fraud and misuse of cloud offerings. A CSP must have an incident response framework to address the misuse of resources and a means for customers to report abuse originating from a CSP. A CSP should also include relevant controls that allow customers to monitor the health of their cloud workload as well as file-sharing or storage applications.

Business Impact

If an attacker has compromised the management plane of a customer's cloud infrastructure, the attacker can use the cloud service for illicit purposes while the customer foots the bill. The bill could be substantial if the attacker consumed substantial resources, such as mining cryptocurrency.

Alternatively, attackers can also use the cloud to store and propagate malware. Enterprises must be aware and have controls in place to deal with these new attack vectors. This may mean procuring security technology that can monitor cloud infrastructure or API calls from and to the cloud service.

Key Takeaways

- Enterprises should monitor their employees in the cloud, as traditional mechanisms are unable to mitigate the risks posed by cloud service usage.
- Employ cloud data loss prevention (DLP) technologies to monitor and stop any unauthorized data exfiltration.

Anecdotes and Examples

Recent examples of issues related to abuse and nefarious use of cloud services include:

- The Zepto variant of the Locky ransomware spreads via cloud services such as Microsoft OneDrive, Google Drive, and Box by sharing a malicious file with potential victims.
- The CloudSquirrel attack arrives via an email phishing attack. This attack email attempts to trick its victim into opening its message using an important-sounding link (such as a "tax invoice"). Once opened, CloudSquirrel infects users by downloading additional malicious encrypted payloads via a Java Archive (JAR) file. The malware then establishes a connection with its command and control hosted in Dropbox. Its commands masquerade as plain text files with fake extensions such as.mp4, .wmv, .png, .dat, and .wma.

CSA Security Guidance

Domain 7: Infrastructure Security
Domain 9: Incident Response
Domain 10: Application Security
Domain 6: Management Plane and Business Continuity

CCM Controls

AIS Application and Interface Security
AIS-02: Customer Access Requirements

BCR Business Continuity Management and Operational Resilience
BCR-09: Impact Analysis

CCC Change Control and Configuration Management
CCC-02: Outsourced Development

DSI Data Security and Information Lifecycle Management
DSI-01: Classification
DSI-02: Data Inventory / Flows
DSI-04: Handling / Labeling / Security Policy

EKM Encryption and Key Management
EKM-03: Sensitive Data Protection

GRM Governance and Risk Management
GRM-01: Baseline Requirements

HRS Human Resources
HRS-05: Mobile Device Management
HRS-08: Technology Acceptable Use
HRS-09: Training / Awareness

IAM Identity and Access Management
IAM-02: Credential Lifecycle / Provision Management
IAM-04: Policies and Procedures
IAM-05: Segregation of Duties
IAM-09: User Access Authorization
IAM-10: User Access Reviews
IAM-11: User Access Revocation
IAM-12: User ID Credentials

IVS Infrastructure and Virtualization Security
IVS-01: Audit Logging / Intrusion Detection
IVS-02: Change Detection
IVS-06: Network Security
IVS-13: Network Architecture

MOS Mobile Security

MOS-02: Application Stores
MOS-03: Approved Application
MOS-04: Approved Software for BYOD
MOS-05: Awareness and Training
MOS-06: Cloud Based Services
MOS-19: Security Patches

TVM Threat and Vulnerability Management

TVM-02: Vulnerability / Patch Management

THREAT ANALYSIS	LINKS AND REFERENCES
☑ Spoofing Identity ☑ Tampering with Data ☑ Repudiation ☑ Information Disclosure ☑ Denial of Service ☑ Elevation of Privilege	1. *Malware Used by China APT Group Abuses Dropbox:* http://www.securityweek.com/malware-used-china-apt-group-abuses-dropbox 2. *Zepto variant of Locky ransomware delivered via popular Cloud Storage apps:* https://resources.netskope.com/h/i/273457617-zepto-variant-of-locky-ransomware- delivered-via-popular-cloud-storage-apps 3. *CloudSquirrel Malware Squirrels Away Sensitive User Data Using Popular Cloud Apps:* https://resources.netskope.com/h/i/272453388-cloudsquirrel-malware-squirrels-away- sensitive-user-data-using-popular-cloud-apps 4. *CloudFanta Pops with the Cloud using SugarSync:* https://resources.netskope.com/h/i/295875750-cloudfanta-pops-with-the-cloud-using-sugarsync 5. *Data Theft Via the Cloud: You Don't Need Flash Drives Any More:* https://blog.learningtree.com/data-theft-via-cloud-dont-need-flash-drives/ 6. *What Is Cloud DLP?:* https://digitalguardian.com/blog/what-cloud-dlp 7. *Best Practices for Cloud Security:* https://insights.sei.cmu.edu/sei_blog/2018/03/best-practices-for-cloud-security.html

Conclusion

As cloud business models and security tactics evolve, this report raises awareness of critical security issues such as data breaches, misconfiguration and identity, and access management. Other threats highlight lack-of-control hurdles that users may experience with CSPs, such as limited cloud usage visibility and weak control plane. These issues can lead to data breaches or leaks beyond the traditional landscape, as seen in many past cases.

Considering that user interfaces and APIs are the modern way to consume services, it is concerning that there are still significant challenges when it comes to securing these features.

The cloud—with its complexity—is also the perfect place for attackers to hide. It is also, unfortunately, an ideal launchpad for attacks. Last but not least, insider threats make it more challenging to protect organizations from data loss.

All of these pitfalls require more industry attention and research.

This *Top Threats in Cloud Computing* report suggests an interesting and somewhat new perspective on cloud security. This new outlook focuses on configuration and authentication, and shifts away from the traditional focus on information security (e.g., vulnerabilities and malware). Regardless, these security issues are a call to action for developing and enhancing cloud security awareness, configuration, and identity management.

Appendix: Methodology

In creating *The Egregious 11: Cloud Computing Top Threats in 2019* report, the CSA *Top Threats Working Group* conducted research in two primary stages. Both stages used surveys and questionnaires as instruments of study.

In the first stage of research, the group's goal was to create a shortlist of cloud security concerns. The group started with a list of 26 security concerns (updating the previous report's 12 and adding 14 new issues). The group discussed the 26 points in a series of meetings, asking working group members to indicate the importance of each matter in relation to their respective organization. This stage of the research also provided the opportunity for working group members to suggest additional concerns not included in the list of 26. After considering all the survey results and other information, the working group identified the top 19 most salient cloud security concerns.

In the second stage of the research, the group's main goal was to rank—via importance—this condensed list of 19. The group wanted the study to capture what security professionals thought were the most relevant cloud security concerns, so a 10-point sliding scale was chosen as the research instrument. Respondents were instructed to rate cloud security issues from "1 to 10," with "1" being "very insignificant" and "10" being "very significant". The points for each category were averaged, and the security concerns were then ranked according to their mean. The working group then arrived at the top 11 by excluding all security issues with a mean of less than seven.

Finally, the working group also analyzed the security concerns using the STRIDE threat model, which was developed by Microsoft to evaluate information security threats. Specifically, the security concerns discussed in this paper are evaluated to determine whether they fall into any of the following threat categories:

- Spoofing identity (S)
- Tampering with data (T)
- Repudiation (R)
- Information Disclosure(I)
- Denial of service (D)
- Elevation of privilege (E)

