The Shifting focus of Cloud Computing issues from information security to business resilience; audit and control approaches to reducing organizational risk

Fernando Martinez PhD CISM CISA CGEIT CISSP
APGM Certified CISM and CISA Instructor
ISACA Central Florida Webinar
February 21, 2023

Introduction

Cloud security skills and strategy differ from traditional on-premise data centers

Management ingenuity in modeling and anticipating, then galvanizing organizational readiness, trumps any technical solution

Basics

Inventory

Data, enumerate and classify.
Information Systems,
identify and associate.
Infrastructure, in particular
boundary layers.
Users, by system
with focus on privilege.

Basics

Risk stratify Information Systems.

Build controls to audit, monitor, and validate their effectiveness

Don’t ignore block and tackle.

Closed-loop processes that are predictable and audited, especially where vulnerability management and known exploits are concerned

Basics

Stay informed

Find sources meaningful to you.

Rehearse

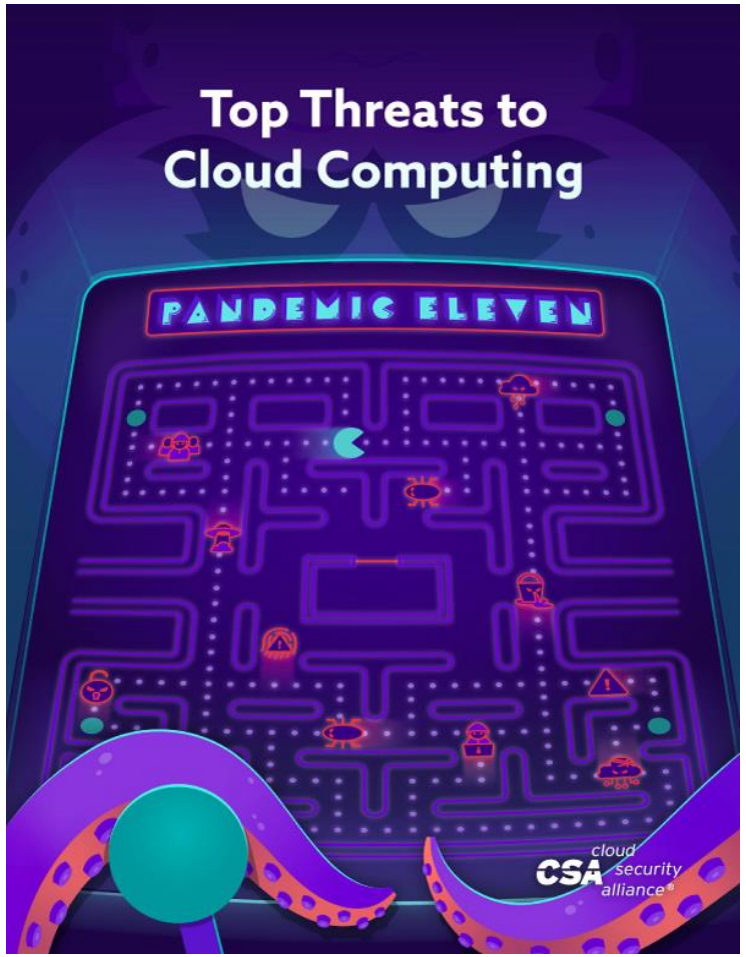
Built on current and active trends.

To the greatest extend that is practical and cost effective.

Third and Fourth-party risk

Requires iterative and persistent management.

Cloud Security Alliance Report



[1] https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/

Shift in priorities

“Data breaches and data loss were top concerns las year. This year, they weren’t even in the top 11”

Cloud customers are getting smarter, getting away from worrying about end results and looking at the causes of those results.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

Shift in priorities

CSP's are doing a better job protecting their infrastructure and shifting the focus to the cloud user who is responsible for protecting the data, applications and access in their cloud environments.

Organizations consuming cloud services need to do everything they can to mitigate the risk of security events.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

Reflect

Increased focus on architecture.

Concerns about limited cloud visibility.

Limited cloud usage visibility and a weak control plane.

A call to action for developing and enhancing cloud security awareness, configuration and identity management.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

Summary of Top Threats

1. Insufficient identity, credential, 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. Unsecure third-party resources
7. System vulnerabilities
8. Accidental cloud data disclosure/disclosure
9. Misconfiguration and exploitation of serverless and container workloads
10. Organized crime/hackers/APT
11. Cloud storage data exfiltration

[1] https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/

1. Insufficient identity, credential, access and key management (Prev #4)

Identity and access are foremost in the minds of cybersecurity pros because protecting your data starts and ends with access.

Identity and access in a CSP platform is everything. “If you have the keys to the kingdom” you are a threat to the stability and security of any organization

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

1. Insufficient identity, credential, access and key management (Prev #4)

“Attackers no longer try to brute-force their way into enterprise architecture. With so many ways to compromise and steal corporate credentials, the preferred tactic is to pose as a legitimate user in order to avoid detection.”

Priority is to ensure that trusted parties only have access to the data that is absolutely necessary.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

1. Insufficient identity, credential, access and key management (Prev #4)

Cloud platforms come with a requirement to effectively manage user and system access and privileges. It's one of the primary responsibilities of the enterprise in a *shared responsibility* [3] model.

Operational policies and structured risk models are vital.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

[3] https://www.csoonline.com/article/3619799/the-shared-responsibility-model-explained-and-what-it-means-for-cloud-security.html

2. Insecure interfaces and API's (Prev #7)

Vulnerabilities due to misconfiguration, coding vulnerabilities, or lack of authentication and authorization.

Organizations face a challenging task in managing API's. This dynamic environment requires a nimble and proactive approach to change control and remediation.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

2. Insecure interfaces and API's (Prev #7)

The attack surface provided by API's should be tracked, configured, and secured.

Traditional controls and change management tactics need to be updated to reflect cloud-based API growth and change.

Embrace technology to monitor continuously for anomalous API traffic and remediate problems in near real-time.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

3. Misconfiguration and inadequate change control (Prev #2)

Misconfiguration or sub-optimal setup of computing assets that may leave them vulnerable to unintended damage or external and internal malicious activity.

One of the significant advantages of the cloud is scalability, but this also means that one misconfiguration can have magnified ramifications across multiple systems.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

3. Misconfiguration and inadequate change control (Prev #2)

Use available technologies that scan continuously for misconfigured resources to allow remediation of vulnerabilities in real-time.

Approved changes must strictly follow defined change management approaches to ensure that approved changes are made properly, and using real-time automated verification.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

4. Lack of cloud security architecture and strategy (Prev #3)

“Most security folks looking after cloud security must consider what mix of default controls from the cloud provider, premium controls from the same, and what third-party security product offerings address their specific risk profile, and sometimes that profile is different at the application level”

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

4. Lack of cloud security architecture and strategy (Prev #3)

Infrastructure design and decisions should consider business objectives, risk, security threats, and legal compliance in cloud services.

It is important to develop and adhere to an infrastructure strategy and design principles.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

5. Insecure software development

By leveraging *shared responsibility* [3], items like patching can be owned by a CSP rather than the business.

CSP's place a heightened importance on security and will provide guidance on how to implement services in a secure fashion.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

[3] https://www.csoonline.com/article/3619799/the-shared-responsibility-model-explained-and-what-it-means-for-cloud-security.html

6. Unsecure third-party resources

Third-party risks exist in every product and service we consume.

A product or service is the sum of all the other products and services it is using. An exploit can start at any point in the supply chain for the product and proliferate from there.

Threat actors know they only need to compromise the weakest link in a supply chain to spread malicious software.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

6. Unsecure third-party resources

Identify and track the third parties you are using. Stay informed.

Perform a periodic review (audit) of the third-party resources. Remove products you don't need; revoke any access or permissions you may have granted to your application or infrastructure.

Pen-test your applications, teach your developers about secure coding and testing

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

7. System vulnerabilities

Include zero-day, missing patches, vulnerable misconfiguration or default settings, and weak or default credentials.

Security risks due to system vulnerabilities can be greatly minimized through routine vulnerability detection and patch deployment (closed-loop processes)

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

8. Accidental cloud data disclosure

Review your (PaaS) databases, storage and compute workloads hosting databases, including virtual machines, containers and database software installed on them. Audit, catalog, risk-stratify and review on a periodic schedule.

Reduce access exposure by ensuring that the database is configured to the least-privileged IAM policy, and that assignments of this policy are controlled and monitored.

9. Misconfiguration and exploitation of serverless and container workloads

Implement Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), and cloud workload protection platforms to increase security visibility, enforce compliance, and achieve the least privilege in serverless and containerized workloads.

Extra rigor around strong application security and engineering best practices – before migrating to serverless technology that remove traditional security controls.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

10. Organized crime, hackers and APT groups

APT groups typically focus their thieving ways at data acquisition.

Stage “red-team” exercises to better protect from APT attacks.

Perform threat-hunting exercises to identify the presence of any APT’s on the network.

Conduct a BIA on your organization to understand your information assets.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

10. Organized crime, hackers and APT groups

Participate in cybersecurity information sharing groups.

Understand any relevant APT groups and their tactics, techniques and procedures (TTP's).

Ensure security monitoring tools are tuned to detect TTP's of any relevant APT group.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

11. Cloud storage data exfiltration

Many times occurs without the knowledge of the data owner.

Use zero-trust model where identity-based security controls are used to provide least privileged access to data.

Remediation of vulnerabilities in IaaS and strong identity and access control of both people and non-human personas.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

11. Cloud storage data exfiltration

Apply the CSP's best practices guides, monitoring and detection capabilities.

Evaluate a cloud providers security resilience and, at a minimum, security standards adherence, legal agreement, and service level agreement (SLA).

Classifying data can help in setting different controls, and if exfiltration happens, assessing the impact and recover actions required.

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

Audit considerations

- Evaluate the CSP security posture
  - Review security P&P, risk assessments
- Determine the attack surface
  - Monitoring tools, prioritize assets at higher risk
- Validate strong access controls
  - Password policies, MFA, limited admin privileges, least privilege
- External sharing standards
- Patching, prioritizing most critical assets and patches
- Use SIEM – industry standard for auditing activity

THANKS FOR ATTENDING!

Fernando Martinez PhD
fmartinez@tha.org
http://Linkedin.com/in/fmartinezphd

References

[1] https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/

[2] https://www.csoonline.com/article/3043030/top-cloud-security-threats.html

[3] https://www.csoonline.com/article/3619799/the-shared-responsibility-model-explained-and-what-it-means-for-cloud-security.html

[4] https://appinventiv.com/blog/cloud-security-risks-and-solutions/

[5] https://www.neoito.com/blog/top-cloud-security-challenges/

[6] https://www.scmagazine.com/news/cloud-security/top-challenges-for-cloud-security-in-2023-managing-growing-cyberattacks-delivering-visibility-and-consolidating-tool-sprawl

[7] https://thenewstack.io/the-top-4-threats-to-securing-your-cloud-infrastructure/

[8] https://www.geeksforgeeks.org/security-issues-in-cloud-computing/

[9] https://www.computerweekly.com/news/365530175/Cloud-security-top-risk-to-enterprises-in-2023-says-study

[10] https://www.csoonline.com/article/3686579/misconfiguration-and-vulnerabilities-biggest-risks-in-cloud-security-report.html