Top Threats to Cloud Computing

cloud security alliance®

The permanent and official location for Cloud Security Alliance Top Threats research:
https://cloudsecurityalliance.org/research/working-groups/top-threats/

Acknowledgments

Co-chairs

Jon-Michael Brook
Alexander Stone Getsin
Michael Roza

Contributors

Jon-Michael C Brook
Victor Chin
Hugh Foskett
Alex Getzin
Vic Hargrave
Shachaf Levy
Andrew McCormick
Stephen Pieraldi
Michael Roza
Marcus Ryan
Alon Schindel
Shira Shamban

Reviewers

Guy Dahan
Moshe Ferber
Alex Rebo
Daniel Schwartzer
Udith Wickramasuriya

CSA Global Staff

Sean Heide
Claire Lehnert (graphic design)
Stephen Lumpe (graphic design)

Table of Contents

Executive Summary

The *Top Threats* reports traditionally aim to raise awareness of threats, vulnerabilities, and risks in the cloud. In this sixth installment, we surveyed over 700 industry experts on security issues in the cloud industry. This year our respondents identified eleven important security issues to their cloud environments. The *Top Threats* Working Group used the survey results and its expertise to create the 2022 "*Top Threats* to Cloud Computing - Pandemic Eleven" report.

The latest report highlights the Pandemic Eleven (ranked in order of significance per the survey described on page 8). Also shown are the 2019 survey rankings or analog in parentheses):

1. Insufficient Identity, Credentials, Access, and Key Management (4)
2. Insecure Interfaces and APIs (7)
3. Misconfiguration and Inadequate Change Control (2)
4. Lack of Cloud Security Architecture and Strategy (3)
5. Insecure Software Development
6. Unsecured Third-Party Resources
7. System Vulnerabilities (8)
8. Accidental Cloud Data Disclosure
9. Misconfiguration and Exploitation of Serverless and Container Workloads
10. Organized Crime/Hackers/APT (11)
11. Cloud Storage Data Exfiltration

Observations and Rationale

The COVID-19 pandemic and subsequent lockdowns redefined the workplace, stressing work from home as no longer a nice-to-have flexibility benefit, but a necessity for continued corporate operations. The pandemic and the complexity of cloud workloads, supply chains, and new technologies such as Edge Compute, Internet of Things (IoT), Operational Technology (OT), and Blockchain shifted the cloud security landscape. New concepts such as SDP (Software Defined Perimeter) and ZTA (Zero Trust Architecture) altered our view of access to the landscape.

Analyzing the responses in survey results, there is a continuing drop in the ranking of traditional cloud security issues under the responsibility of cloud service providers (CSPs). Concerns such as denial of service, shared technology vulnerabilities, CSP data loss, and system vulnerabilities—featured in the 'Egregious Eleven (EE)' Cloud Computing *Top Threats* in 2019 —were now rated low enough to be excluded from this report. These omissions continue the apparent trust in cloud; vintage cloud security issues in Infrastructure as a Service (IaaS) environments seem to be less of a concern. Additionally, we observed that data breaches no longer dominate as the top cloud security concern.

New, highly rated items in the survey point to cloud adopters as the weak links. Respondents no longer question whether the metastructure (EE:9), weak control plane (EE:8) or usage visibility (EE:10) will be an issue in their cloud deployments. The focus trend from the Treacherous Twelve through the Egregious Eleven to this survey continues pushing responsibility up the stack. The Pandemic Eleven highlights circumstances directly in the user's control: identity and access management, cryptography, configuration management, poor coding practices and ignoring

strategic cloud direction. The uptick in agile project management and DevOps hoists these combined problems directly on the end software teams.

Separating the highest performing cloud organizations will come down to those companies that emphasize change management, increase employee cross-training, embed team security champions and enable security & compliance culturally. Cloud continues to flourish and become an everyday expectation long after the immediate demands of the COVID lockdowns. Investigate these eleven threats, risks and vulnerabilities to secure your cloud for future success.

Target Audience

Cloud and security practitioners and enthusiasts would benefit from this report to gain an up to date insight into the state of cloud security threats and challenges, how they came to impact the industry, and what can be done to improve as an individual or an industry. Finally, this survey-based research will equip compliance, risk, technology staff, and executive management with technology trends and high-priority cloud security considerations relevant to the present time.

The Survey

In creating the 2022 "Top Cloud Threats to Cloud Computing - Pandemic Eleven" report, the CSA *Top Threats Working Group* conducted research in two stages. Both stages used surveys to gather the thoughts and opinions of cybersecurity professionals concerning the most relevant threats, vulnerabilities, and risks security issues) to cloud computing with the ultimate goal of identifying the *Top Threats* for 2022.

During the first research stage, the group's goal was to create a shortlist of cloud security issues through an in-person survey of the working group's members. The group started with the previous report (*Top Threats* to Cloud Computing: Egregious Eleven 2019) of eleven *Top Threats* (security issues) and then added 15 new issues through discussion. The group then reviewed the 26 issues in a series of meetings, asking working group members to indicate the importance of each matter to their respective organizations and their knowledge of organizations familiar to themselves.

This initial stage of the research also allowed working group members to suggest additional concerns not included in the list of 26. After considering all the information, the working group identified the top 19 most salient cloud security issues.

In the second stage of the research, the group's main goal was to rank—by importance—this condensed list of 19 security issues using an online survey of security professionals primarily outside of those in the working group. A 10-point sliding scale was chosen to reflect its importance. The survey participants were instructed to rate each cloud security issue from 1 to 10, with one being "very insignificant" and ten being "very significant." The points for each category were totaled and then averaged. The security issues were then ranked according to their mean. The working group then arrived at the Top 11 Threats below.

Survey Results Rank	Survey Average Score	Issue Name
1	7.729927	Insufficient ID, Credential, Access and Key Mgt, Privileged Accounts
2	7.592701	Insecure Interfaces and APIs
3	7.424818	Misconfiguration and Inadequate Change Control
4	7.408759	Lack of Cloud Security Architecture and Strategy
5	7.275912	Insecure Software Development
6	7.214493	Unsecure Third Party Resources
7	7.143066	System Vulnerabilities
8	7.114659	Accidental Cloud Data Disclosure/ Disclosure
9	7.097810	Misconfiguration & Exploitation of Serverless & Container Workloads
10	7.088534	Organized Crime/ Hackers/ APT
11	7.085631	Cloud Storage Data Exfiltration

With the 11 *Top Threats* identified, the working group performed an analysis of each issue. Each analysis describes the item, whether the CSP or cloud customer owns the shared responsibility and defines where it might be found within the cloud stack and type of cloud service (SaaS, PaaS, IaaS or SPI) model. Business Impacts, Key Takeaways, Anecdotes and real world Examples demonstrate what and where to expect each risk. Conceptual inference and mitigations described through the CSA products include The Security Guidance's Common Body of Knowledge (CBK) v4 domain mappings, Cloud Controls Matrix (CCM) v4 Controls, STRIDE threat modeling relevance and reference links for further detail on the anecdotes.

Security Issue 1:

Insufficient Identity, Credential, Access and Key Mgt, Privileged Accounts

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

Security Responsibility	
✓ Customer	
✗ Cloud Service Provider	
✗ Shared	
Architecture	
✓ Application	✓ Meta
✓ Info	✗ Infra
Cloud Service Model	
✓ Software as a Service (SaaS)	
✓ Platform as a Service (PaaS)	
✓ Infrastructure as a Service (IaaS)	

Proper maintenance and ongoing vigilance are important. The use of risk-scoring in Identity and Access Management (IAM) enhances security posture. Using a clear risk assignment model, diligent monitoring, and proper isolation of its behavior can help cross-check IAM systems. Tracking target access and frequency for risk scoring are also critical to understanding risk context.

Privileged accounts must be deprovisioned in a precise and immediate manner in order to avoid personnel access after offboarding or role change. This reduces the data exfiltration or the likelihood of compromise. Outside of deprovisioning privileged accounts, it is imperative that roles and responsibilities match the level of 'need to know'. Multiple over-privileged personnel create a higher likelihood of data mismanagement or account takeover.

Business Impact

Negative consequences of Insufficient Identity, Credentials, Access and Key Management, and Privileged Accounts may include:

- Negative business performance and productivity due to reactive and overly restrictive lockdowns
- Employee testing fatigue resulting in a lack of compliance and apathy to security
- Data replacement or corruption vs. exfiltration by unauthorized or malicious users
- Loss of trust and revenue in the market
- Financial expenses incurred due to incident response and forensics
- Ransomware and supply chain disruption

Key Takeaways

Proper IAM, credential and key management results may include:

1. Hardened defenses at the core of enterprise architectures shift hacking to endpoint user identity as low-hanging fruit.
2. Robust zero trust layer requires more than simple authentication for discrete users and application-based isolation.
3. Operational policies and structured risk are models also vital for advanced tools such as CIEM. [1]
4. User objects must be given risk scores that dynamically adjust as the business requires. Trust should be earned rather than simply providing keys and codes.

Anecdotes and Examples

Here are some recent examples of this security Issue's cloud incidents:

- (2021) State-sponsored attacks are on the rise and getting more sophisticated. 2021 saw breaches that involved Twitch, Cosmology Kozmetik, PeopleGIS, Premier Diagnostics, SeniorAdvisor, Reindeer, and Twillo, with the majority of these attacks being privilege abuse from insider threats. Companies that don't monitor risk and resilience, face a dynamic threat landscape flat-footed. [2]
- (10/2021) A closer look at SEGA Europe's cloud highlights two important configuration management cloud misconfigurations - The AWS S3 bucket was set to public access permissions. Hard-coded credentials were stored in the cloud. Content replacement in AWS and CDN networks could have been avoided if sandbox submissions were implemented, allowing systems more time to validate changes and risk-score the access context. [3]
- (1/2019 - 7/2019) CapitalOne AWS insider breach, where borrowed dynamic IAM roles were key in the breach. While S3 buckets were not exposed to the Internet like many other breaches, an EC2 instance with an excessive IAM role might have been the culprit. [4]

CSA CBK Security Guidance Version 4.0

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 11: Data Security and Encryption
Domain 12: Identity, Entitlement, and Access Management
Domain 14: Related Technologies

CSA CCM Controls Version 4.0

AIS Application and Interface Security
AIS-01: Application and Interface Security Policy and Procedures
AIS-02: Application Security Baseline Requirements
AIS-03: Application Security Metrics

CCC Change Control and Configuration Management
CCC-07: Detection of Baseline Deviation
CCC-08: Exemption Management

DSP Data Security & Privacy Lifecycle Management
DSP-03: Data Inventory
DSP-04: Data Classification
DSP-07: Data Protection by Design and Default
DSP-17: Sensitive Data Protection
DSP-19: Data Location

GRC Governance Risk and Compliance Management
GRC-02: Risk Management Program
GRC-05: Information Security Program
GRC-06: Governance Responsibility Model

IAM Identity and Access Management
IAM-01: Identity and Access Management Policy and Procedures
IAM-03: Identity Inventory
IAM-05: Least Privilege
IAM-08: User Access Review

LOG Logging and Monitoring
LOG-10: Encryption Monitoring and Reporting

IVS Infrastructure and Virtualization Security
IVS-03: Network Security
IVS-06: Segmentation and Segregation

TVM Threat & Vulnerability Management
TVM-08: Vulnerability Prioritization

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. CIEM Home - CIEM - HOME (ciemgroup.com) 2. Worst AWS Data Breachest of 2021 https://sonraisecurity.com/blog/worst-aws-data-breaches-of-2021/ 3. SEGA Europe Thoroughly Scrutinizes its Cloud Security https://vpnoverview.com/news/sega-europe-security-report/ Securin Blog | Lessons Learned from SEGA Europe's recent security blunder SEGA Barely Avoided Huge Data Breach After It Left Database Publicly Open | Eyerys 4. The Capital One - AWS incident highlights the roles and responsibilities of cloud customers, providers https://diginomica.com/capital-one-aws-incident-highlights-roles-and-responsibilities-cloud-customers-providers
✗	Tampering with Data	
✗	Repudiation	
✓	Disclosure	
✗	Denial of Service	
✗	Elevation of Privilege	

Security Issue 2:
Insecure Interfaces and APIs

API usage continues to grow in popularity; securing these interfaces has become paramount. APIs and microservices must be checked for vulnerabilities due to misconfiguration, poor coding practices, a lack of authentication and inappropriate authorization. These oversights can potentially leave the interfaces vulnerable to malicious activity. Common examples include 1. Unauthenticated endpoints; 2. Weak authentication; 3. Excessive permissions; 4. Standard security controls disabled; 5. Unpatched systems; 6. Logical design issues; and 7. Disabled logging or monitoring. Misconfiguration of APIs and other interfaces is a leading cause of incidents and data breaches. These could allow exfiltration, deletion or modification of resources, data adjustments, or service interruptions.

Security Responsibility	
✓ Customer	
✓ Cloud Service Provider	
✗ Shared	
Architecture	
✓ Application	✓ Meta
✓ Info	✗ Infra
Cloud Service Model	
✓ Software as a Service (SaaS)	
✓ Platform as a Service (PaaS)	
✓ Infrastructure as a Service (IaaS)	

Organizations are rapidly adopting APIs (as both providers and consumers) with an eye towards improved connectivity and agility. Benefits include enabling digital experiences for API developers and customers. Developers face a challenging task in managing and securing these APIs due to their rapid growth and adoption. An Akamai 2021 report documented "In [the previous year], Akamai delivered more than 300 trillion API requests—a 53% year-over-year increase." [1] The complex web of various types of API provider and consumer patterns also contributes to even cataloging APIs. Cataloging APIs must include details such as internal or external facing, what they are used for, what data are exposed and how are they consumed. Just as APIs streamline a digital ecosystem, cloud technologies are a catalyst for quickly and easily creating or using APIs. Scaling and automation will require standardizing security patterns across multiple technologies and Cloud Service Providers. Continuous monitoring and testing will also create problems at the current exponential rates.

Business Impact

The risk of an insecure interface or API varies depending on the usage and data associated with the API, as well as how quickly the vulnerability is detected and mitigated.

The most commonly reported business impact is the unintended exposure of sensitive or private data left unsecured by the API.

Key Takeaways

Here is a list of key takeaways:

1. The attack surface provided by APIs should be tracked, configured, and secured.
2. Traditional controls and change management policies and approaches need to be updated to keep pace with cloud-based API growth and change.
3. Companies should embrace automation and employ technologies that monitor continuously for anomalous API traffic and remediate problems in near real-time.

Anecdotes and Examples

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

1. (April 28, 2021) It was reported by a security researcher that an Experian partner website let anyone look up the credit score of tens of millions of Americans just by supplying their name and mailing address according to what KrebsOnSecurity has learned. While the data set belonged to the credit bureau Experian, this service was made available by third parties. [2]
2. (May 5, 2021) Broken user authentication and broken object-level authorization exposed Peloton customers' PII via APIs when called directly. This included user IDs, location, weight, gender, age, and more. [3]
3. (April 22, 2021) John Deere, a manufacturer of agricultural machinery, heavy equipment, and lawn care equipment, among other things, exposed the ability to query for usernames without authentication or rate-limiting in place. Researchers quickly determined that almost 20% of Fortune 1000 companies had John Deere accounts. Additional research led to VIN API lookups revealing equipment owner information, including address and tractor name, among other data. [4]

CSA CBK Security Guidance Version 4.0

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

CSA CCM Controls Version 4.0

AIS **Application and Interface Security**
AIS-01: Application and Interface Security Policy and Procedures
AIS-04: Secure Application Design and Development
AIS-06: Automated Secure Application Deployment

CEK **Cryptography, Encryption and Key Management**
CEK-03: Data Encryption
CEK-04: Encryption Algorithm

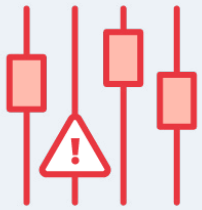
CCC **Change Control and Configuration Management**
CCC-01: Change Management Policy and Procedures
CCC-02: Quality Testing
CCC-05: Change Agreements

DSP **Data Security and Privacy Lifecycle Management**
DSP-01: Security and Privacy Policy and Procedures
DSP-03: Data Inventory
DSP-04: Data Classification
DSP-05: Data Flow Documentation

IVS **Infrastructure and Virtualization Security**
IVS-03: Network Security
IVS-04: OS Hardening and Base Controls
IVS-09: Network Defense

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. Akamai Report: https://www.ir.akamai.com/static-files/1ef574a5-ae14-48f6-854a-47d96c4a75fe 2. Experian API Exposed Credit Scores of Most Americans: https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/ 3. Peloton's Leaky API Spilled Riders' Private Data: https://threatpost.com/pelotons-spilled-riders-data/165880/ 4. Leaky John Deere API's: Serious Food Supply Chain Vulnerabilities: https://sick.codes/leaky-john-deere-apis-serious-food-supply-chain-vulnerabilities-discovered-by-sick-codes-kevin-kenney-willie-cade/
✓	Tampering with Data	
✗	Repudiation	
✓	Disclosure	
✗	Denial of Service	
✗	Elevation of Privilege	

Security Issue 3:
Misconfiguration and Inadequate Change Control



Security Responsibility	
✓ Customer	
✓ Cloud Service Provider	
✓ Shared	
Architecture	
✓ Application	✓ Meta
✓ Info	✗ Infra
Cloud Service Model	
✓ Software as a Service (SaaS)	
✓ Platform as a Service (PaaS)	
✓ Infrastructure as a Service (IaaS)	

Misconfigurations are the incorrect or sub-optimal setup of computing assets that may leave them vulnerable to unintended damage or external/internal malicious activity. Lack of system knowledge or understanding of security settings and nefarious intentions can result in misconfigurations. Some common misconfigurations are: 1. Unsecured data storage elements or containers, 2. Excessive permissions, 3. Default credentials and configuration settings are left unchanged, 4. Standard security controls disabled, 5. Unpatched systems, 6. Logging or monitoring disabled, 7. Unrestricted access to ports and services, 8. Unsecured Secrets Management, and 9. Poorly configured or lack of configuration validation. Misconfiguration of cloud resources is a leading cause of data breaches and could allow deletion or modification of resources and service interruptions.

Inadequate change control in cloud environments can result in incorrect configurations and prevent misconfigurations from being remediated. Cloud environments and cloud computing methodologies differ from traditional information technology (IT) in ways that make changes more difficult to control. Traditional change processes involve multiple roles and approvals and therefore take days or weeks before reaching production. Cloud computing best practices rely on automation, expansion of roles, and access to support rapid change. In the corporate data center, static infrastructure elements can become abstracted as code in a cloud environment. Finally, using multiple cloud providers adds complexity, with each provider's unique capabilities enhanced and expanded almost daily. This dynamic environment requires an agile and proactive approach to change control and remediation that many companies are trying to master.

Business Impact

The impact of a misconfiguration/Inadequate change control can be severe depending on the nature of the misconfiguration/improper change and how quickly it is detected and mitigated. Using the Certificate of Cloud Auditing Knowledge Study Guide, impact classifications are:

1. Disclosure of Data - Technical Impact - Confidentiality
2. Loss of Data - Technical Impact - Availability
3. Destruction of Data - Technical Impact - Integrity
4. System Performance - Operational Impact
5. System Outage - Operational Impact
6. Ransom Demands - Financial Impact
7. Non-Compliance and Fines - Compliance and Financial Impact
8. Lost Revenue - Financial Impact
9. Reduction in Stock Price - Financial Impact
10. Company Reputation - Reputational Impact

Key Takeaways

Here are some of the key takeaways:

- Companies need to embrace available technologies that scan continuously for misconfigured resources to allow remediation of vulnerabilities in real-time.
- Change management approaches must reflect the unceasing and dynamic nature of continuous business transformations and security challenges to ensure approved changes are made properly using real-time automated verification.

Anecdotes and Examples

Recent incidents resulting from misconfiguration and inadequate change control include:

1. (March 9, 2022) It was reported that nearly 70% of ServiceNow instances tested had security issues due to misconfiguration of customer-managed ServiceNow ACL (Access Control List) configurations and overprovisioning of permissions to guest users. [1]
2. (October 4, 2021) Facebook-owned apps Facebook, Instagram, Whatsapp, and Oculus went offline. Misconfigured changes interrupted communication, where the backbone routers coordinating network traffic between data centers caused issues that interrupted communication. The disruption to network traffic had a cascading effect on how the data centers communicated, bringing services to a halt. This outage also impacted many of the internal tools and systems used in day-to-day operations, complicating the issue's diagnosis and resolution. [2]
3. (January 7, 2021) it was reported that Microsoft misconfigured its own Microsoft Azure Blob (cloud) storage buckets, which housed third-party data. Over 100 "pitch decks" and source codes from companies hoping to partner with Microsoft had their ideas and intellectual property disclosed. [3]

CSA CBK Security Guidance Version 4.0

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

CSA CCM Controls Version 4.0

A&A **Audit and Assurance**
A&A-02: Independent Assessments
A&A-03: Risk-Based Planning Assessment

AIS **Application and Interface Security**
AIS-02: Application Security Baseline Requirements
AIS-04: Secure Application Design and Development
AIS-05: Automated Application Security Testing

BCR **Business Continuity Management and Operational Resilience**
BCR-02: Risk Assessment and Impact Analysis
BCR-03: Business Continuity Strategy
BCR-08: Backup

CCC **Change Control and Configuration Management**
CCC-02: Quality Testing
CCC-04: Unauthorized Change Protection
CCC-09: Change Restoration

CEK **Cryptography, Encryption & Key Management**
CEK-03: Data Encryption
CEK-05: Encryption Change Management

DSP **Data Security & Privacy Lifecycle Management**
DSP-07: Data Protection by Design and Default
DSP-08: Data Privacy by Design and Default
DSP-17: Sensitive Data Protection

GRC **Governance Risk and Compliance Management**
GRC-02: Risk Management Program
GRC-05: Information Security Program

HRS **Human Resources**
HRS-09: Personnel Roles and Responsibilities
HRS-11: Security Training / Awareness

IAM **Identity and Access Management**
IAM-03: Identity Inventory
IAM-08: User Access Review

IVS **Infrastructure and Virtualization Security**
IVS-02: Change Detection
IVS-03: Network Security
IVS-04: OS Hardening and Base Controls

LOG **Logging and Monitoring**
LOG-03: Security Monitoring and Alerting
LOG-05: Audit Logs Monitoring and Response
LOG-12: Access Control Logs

SEF **Security Incident Management, E-Discovery, & Cloud Forensics**
SEF-03 Incident Response Plans
SEF-04 Incident Response Testing
SEF-06 Event Triage Processes

TVM **Threat & Vulnerability Management**
TVM-07 Vulnerability Identification
TVM-08 Vulnerability Prioritization
TVM-09 Vulnerability Management Reporting

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. Major Security Misconfiguration Impacting ServiceNow Instances Discovered https://appomni.com/press_release/2022-major-security-misconfiguration-impacting-servicenow-and-other-saas-instances-discovered/ Major Security Misconfiguration Impacting ServiceNow and Other SaaS Instances Discovered https://appomni.com/resources/aolabs/appomni-discovers-security-misconfiguration-impacting-servicenow/ ServiceNow Shared Security Model and Access Control Information https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1095978 ServiceNow releases guidance on Access Control List misconfigurations https://www.zdnet.com/article/servicenow-releases-guidance-on-access-control-list-misconfigurations-after-report-highlights-prevalence/ 2. Understanding How Facebook Disappeared from the Internet https://blog.cloudflare.com/october-2021-facebook-outage/ Update about the October 4th outage https://engineering.fb.com/2021/10/04/networking-traffic/outage/ More details about the October 4 outage https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/ Why Facebook, Instagram, and WhatsApp All Went Down Today https://www.wired.com/story/why-facebook-instagram-whatsapp-went-down-outage/ 3. Report: Software Companies Exposed to Hacking in Major Data Breach https://www.vpnmentor.com/blog/report-microsoft-dynamics-leak/ *Additional:* 4. Report: Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach https://www.websiteplanet.com/blog/prestige-soft-breach-report/ Leaky AWS S3 bucket once again at centre of data breach https://www.computerweekly.com/news/252491842/Leaky-AWS-S3-bucket-once-again-at-centre-of-data-breach 5. Unsecured-aws-server-exposed-airport-employee-records-3tb-in-data https://www.zdnet.com/article/unsecured-aws-server-exposed-airport-employee-records-3tb-in-data/ 6. https://www.zdnet.com/article/amazon-steps-in-to-close-exposed-flexbooker-bucket-after-december-data-breach/
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	
✓	Elevation of Privilege	

Security Issue 4:

Lack of Cloud Security Architecture and Strategy

Cloud security strategy and security architecture encompasses the consideration and selection of cloud deployment models, cloud service models, cloud service providers (CSPs), service region availability zone, specific cloud services, general principles[1], and pre-determinations[2]. Furthermore, a forward-looking design of IAM[3], networking and security controls across different cloud accounts, vendors, services, and environments are in scope. Consideration of strategy should precede and dictate design, but it is common that cloud challenges demand an incremental and agile approach to planning.

Security Responsibility
✓ Customer
✗ Cloud Service Provider
✗ Shared
Architecture
✓ Application ✓ Meta
✓ Info ✓ Infra
Cloud Service Model
✓ Software as a Service (SaaS)
✓ Platform as a Service (PaaS)
✓ Infrastructure as a Service (IaaS)

The fast pace of change and the prevalent, decentralized, self-service approach to cloud infrastructure administration hinder the ability to account for technical and business considerations and conscious design. However, security considerations and risks must not be ignored if cloud endeavors are to be successful and safe. Industry breach cases anecdotes show that lacking such planning may lead to cloud environments and applications failing to become resilient to cyber attacks, or efficiently do so. These same challenges can contribute to the easier implementation of cloud security strategy and design.

Business Impact

The absence of a cloud security strategy and architecture limits the viability for effective and efficient enterprise and infrastructure security architecture to be implemented. Without these security/compliance goals will fail to be met, resulting in fines and breaches, or doing so will be costly due to implementing workarounds, refactoring and migrating.

1 general cloud computing principles could encompass preference for CSP based on impact (national or social) considerations ('local first, etc') or, - tolerance of avoidance of on-demand service consumption and billing models; some love it because it eliminates friction, others avoid because it makes budgeting less predictable. its interesting because it isn't binary and because it affects both the design of your technology and is impactful enough to consider under 'strategy' - at scale and early on.

2 pre-determinations can encompass existing vendor lock-ins, business intentions to expand in a certain region which require local data residency, a company-wide preference for a certain CSP or model (like 0-servers footprint which I've seen attempt to be adopted even in banking).

3 identity and access management, as a domain, not a specific cloud service.

Key Takeaways

Here are some of the key takeaways:

- Companies should consider business objectives, risk, security threats, and legal compliance in cloud services and infrastructure design and decisions.
- Consider cloud services and infrastructure strategy and design principles more important to develop and adhere to, given the rapid pace of change and limited centralized control.
- Consider due diligence and third-party vendor security assessments as foundational practices. Complement with threat modeling, secure design and integration with an eye toward vendor failure impacts.

Anecdotes and Examples

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

- (January 2021) US Clothing store, Bonobos, owned by Walmart, suffered a massive data breach exposing millions of customers' personal information. A threat actor known as ShinyHunters posted the full Bonobos database (70 GB of SQL database containing 7 million user records) inclusive of customers' addresses, phone numbers, partial credit card numbers, and orders made on the site. This occurred due to a compromise of an external cloud backup service hosting the backup file. A selection of access controls, encryption, vendor security, redundancy, and other domains can be employed to limit impacts or likelihood of similar breaches. [1] [2]
- (July 2, 2021) Kaseya received reports from customers suggesting unusual behavior and malware executing on endpoints managed by Kaseya. Attackers could exploit zero-day vulnerabilities in the virtual storage appliance (VSA) product to bypass authentication and run arbitrary command execution. This allowed the attackers to leverage the standard VSA product functionality to deploy ransomware to the endpoints of manage service provider (MSP) clients (i.e., clients of clients). This failure affected many customers due to a strategy of automated, zero-touch updates to software deployed in different environments, and a SaaS model of critical software change management; vendors and consumers can reconsider this strategy to limit similar attacks in the future. [3]

CSA CBK Security Guidance Version 4.0

Domain 1: Cloud Computing Concepts and Architectures
Domain 2: Governance and Enterprise Risk Management
Domain 6: Management Plane and Business Continuity

CSA CCM Controls Version 4.0

A&A Audit and Assurance
A&A-03 Risk Based Planning Assessment
A&A-04 Requirements Compliance

AIS Application and Interface Security
AIS-04 Secure Application Design and Development

BCR Business Continuity Management and Operational Resilience
BCR-02 Risk Assessment and Impact Analysis
BCR-03 Business Continuity Strategy
BCR-04 Business Continuity Planning
BCR-08 Backup

CEK Cryptography, Encryption & Key Management
CEK-08 CSC Key Management Capability
CEK-07 Encryption Risk Management

DCS Datacenter Security
DCS-01 Off-Site Equipment Disposal Policy and Procedures

DSP Data Security & Privacy Lifecycle Management
DSP-07 Data Protection by Design and Default
DSP-05 Data Flow Documentation
DSP-01 Security and Privacy Policy and Procedures
DSP-09 Data Protection Impact Assessment

GRC Governance Risk and Compliance Management
GRC-08 Special Interest Groups
GRC-02 Risk Management Program

IAM Identity and Access Management
IAM-04 Separation of Duties
IAM-05 Least Privilege
IAM-09 Segregation of Privileged Access Roles
IAM-01 Identity and Access Management Policy and Procedures
IAM-06 User Access Provisioning

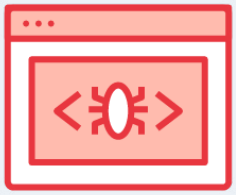
IPY Interoperability & Portability
IPY-01 Interoperability and Portability Policy and Procedures

IVS Infrastructure and Virtualization Security
IVS-03 Network Security
IVS-05 Production and Non-Production Environments
IVS-08 Network Architecture Documentation
IVS-06 Segmentation and Segregation

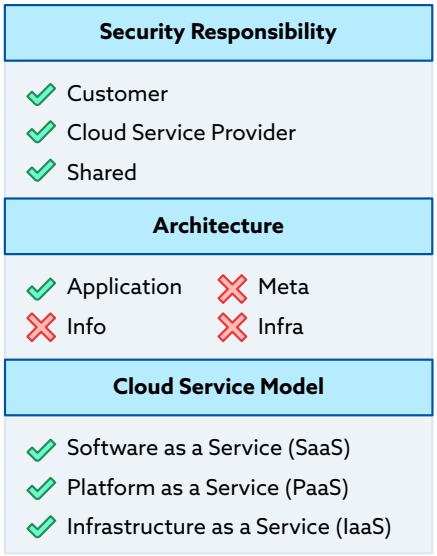
STA Supply Chain Management, Transparency and Accountability
STA-01 SSRM Policy and Procedures
STA-08 Supply Chain Risk Management

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. Incident Overview & Technical Details https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961 2. Independence Day: REvil uses supply chain exploit to attack hundreds of businesses https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/ 3. Data breach at Bonobos hits up to 7 million: What to do [updated] https://www.tomsguide.com/news/bonobos-data-breach-7-million
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	
✓	Elevation of Privilege	

Security Issue 5:
Insecure Software Development



Software is complex, with cloud technologies tending to add to the complexity . In that complexity, unintended functionality emerges which could allow for the creation of exploits [1] and likely misconfigurations. Thanks to the accessibility of the cloud, threat actors can leverage these "features" more easily than ever before.



Adopting a cloud first strategic posture allows entities to offload maintenance and security headaches to a cloud service provider (CSP). Entrusting a CSP to manage the infrastructure and/or platform layers prevents developers from reinventing the wheel. Services for key storage/management and secure Continuous Integration/Continuous Deployment (CI/CD) allow developers to direct their focus on business logic.

CSPs will offer features for identity and access management (IAM), giving developers vetting tools and guidance on proper implementation. This in turn removes the need for companies building services themselves, which frees resources to be invested in more impactful business priorities.

Ensuring each developer understands the company's assumptions of shared responsibilities with the CSP requires education. For example, if an 0-day exploit was reported for Kubernetes and a company is leveraging its CSP's Kubernetes solutions, the CSP owns the responsibility to mitigate the issue. A web application using cloud native technologies with a business error would be the responsibility of the developer to fix. In either case, resultant information disclosures impact the company.

No developer sets out to create insecure software. Yet, every month patches are released by major software vendors fixing bugs that can be used to impact the confidentiality, integrity, and/or availability of a system. Not all software bugs have security implications, but as history has proven, even odd quirks can become significant threats [2]. Embracing cloud technologies allows companies to hone their focus on that which is unique to their business, while letting the CSP own and manage everything else that may be commoditized.

Business Impact

Some of the effects of insecure software development include:

- Loss of customer confidence of the product or solution
- Damage to brand reputation due to a data breach
- Legal and financial impact due to lawsuits.

Key Takeaways

Here are some of the key takeaways:

- Using cloud technologies prevents reinventing existing solutions, allowing developers to focus on issues unique to the business.
- By leveraging the shared responsibility model, items like patching can be owned by a CSP, rather than the business.
- CSPs place an importance on security, and will offer guidance on how to implement services in a secure fashion, such as a Well Architected Framework or secure design patterns.

Anecdotes and Examples

Recent examples of issues related to account hijacking include:

- (December 9, 2021) The infamous Log4Shell vulnerability allowed RCE trivially due to a parsing bug in the log4j library [3].
- (January 5, 2021) The ubiquitous Microsoft Exchange saw a family of vulnerabilities released (ProxyOracle, ProxyShell), providing several avenues for remote code execution and credential theft [4].
- (September 13, 2021) Apple's iOS was discovered to be exploited by NSO's Pegasus software, leveraging a zero-click vulnerability that could allow remote code execution [5].

CSA CBK Security Guidance Version 4.0

Domain 1: Cloud Computing Concepts and Architecture
Domain 10: Application Security
Domain 12: Identity, Entitlement, and Access Management
Domain 13: Security as a Service

CSA CCM Controls Version 4.0

AIS Application and Interface Security
AIS-02: Application Security Baseline Requirements
AIS-04: Secure Application Design and Development
AIS-05: Automated Application Security Testing
AIS-06: Automated Secure Application Deployment

CCC Change Control and Configuration Management
CCC-02: Quality Testing

TVM Threat & Vulnerability Management
TVM-04: Detection Updates

IAM Identity and Access Management
IAM-01: Identity and Access Management Policy and Procedures
IAM-04: Segregation of Duties
IAM-05: Least Privilege
IAM-14: Strong Authentication
IAM-16: Authorization Mechanisms

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. I always call them glue bugs, I think I got that from you! https://twitter.com/taviso/status/1379447309864345602 2. An Exploration of JSON Interoperability Vulnerabilities https://bishopfox.com/blog/json-interoperability-vulnerabilities 3. Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package https://www.lunasec.io/docs/blog/log4j-zero-day/ 4. A New Attack Surface on MS Exchange Part 1 - ProxyLogon! https://blog.orange.tw/2021/08/proxylogon-a-new-attack-surface-on-ms-exchange-part-1.html 5. A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	
✓	Elevation of Privilege	

Security Issue 6:
Unsecure Third-Party Resources

Security Responsibility
✓ Customer
✓ Cloud Service Provider
✓ Shared
Architecture
✓ Application ✓ Meta
✓ Info ✓ Infra
Cloud Service Model
✓ Software as a Service (SaaS)
✓ Platform as a Service (PaaS)
✓ Infrastructure as a Service (IaaS)

In a world where cloud computing adoption is increasing rapidly, a third-party resource could mean different things: from open source code, through SaaS products and API risks (Security Issue 2), and all the way to a managed service provided by a cloud vendor. Risks stemming from third-party resources are also considered supply chain vulnerabilities since they are a part of the process of delivering your products or services. These risks exist in every product and service consumed. Still, due to the increasing reliance on third-party services and software-based products in recent years, more exploits of these vulnerabilities and hackable configurations occur. In fact, according to research from Colorado State University, two-thirds of breaches are a result of supplier or third-party vulnerabilities.

Because a product or service is a sum of all the other products and services they are using, the exploit can start at any point in the chain, and proliferate from there. For the malicious hacker, this means that to achieve their goal, they "only" need to look for the weakest link as an entry point. In the world of software, it's a common practice to use SaaS and open source to scale. Malicious hackers receive the same opportunity to grow, hurting more targets with the same exploit.

Business Impact

- Loss or stoppage of key business processes.
- Business data being accessed by outside parties (Security Issue 11).
- Patching or fixing a security issue depends on the provider and how quickly they respond. Once they provide the fix, integration might require updating internal applications and products. Impact on a business can be crucial, depending on the importance of the vulnerable component to an application.

Key Takeaways

Here are some of the key takeaways:

- You can't prevent vulnerabilities in code or products you didn't create, but you can try and make a good decision about which product to use. Look for the products that are officially supported; Also those with compliance certifications, who are openly speaking about their security efforts, who have a bug bounty program, and who treat their users responsibly by reporting security issues and delivering fixes quickly.
- Identify and track the third parties you are using. You don't want to find out you've been using a vulnerable product only when the list of victims is published. This includes open-source, SaaS products, cloud providers and managed services, and other integrations you may have added to your application.
- Perform a periodic review of the third-party resources. If you find products you don't need, remove them and revoke any access or permissions you may have granted them into your code repository, infrastructure, or application.
- Don't be the weakest link. Penetration-test your application within an applicable scope ideal for your company, teach your developers about secure coding, and use static application security testing (SAST) and dynamic application security testing (DAST) solutions.

Anecdotes and Examples

Recent third-party-related issues include:

- (December 13, 2020, through April 6, 2021) Solarwinds is a US-based network monitoring company. In 2020, it was published that thousands of its government and private customers were hurt in a supply chain attack that used different vectors, leading from the Solarwinds network and products into their customers' networks, credentials, and private data. The real effect of this attack is still unknown. Due to the sensitive data that was exfiltrated, some organizations had to rebuild their entire networks and servers. [1] [2]
- (November 2021) Log4shell is a zero-day vulnerability found in the popular open-source Java logging framework Log4j. The vulnerability was disclosed in November 2021 and patched a few days later. It is considered the largest vulnerability ever due to the popularity of this framework. The attackers used this vulnerability for crypto mining, ransomware attacks, botnets, and spamming. [3] [4]
- (May 2019 until August 2021) The North American subsidiary of The Volkswagen Group suffered from a data breach caused by one of its vendors, who left a storage service unprotected for almost two years, from May 2019 until August 2021. The breached data included Personally Identifiable Information (PII) and, for some customers, more sensitive financial data, and involved 3.3 million customers. [5] [6]

CSA CBK Security Guidance Version 4.0

Domain 1: Cloud Computing Concepts and Architectures
Domain 2: Governance and Enterprise Risk Management
Domain 7: Infrastructure Security
Domain 10: Application Security
Domain 12: Identity, Entitlement, and Access Management

CSA CCM Controls Version 4.0

BCR Business Continuity Management and Operational Resilience
BCR-01: Business Continuity Management Policy and Procedures
BCR-02: Risk Assessment and Impact Analysis
BCR-03: Business Continuity Strategy

CCC Change Control and Configuration Management
CCC-04: Unauthorized Change Protection
CCC-05: Change Agreements

DCS Datacenter Security
DCS-05: Assets Classification
DCS-06: Assets Cataloging and Tracking
DCS-07: Controlled Access Points

DSP Data Security & Privacy Lifecycle Management
DSP-03: Data Inventory
DSP-05: Data Flow Documentation
DSP-06: Data Ownership and Stewardship
DSP-08: Data Privacy by Design and Default
DSP-10: Sensitive Data Transfer
DSP-16: Data Retention and Deletion

IAM Identity and Access Management
IAM-05: Least Privilege
IAM-10: Management of Privileged Access Roles
IAM-11: CSCs Approval for Agreed Privileged Access Roles
IAM-14: Strong Authentication
IAM-16: Authorization Mechanisms

IPY Interoperability & Portability
IPY-01: Interoperability and Portability Policy and Procedures
IPY-02: Application Interface Availability
IPY-03: Secure Interoperability and Portability Management
IPY-04: Data Portability Contractual Obligations

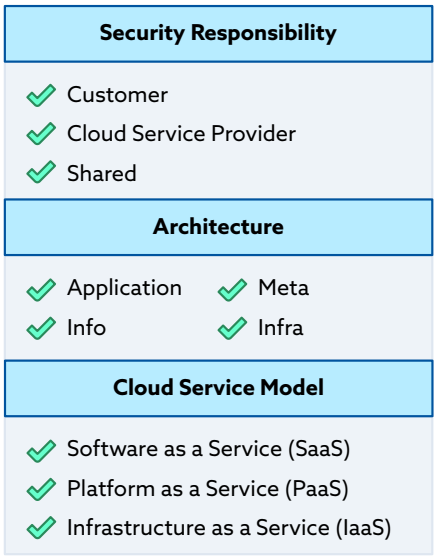
SEF Security Incident Management, E-Discovery, & Cloud Forensics
SEF-01: Security Incident Management Policy and Procedures
SEF-03: Incident Response Plans
SEF-07: Security Breach Notification

STA Supply Chain Management, Transparency and Accountability
STA-01: SSRM Policy and Procedures
STA-02: SSRM Supply Chain
STA-03: SSRM Guidance
STA-04: SSRM Control Ownership
STA-05: SSRM Documentation Review
STA-06: SSRM Control Implementation
STA-07: Supply Chain Inventory
STA-08: Supply Chain Risk Management
STA-09: Primary Service and Contractual Agreement
STA-10: Supply Chain Agreement Review
STA-11: Internal Compliance Testing
STA-12: Supply Chain Service Agreement Compliance
STA-13: Supply Chain Governance Review
STA-14: Supply Chain Data Security Assessment

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. Solarwinds the supply chain hack https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/ 2. Using Microsoft for the Solarwinds hack https://www.reuters.com/article/us-global-cyber-usa-idUSKBN28Y1BF 3. Log4J hack https://blog.cloudflare.com/inside-the-log4j2-vulnerability-cve-2021-44228/ 4. More than 1.2m attacks using log4j https://www.ft.com/content/d3c244f2-eaba-4c46-9a51-b28fc13d9551 5. Volkswagen and Audi customer's data leakage https://www.bleepingcomputer.com/news/security/audi-volkswagen-data-breach-affects-33-million-customers/ 6. Two third of breaches are supply chain attacks https://www.nationaldefensemagazine.org/articles/2020/7/2/hackers-putting-global-supply-chain-at-risk
✗	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✗	Denial of Service	
✓	Elevation of Privilege	

Security Issue 7:
System Vulnerabilities

System vulnerabilities are flaws in cloud service platforms. They may be exploited in an attempt to compromise confidentiality, integrity, and availability of data, potentially disrupting service operations. All components can contain vulnerabilities that may leave cloud services open to attack. Implementing security hardening practices that align with the below vulnerability categories is essential to mitigating their security risks.



There are four main categories of system vulnerabilities:

- **Zero-day vulnerabilities** - Newly discovered vulnerabilities for which patches do not exist. Hackers work quickly to exploit vulnerabilities like these since there is nothing to stop them until patches are deployed. The recently discovered Log4Shell is a notable example of a serious zero-day vulnerability that affected services using the widely deployed Java-based Log4j logging facility.
- **Missing security patches** - Once patches to known critical vulnerabilities become available, deploying them as soon as possible reduces the system's attack surface. Over time, newer system vulnerabilities will be discovered and patches made available. As the number of unpatched vulnerabilities increases, so does the overall system security risk.
- **Configuration-based vulnerabilities** - This kind of vulnerability arises when a system is deployed with default or misconfigured settings. Examples of configuration-based vulnerabilities include using legacy security protocols, weak encryption ciphers, weak permissions, and inadequately protected system management interfaces. Running unnecessary services on a system is another configuration-related issue.
- **Weak or default credentials** - The lack of strong authentication credentials provides potential attackers easy access to system resources and associated data. Similarly, passwords not stored securely may be stolen and used to break into systems.

Business Impact

- Many successful data breaches result from attacks that exploit system vulnerabilities. IBM's *Cost of Data Breach 2021 Report* [2] indicated that vulnerabilities in third-party software were responsible for 14% of the data breaches studied, while cloud misconfiguration and compromised credentials accounted for 20% and 15%, respectively.
- When a data breach occurs, a company's business can be disrupted, preventing customers from using the company's services. In the aftermath of a breach, acquiring new customers may be harder if the company's brand and services are no longer trusted. Both outcomes can translate to a loss of revenue.

- The IBM report identified four data breach cost centers and their average cost per incident in millions of USD. Detection and escalation accounted for 29% of the breaches ($1.24 million), notification 6% ($0.27 million), post-breach response 27% ($1.14 million), and loss of business 38% ($1.59 million). The total cost per incident was $4.24 million. The data breaches in these cases involved 2k to 101k compromised records. For large breaches of 50 million to 65 million records, the total average cost per incident was $401 million.

Key Takeaways

Here are some of the key takeaways:

- System vulnerabilities are flaws within system components often introduced through human error, making it easier for hackers to attack a company's cloud services.
- Post Incident Response is a costly proposition. Losing company data can negatively impact a business's bottom line in revenue and reputation.
- Security risks due to system vulnerabilities can be greatly minimized through routine vulnerability detection and patch deployment combined with rigorous IAM practices.

Anecdotes and Examples

Recent examples of issues related to system vulnerabilities include:

- (December 9, 2021) Log4Shell vulnerability CVE-2021-45046 is a remote-code vulnerability that affects the Java-based Log4j logging facility versions 2.0beta9 to 2.14.1. Log4Shell is a severe threat given the widespread use of Java in cloud systems. Attackers can exploit Log4Shell by submitting a malicious request to a vulnerable system that causes the system to execute arbitrary code enabling the attacker to steal information, launch ransomware, or take over control of the system. The CISA, FBI, NSA, and other government organizations expect the exploitation of Log4Shell to continue for an extended time. [1]
- (August 2021) Security researchers at cloud security company Wiz disclosed that they gained complete access to the data of several thousand Microsoft Azure customers. Security flaws in Azure's CosmosDB, referred to by the researchers as ChaosDB, the vulnerability allowed users to download, delete, or otherwise manipulate data without user credentials. [2]
- (September 2021) Researchers at Microsoft observed a cyberespionage group with ties to the Russian government deploying a backdoor that exploits ActiveDirectory Federation and steals configuration databases and security tokens. Microsoft refers to the malware as FoggyWeb and attributes it to the Russian hacker group APT29 (aka Cozy Bear and NOBELIUM). [2]
- (2021) According to Ivanti's Ransomware Spotlight Year-End 2021 Report, the number of vulnerabilities associated with ransomware attacks rose from 233 in 2020 to 288 in 2021, representing an increase of 29%. [3]

CSA CBK Security Guidance Version 4.0

Domain 7: Infrastructure Security
Domain 10: Application Security
Domain 11: Data Security and Encryption
Domain 12: Identity, Entitlement, and Access Management

CCM Controls Version 4.0

AIS Application and Interface Security
AIS-01: Application Security Policy and Procedures
AIS-02: Application Security Baseline Requirements
AIS-06: Automated Secure Application Deployment
AIS-07: Application Vulnerability Remediation

CEK Cryptography, Encryption & Key Management
CEK-03: Data Encryption
CEK-04: Encryption Algorithm

IAM Identity and Access Management
IAM-02: Strong Password Policy and Procedures
IAM-14: Strong Authentication
IAM-15: Passwords Management
IAM-16: Authorization Mechanisms

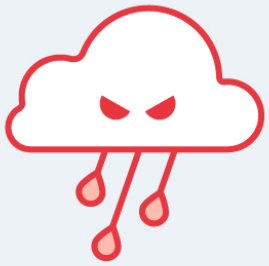
IVS Infrastructure and Virtualization Security
IVS-04: OS Hardening and Base Controls

TVM Threat and Vulnerability Management
TVM-01: Threat and Vulnerability Management Policy and Procedures
TVM-02: Malware Protection Policy and Procedures
TVM-03: Vulnerability Remediation Schedule
TVM-04: Detection Updates
TVM-05: External Library Vulnerabilities
TVM-06: Penetration Testing
TVM-07: Vulnerability Identification
TVM-08: Vulnerability Prioritization
TVM-09: Vulnerability Management Reporting

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. Log4Shell 0-day Vulnerability: All You Need to Know https://jfrog.com/blog/log4shell-0-day-vulnerability-all-you-need-to-know/ 2. Microsoft's very bad year for security: A timeline https://www.csoonline.com/article/3635849/microsofts-very-bad-year-for-security-a-timeline.html 3. Ransomware Spotlight Year End 2021 Report (Ivanti) https://www.ivanti.de/lp/security/reports/ransomware-spotlight-year-end-2021-report Additional: 1. 2021 marks another record year for security vulnerabilities https://www.techrepublic.com/article/2021-marks-another-record-year-for-security-vulnerabilities/ 2. Cost of Data Breach Report (IBM) https://www.ibm.com/security/data-breach 3. Cybersecurity vulnerabilities and their business impact https://www.verizon.com/business/resources/articles/s/cyber-security-vulnerabilities-and-their-business-impact 4. Mitigating Log#Shell and Other Log4j-Related Vulnerabilities https://www.cisa.gov/uscert/ncas/alerts/aa21-356a 5. The Internet is on Fire https://www.wired.com/story/log4j-flaw-hacking-internet/ 6. Ransomware attacks are increasingly exploiting security vulnerabilties https://www.techrepublic.com/article/ransomware-attacks-are-increasingly-exploiting-security-vulnerabilities/ 7. Top Routinely Exploited Vulnerabilities https://www.cisa.gov/uscert/ncas/alerts/aa21-209a 8. What are the different types of vulnerabilities? https://www.packetlabs.net/types-of-vulnerabilities/
✗	Repudiation	
✓	Disclosure	
✗	Denial of Service	
✓	Elevation of Privilege	

Security Issue 8:

Accidental Cloud Data Disclosure



Cloud services enable companies to build, innovate, and scale at a pace never seen before. However, the complexity of the cloud and a shift to cloud-service ownership, with diverse teams and business units, often leads to a lack of security governance and control. Increasing numbers of configurations for cloud resources in different CSPs make misconfigurations more common, and the lack of transparency into cloud inventory and adequate network exposure can lead to unintentional data leaks.

Security Responsibility
✓ Customer
✓ Cloud Service Provider
✓ Shared
Architecture
✓ Application ✓ Meta
✓ Info ✗ Infra
Cloud Service Model
✓ Software as a Service (SaaS)
✓ Platform as a Service (PaaS)
✓ Infrastructure as a Service (IaaS)

Data exposure is still widespread. Over 55% of companies have at least one database that is currently publicly exposed to the internet [1]. Many of these databases use weak passwords or do not require authentication, making them an easy target for attackers who continuously scan the internet searching for such exposed databases. Considering that an unsecured Elasticsearch server can be breached in eight hours [2], such exposures must be fixed as soon as possible.

Business Impacts

The ease of use of the cloud, and specifically, the speed at which managed databases and storage objects can be set up makes them extremely popular.

- These databases can contain sensitive customer data, employee information, product data, and more. Exposure of such data results in unexpected expenses - to forensic teams, customer support processes, and compensation to affected customers.
- According to IBM Research [3], in 2021, data breach costs rose from USD 3.86 million to USD 4.24 million. In their report, IBM mentions additional indirect costs of data breaches, such as in-house investigation and communication, current customer loss, and future customer loss due to the impact of the trust in the company.

Key Takeaways

To prevent unintentional data leaks, we suggest cloud customers ensure they can answer the following questions easily:

1. Review your PaaS Databases, storage, and compute workloads hosting databases. Include VMs, containers, and the DB software installed on them. Configuration-based solutions have

limited capabilities to provide the necessary visibility and cannot inspect or scan workloads.
2. Choose exposure engines that have full visibility of your cloud environment to identify any routing or network services that allow traffic to be exposed externally. Includes load balancers, application load balancers, CDNs, network peering, cloud firewalls, Kubernetes networking, etc...
3. Reduce access exposure by ensuring that databases implement least-privileged IAM policy, and assignments of this policy are controlled and monitored.

Anecdotes and Examples

Recent examples of Accidental Cloud Data Disclosure issues include:

- VIP Games, 23M records, January 2021 - A cloud misconfiguration exposed 23M records of over 60K users containing emails, user names, social issues al network ID, and player data on the web [4].
- Reverb, 5.6M records, April 2021 – Elasticsearch storing 5.6M customer records were exposed on the web [5].
- The Telegraph, 10TB records, September 2021 - UK newspaper The Telegraph exposed a 10TB database with subscriber data [6].
- Securitas, 1M records, January 2022 - Unauthenticated AWS server exposed 3TB in airport employee records. [7]
- FlexBooker, 19M records, February 2022 - Amazon steps in to close the exposed FlexBooker bucket after the December data breach. [8]

CSA CBK Security Guidance Version 4.0

Domain 5: Information Governance
Domain 7: Infrastructure Security
Domain 12: Identity, Entitlement and Access Management

CSA CCM Controls Version 4.0

AIS **Application and Interface Security**
AIS-02: Application Security Baseline Requirements
AIS-04: Secure Application Design and Development

IAM **Identity and Access Management**
IAM-01: Identity and Access Management Policy and Procedures
IAM-03: Identity Inventory

BCR **Business Continuity Management and Operational Resilience**
BCR-05: Documentation

DSP **Data Security and Information Lifecycle Management**
DSP-03: Data Inventory
DSP-08: Data Protection by Design and Default

GRC **Governance, Risk and Compliance**
GRC-01: Governance Program Policy and Procedures
GRC-02:Risk Management Program

IVS **Infrastructure and Virtualization Security**
IVS-01: Infrastructure and Virtualization Security Policy and Procedures
IVS-03: Network Security
IVS-06: Segmentation And Segregation

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. 2022 Cloud Security Threats report https://www.wiz.io/ty/2022-cloud-security-threats-report 2. Unsecured Elasticsearch server breached in eight hours flat https://www.computerweekly.com/news/252484365/Unsecured-ElasticSearch-server-breached-in-eight-hours-flat 3. How much does a data breach cost? https://www.ibm.com/security/data-breach 4. A cloud misconfiguration exposed 23M records of over 60K users containing emails, user names, social network ID, and player data on the web https://portswigger.net/daily-swig/online-gaming-platform-vip-games-exposes-23-million-data-records-on-misconfigured-server 5. Elasticsearch storing 5.6M customer records was exposed on the web https://www.bitdefender.com/blog/hotforsecurity/etsy-owned-musical-instrument-marketplace-reverb-suffers-data-breach 6. UK newspaper The Telegraph exposed 10TB database with subscriber data https://securityaffairs.co/wordpress/123020/data-breach/the-telegraph-data-leak.html 7. Unauthenticated AWS server exposed 3TB in airport employee records https://www.zdnet.com/article/unsecured-aws-server-exposed-airport-employee-records-3tb-in-data/ 8. Amazon steps in to close exposed FlexBooker bucket after December data breach https://www.zdnet.com/article/amazon-steps-in-to-close-exposed-flexbooker-bucket-after-december-data-breach/
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✗	Denial of Service	
✗	Elevation of Privilege	

Security Issue 9:

Misconfiguration and Exploitation of Serverless and Container Workloads

The migration to cloud infrastructure and adoption of DevOps practices enable IT teams to deliver value to the business faster than ever. Managing and scaling the infrastructure and security controls to run applications is still a significant burden on development teams. Legacy infrastructure teams used to managing on-prem environments must learn new skills like Infrastructure as Code and cloud security. The same teams must take on more responsibility for the network and security controls supporting their applications. Serverless and cloud-native containerized workloads can seem like a silver bullet for this problem, offloading that responsibility to the cloud service provider (CSP). Still, it requires a higher level of cloud and application security maturity than migrating virtual machines to the cloud.

Security Responsibility	
✓ Customer	
✓ Cloud Service Provider	
✓ Shared	
Architecture	
✗ Application	✓ Meta
✓ Info	✗ Infra
Cloud Service Model	
✗ Software as a Service (SaaS)	
✓ Platform as a Service (PaaS)	
✓ Infrastructure as a Service (IaaS)	

In a serverless model, the CSP takes responsibility for the security and management of the underlying infrastructure. In addition to the development and operational benefits, this reduces attack surface because CSPs run function code in short-lived containers by default. The constantly refreshing system significantly limits persistence in the event of an exploit. However, if a CSP allows customers to configure serverless containers with longer lifetimes and "warm start" configurations, the environment becomes less secure. Additional risks include a temporary file system and shared memory may also leak sensitive information. Access to the temporary storage may be used to host or execute malware and should be wiped by application code.

The serverless responsibility model results in a more nuanced and complex environment. In an analysis done by Netskope, 4% of IAM policies analyzed had full administrative access, and 60% had the AWS AdministratorAccess role [1]. Supposing those permissions were assigned to a public-facing AWS serverless Lambda function, vulnerabilities could be numerous. Access to cloud environments, sensitive data leakage, or AWS account takeovers are all possibilities.

The lack of control over the infrastructure also limits mitigation options for application security issues and the visibility of traditional security tooling. This makes it critical to build strong organizational practices around cloud hygiene, application security, observability, access control, and secrets management to reduce the blast radius of an attack.

Business Impact

Serverless and containerized workloads can significantly increase agility, reduce cost, simplify operations, and even increase security. Applications implemented with serverless technology without the necessary expertise and due diligence can result in major breaches, data loss, and financial exhaustion.

Key Takeaways

Here are some of the key takeaways:

- Companies should implement automated checking through Cloud Security Posture Management, Cloud Infrastructure Entitlement Management, and Cloud Workload Protection Platforms.
- Investments should be made into cloud security training, governance processes, and reusable secure cloud architecture patterns to reduce the risk and frequency of insecure cloud configurations.
- Development teams should put extra rigor around strong application security and engineering best practices before migrating to serverless technologies that remove traditional security controls.

Anecdotes and Examples

Recent examples of issues related to serverless and container exploit include:

- As of 2021, there's a growing body of research around Denial of Wallet (DoW) attacks. A DoW attack is functionally similar to a Denial of Service (DoS) attack. The attacker sends a large volume of requests to a serverless application to impact the underlying infrastructure. But in a DoW attack, the objective is to cost a cloud customer money by taking advantage of the auto-scaling consumption model of serverless platforms. These attacks can be mitigated with concurrency limits, but that changes the attack vector from Denial of Wallet to Denial of Service. [2]
- (2021) Several escape vulnerabilities were discovered across different container runtimes and environments, including CVE-2022-0811 (CRI-O container escape vulnerability) [3], CVE-2022-0185 (Linux Kernel buffer overflow [4], and Azurescape [5]. Each of these vulnerabilities creates the potential for an attacker to escape the container environment and gain privileged access to the container host. In the case of Azurescape, this even allowed the potential of running code in another Azure customer's Azure Container Instance environment.
- (February 2022) Researchers from Cado Labs found evidence of the first known malware to directly target AWS Lambda, dubbed Denonia, being actively used in the wild. Denonia is a Monero mining Lambda function that uses DNS over HTTPS to communicate with the C2 server. While this malware does not exploit any vulnerabilities in Lambda and would require administrative privilege to deploy, it is an example of how attackers can use serverless environments for financial gain at an organization's expense. [6]

CSA CBK Security Guidance Version 4.0

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

CSA CCM Controls Version 4.0

A&A **Audit and Assurance**
A&A-02: Independent Assessments
A&A-03: Risk Based Planning Assessment
A&A-04: Requirements Compliance
A&A-05: Audit Management Process
A&A-06: Remediation

AIS **Application and Interface Security**
AIS-02: Application Security Baseline Requirements
AIS-03: Application Security Metrics
AIS-04: Secure Application Design and Development
AIS-05: Automated Application Security Testing
AIS-06: Automated Secure Application Deployment
AIS-07: Application Vulnerability Remediation

BCR **Business Continuity Management and Operational Resilience**
BCR-02: Risk Assessment and Impact Analysis
BCR-03: Business Continuity Strategy

CCC **Change Control and Configuration Management**
CCC-02: Quality Testing
CCC-04: Unauthorized Change Protection
CCC-09: Change Restoration

CEK **Cryptography, Encryption & Key Management**
CEK-03: Data Encryption
CEK-05: Encryption Change Management

DSP **Data Security & Privacy Lifecycle Management**
DSP-07: Data Protection by Design and Default
DSP-08: Data Privacy by Design and Default
DSP-17: Sensitive Data Protection

IAM **Identity and Access Management**
IAM-03: Identity Inventory
IAM-05: Least Privilege
IAM-09: Segregation of Privileged Access Roles
IAM-10: Management of Privileged Access Roles
IAM-14: Strong Authentication
IAM-16: Authorization Mechanisms

IVS **Infrastructure and Virtualization Security**
IVS-02: Capacity and Resource Planning
IVS-03: Network Security
IVS-04: OS Hardening and Base Controls
IVS-05: Production and Non-Production Environments
IVS-07: Migration to Cloud Environments
IVS-07: Network Defense

LOG **Logging and Monitoring**
LOG-03: Security Monitoring and Alerting
LOG-05: Audit Logs Monitoring and Response
LOG-12: Access Control Logs
LOG-12: Failures and Anomalies Reporting

SEF **Security Incident Management, E-Discovery, & Cloud Forensics**
SEF-03 Incident Response Plans
SEF-04 Incident Response Testing
SEF-06 Event Triage Processes

TVM **Threat & Vulnerability Management**
TVM-07 Vulnerability Identification
TVM-08 Vulnerability Prioritization
TVM-09 Vulnerability Management Reporting

Stride Threat Analysis		Reference Links
✗	Spoofing Identity	1. A-real-world-look-at-aws-best-practices-iam-policies https://www.netskope.com/blog/a-real-world-look-at-aws-best-practices-iam-policies 2. S221421262100079X https://www.sciencedirect.com/science/article/pii/S221421262100079X 3. Cri-o-vulnerability https://blog.aquasec.com/cve-2022-0811-cri-o-vulnerability 4. Linux-kernel-container-escape-in-kubernetes https://blog.aquasec.com/cve-2022-0185-linux-kernel-container-escape-in-kubernetes 5. Azure Escape https://www.paloaltonetworks.com/blog/2021/09/azurescape/ 6. First-malware-targeting-aws-lambda https://thehackernews.com/2022/04/first-malware-targeting-aws-lambda.html
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	
✓	Elevation of Privilege	

Security Issue 10:
Organized Crime, Hackers & APT

Advanced persistent threats (APTs) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network to mine highly sensitive data. [1] These teams may include nationstates as well as organized criminal gangs. The term Organized Crime is meant as a means to describe the manner in which the level of organization a group would have when creating planned and rational acts that reflect the efforts of group individuals[5]. APTs have established sophisticated tactics, techniques, and protocols (TTPs) to infiltrate their targets. It is not uncommon for APT groups to spend months undetected in a target network. This extended time allows them to move laterally towards highly sensitive business data or assets. Some APT groups have historically also favored particular industries or organizations. For example, APT33 has been attributed to threat actors based out of Iran. They have historically targeted the energy and aviation sector. APT groups have various motivations to carry out malicious activities, such as political or economic.

Security Responsibility

- ✓ Customer
- ✓ Cloud Service Provider
- ✓ Both

Architecture

- ✓ Infra
- ✓ Info
- ✓ Meta
- ✓ Application

Cloud Service Model

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

The threat intelligence community closely studies APT groups. Threat intelligence reports educate organizations and nation-states about APT groups and their behavior. Organizations can better protect themselves by conducting red teaming exercises to simulate the behavior of APT groups described in the reports. Such cyber exercises will allow organizations to test and improve their cyber detection capabilities against the various TTPs associated with APT groups. Organizations should also conduct threat hunting activities to attempt to detect the presence of APTs in their networks.

Business Impacts

- The motivations of APT groups vary and can differ from one group to another. Some are politically motivated (i.e., hacktivists), while others are a part of an organized crime group. Several groups are even nation-state actors. For example, APT38 is suspected to be a North Korean state-sponsored group known to conduct cyber heists targeting global financial institutions.
- To understand the business impact that an APT group can have on an organization, it must conduct a business impact analysis on its information assets. This allows the organization to understand how and why an APT group might target an organization and what the potential business impacts of a potential security breach could be.

Key Takeaways

Here are some of the key takeaways:

- Conduct a business impact analysis on your organization to understand your information assets.
- Participate in cybersecurity information sharing groups to understand any relevant APT groups and their TTPs.
- Conduct offensive security exercises to simulate the TTPs of these APT groups and ensure security monitoring tools are tuned for detection.

Anecdotes and Examples

Recent examples of issues related to APTs, organized crime, and hackers:

- (April 5, 2022) Malware hunters at Broadcom's Symantec division have spotted signs that a long-running cyberespionage campaign linked to Chinese nation-state hackers is now going after managed service providers (MSPs) with a more global footprint. [2]
- (February 5, 2016) The Lazarus group (APT38) almost conducted a complete heist of Bangladesh's national bank. [3]
- (January 21, 2022) LAPSUS$ group hacked the internal network of Nvidia and stole confidential data. Instead of ransoming Nvidia for the data, the group demanded that Nvidia release restrictions on its graphical processing units for crypto mining. [4]

CSA CBK Security Guidance Version 4.0

Domain 9: Incident Response
Domain 13: Security as a Service

CSA CCM Controls Version 4.0

TVM Application and Interface Security
TVM-01: Threat and Vulnerability Management Policy and Procedures
TVM-02: Malware Protection Policy and Procedure
TVM-03: Vulnerability Remediation Schedule
TVM-04: Detection Updates
TVM-05: External Library Vulnerabilities
TVM-06: Penetration testing
TVM-07: Vulnerability Identification
TVM-08: Vulnerability Prioritization
TVM-09: Vulnerability Management Reporting
TVM-10: Vulnerability Management Metrics

LOG Logging and Monitoring
LOG-03 Security Monitoring and Alerting
LOG-05 Audit Logs Monitoring and Response

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. APT Definition https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/ 2. Chinese APT Group Targeting Global MSPs: https://www.securityweek.com/symantec-chinese-apt-group-targeting-global-msps 3. How North Korea almost pulled off a billion-dollar hack: https://www.bbc.com/news/stories-57520169 4. Lapsus$ group demanding Nvidia release restrictions on crypto mining on its GPUs: https://cybersecuritynews.com/beware-lapsus-ransomware-group/ 5. Cyber Organized Crime: What is it? https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	
✓	Elevation of Privilege	

Security Issue 11:
Cloud Storage Data Exfiltration

Security Responsibility
✓ Customer
✓ Cloud Service Provider
✓ Shared
Architecture
✓ Application ✓ Meta
✓ Info ✗ Infra
Cloud Service Model
✓ Software as a Service (SaaS)
✓ Platform as a Service (PaaS)
✓ Infrastructure as a Service (IaaS)

Cloud storage data exfiltration is an incident involving sensitive, protected, or confidential information. These data may be released, viewed, stolen, or used by an individual outside of the organization's operating environment. Data exfiltration may be the primary objective of a targeted attack and may result from an exploited vulnerability or misconfiguration, application vulnerabilities, or poor security practice. Exfiltration may involve any kind of information that was not intended for public release, for example, personal health information, financial information, personally identifiable information (PII), trade secrets, and intellectual property.

Victims are not typically aware of data loss in data exfiltration scenarios. The attackers might notify the organization if it's part of their goal, such as direct financial gain or ransomware. Still, in some cases, the fact that data was exfiltrated is unknown or discovered after a long time, making any mitigations irrelevant.

As data is a major asset, cloud ease of use, configuration, elasticity, resilience, and multiple services suitable for all reasonable needs make cloud data storage very appealing. With that, there are multiple venues to exfiltrate it. It can be due to human error or abuse, such as misconfiguration of a PaaS service. Storage objects may also expose sensitive data or files shared externally through personal cloud storage applications.

Other cloud storage data exfiltration might start with a phishing attack, manipulating an application or service. The initial vector of compromise may lead to credential theft or unauthorized access to cloud data. Then, the attacker can take a few potential actions, such as extracting the data for further usage while encrypting the organization's data for ransomware.

Supply chain attacks may offer access to the underlying data, making it more complex to detect and recover. As organizations move towards the Zero Trust model, traditional organizational perimeters play a lesser role. Least privileged access and identity-based security controls should limit data exposure. It's also important to implement cloud posture management to comply with the CSP's best practices or regulatory baselines and mechanisms for attack detection and data disaster recovery.

Business Impacts

There are several potential implications of a data breach:

- Loss of intellectual property, whereas unique knowledge is lost and used in product development, strategic plans, and even a step toward a future attack.
- Loss of customers, stakeholders, partners, and employees' trust might inhibit business conduct, investments, and purchase and reduce the desire to work at and with that organization.
- Regulatory actions include financial fines or a process and business change demand.
- Geopolitical implications can impact business conduct.
- Loss of employees' trust in the organization's ability to protect employee data.

Key Takeaways

Here are some of the key takeaways:

- Cloud storage requires a well-configured environment (SSPM, CSPM).
- To detect and prevent attacks and data exfiltration, apply the CSP best practices guides, monitoring, and detection capabilities.
- Employee awareness training on cloud storage usage is required, as data is scattered in various locations and controlled by various personas.
- Implement client-side encryption where appropriate.
- Classifying data can help in setting different controls, and document the impact and recovery actions required in an incident response plan.

Anecdotes and Examples

Recent examples of issues related to cloud data exfiltration include:

- (6/24/2021) "Facebook is to be sued in Europe over the major leak of user data that dates back to 2019 but which only came to light recently after information on more than 533 million accounts was found posted for free download on a hacker forum." [1]
- (3/11/2019) "Security researchers have found dozens of companies inadvertently leaking sensitive corporate and customer data because the staff is sharing public links to files in their Box enterprise storage accounts that can easily be discovered." [2]
- (4/12/2022) "Amazon Web Services (AWS) on Monday announced that it recently addressed a vulnerability in Amazon Relational Database Service (RDS) that could lead to the exposure of internal credentials." [3]

CSA CBK Security Guidance Version 4.0

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 7: Infrastructure Security
Domain 9: Incident Response
Domain 10: Application Security
Domain 11: Data Security and Encryption
Domain 12: Identity, Entitlement, and Access Management
Domain 13: Security as a Service

CSA CCM Controls Version 4.0

A&A Audit & Assurance
A&A-02: Independent Assessments
A&A-04: Requirements Compliance

AIS Application and Interface Security
AIS-01: Application and Interface Security Policy and Procedures
AIS-04: Secure Application Design and Development
AIS-07: Application Vulnerability Remediation

CCC Change Control and Configuration Management
CCC-03: Change Management Technology
CCC-04: Unauthorized Change Protection
CCC-07: Detection of Baseline Deviation

CEK Cryptography, Encryption & Key Management
CEK-03: Data Encryption
CEK-19: Key Compromise

DCS Data Center Security
DCS-02: Off-Site Transfer Authorization Policy and Procedures

DSP Data Security & Privacy Lifecycle Management
DSP-03: Data Inventory
DSP-04: Data Classification
DSP-07: Data Protection by Design and Default
DSP-08: Data Privacy by Design and Default
DSP-10: Sensitive Data Transfer
DSP-17: Sensitive Data Protection

GRC Governance, Risk and Compliance
GRC-01: Governance Program Policy and Procedures
GRC-08: Special Interest Groups

HRS Human Resources
HRS-04: Remote and Home Working Policy and Procedures
HRS-11: Security Awareness Training

IAM Identity and Access Management
IAM-03: Identity Inventory
IAM-07: User Access Changes and Revocation
IAM-14: Strong Authentication
IAM-16: Authorization Mechanisms

IVS **Infrastructure & Virtualization Security**
IVS-04: OS Hardening and Base Controls
IVS-09: Network Defense

IPY **Interoperability & Portability**
IPY-03: Secure Interoperability and Portability Management

LOG **Logging and Monitoring**
LOG-03: Security Monitoring and Alerting
LOG-05: Audit Logs Monitoring and Response
LOG-12: Access Control Logs

SEF **Security Incident Management, E-Discovery, & Cloud Forensics**
SEF-03: Incident Response Plans
SEF-06: Event Triage Processes

STA **Supply Chain Management, Transparency and Accountability**
STA-02: SSRM Supply Chain
STA-06: SSRM Control Implementation
STA-07: Supply Chain Inventory
STA-08: Supply Chain Risk Management
STA-14: Supply Chain Data Security Assessment

TVM **Threat & Vulnerability Management**
TVM-02: Malware Protection Policy and Procedures
TVM-04: Detection Updates
TVM-07: Vulnerability Identification

UEM **Universal Endpoint Management**
UEM-09: Anti-Malware Detection and Prevention
UEM-14: Third-Party Endpoint Security Posture

Stride Threat Analysis		Reference Links
✓	Spoofing Identity	1. Facebook faces 'mass action' lawsuit in Europe over 2019 breach https://techcrunch.com/2021/04/16/facebook-faces-mass-action-lawsuit-in-europe-over-2019-breach/ 2. Dozens of companies leaked sensitive data thanks to misconfigured Box accounts https://techcrunch.com/2019/03/11/data-leak-box-accounts/ 3. Amazon RDS Vulnerability Led to Exposure of Credentials https://www.securityweek.com/amazon-rds-vulnerability-led-exposure-credentials
✓	Tampering with Data	
✓	Repudiation	
✓	Disclosure	
✓	Denial of Service	
✓	Elevation of Privilege	

Conclusion

As cloud business models and security tactics evolve, this report raises awareness of critical security issues such as (1) Insufficient Identity, Credentials, Access, and Key Management, (2) Insecure Interfaces and APIs, (3) Misconfiguration and Inadequate Change Control, (4) Lack of Cloud Security Architecture and Strategy. Other threats highlight (5) Insecure Software Development, (6) Unsecured Third-Party Resources, (7) System Vulnerabilities.

Insufficient Identity, Credentials, Access, and Key Management holds the top spot. Replay attacks, impersonation and over-permissioning continue in the cloud as though on-premise with the promise of more accessibility. Using self-signed certificates, poor cryptographic management or trusting every root CA are just a few of the questionable choices. With the emphasis on Zero Trust Architecture and SDP it is no wonder that the examples highlighted in the Pandemic Eleven issue one are top of mind to our survey respondents.

The continued adoption of micro-services emphasizes the importance of secured Interfaces and APIs. There should be more of them, and it is concerning that there are still significant challenges in securing these features with cloud playing a minimal part in their development. As these APIs proliferate to SaaS and PaaS offerings, the inefficiencies of the coders and always-on nature of cloud creates a significant risk.

Misconfiguration and Inadequate Change Control previously held the second spot on the Egregious Eleven. This is yet another example of the cloud problems moving up the security stack. Configuration management has been part of organizational capability maturities for decades, and until teams embrace cloud will only compound the problem. Misconfigurations with a cloud's persistent network access and infinite capacity potentially impacts numerous organizations within a company.

Finally, Strategy and Architecture which held the third spot on the last list begs the question, "why is there still such a problem planning and architecting security solutions"? Cloud computing is no longer a novelty - define a big picture approach and execute on the architectural design patterns.

This *Top Threats in Cloud Computing Pandemic Eleven* report continues the trend of the *Top Threats to Cloud Computing: Egregious Eleven 2019* report with a shift 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. The cloud itself is less of a concern, so now we focus more on the implementation of the cloud technologies.