# CxO Trust Newsletter - May 2022

## Top Threats to Cloud Computing Brings to Light New Areas of Focus

**Sean Heide, Research Technical Director, CSA**

Cloud computing, as well as the security that surrounds its implementation, is an ever increasingly difficult area for most enterprises to get right. Due to the sheer amount of vendors and products that teams use day to day, it has increased the threat surface for businesses, oftentimes going unaddressed. This could perhaps stem from lack of knowledge on key areas of focus, but one could also argue it is in direct correlation with not understanding what risks lie in the hands of the service provider vs. customer.

The Top Threats to Cloud Computing report is a release raising awareness around the top threats, vulnerabilities, and risks in the cloud year over year. With over 700 industry experts surveyed, the top identified areas are then highlighted and expanded upon in order to gain a deeper understanding of the cloud landscape. In this year's report, CSA saw a significant change in the order of threats, as well as some new additions that were not seen in previous years reports. This year's report will be released in June at the CxO Trust Summit at RSAC 2022, so please be on the lookout for the links from the CSA homepage.

Because of the flexibility of the document, the Top Threats report can be used by teams in a multitude of ways. One which is a comparison analysis of findings from the survey versus your own businesses current cloud implementations. Provided in the document are also business impacts for each threat, as well as key takeaways. These takeaways help get a granular picture on potential mitigations or ways to address the area.

Lastly, the research group during analysis, has helped the reader combine a control framework when looking through each threat. Mapping each threat to the Cloud Controls Matrix V4 (CCM), readers can begin to understand key impact areas in order to build a game plan for moving forward. Because of the CCM's control objectives spanning across all cloud implementation possibilities, this will provide the reader with a 1 for 1 guidance on remediating their own potential cloud vulnerabilities.

The following are this years order of cloud top threats:

**Security Issue 1: Insufficient Identity, Credentials, Access, and Key Management, 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 consist of electronic files, computer systems, and physical resources, such as server rooms and buildings.

**Security Issue 2: Insecure Interfaces and APIs**

API usage continues to grow in popularity, and securing these interfaces has become paramount. APIs, and similar interfaces, potentially include vulnerabilities due to misconfiguration, coding vulnerabilities, as well as a lack of authentication and authorization among other things. These oversights can potentially leave them 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
7. Logging or monitoring disabled

**Security Issue 3: Misconfiguration and Inadequate Change Control**

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.

**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, and pre-determinations.

**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  and likely misconfigurations. Thanks to the accessibility of the cloud, threat actors can leverage these “features” more easily than ever before.

**Security Issue 6: Unsecure Third-Party Resources**

Being vigilant in your decision for which vendors to go with is the first step in protecting your business and following a risk first mindset. Unsecured third party resources can bring into your environment potential security flaws, limited integrations, and lack of oversight. Third party resources must be vetted through security reviews, meeting business requirements, and undergoing annual reviews to make sure they are still meeting specific criteria.

**Security Issue 7: System Vulnerabilities**

System vulnerabilities are flaws in cloud service platforms that are exploited in order to compromise confidentiality, integrity, and availability of data, and disrupt service operations.

**Security Issue 8: Accidental Cloud Data Disclosure**

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 Issue 9: Misconfiguration and Exploitation of Serverless and Container Workloads**

The migration to cloud infrastructure and adoption of DevOps practices have enabled IT teams to deliver value to the business faster than ever. But managing and scaling the infrastructure and security controls to run their applications is still a significant burden on development teams. It also requires teams used to managing legacy infrastructure on-prem to learn new skills like Infrastructure as Code and cloud security.

**Security Issue 10: Organized Crime, Hackers & APT**

Advanced Persistent Threats (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, allowing them to move laterally towards highly sensitive business data or assets.

**Security Issue 11: Cloud Storage Data Exfiltration**

Cloud storage data exfiltration is an incident in which sensitive, protected, or confidential information is released, viewed, stolen, or used by an individual outside of the organization's operating environment.

Ultimately, it is up to the reader to interpret these results and the manner in which they are able to use them. As said earlier, there is no one correct way to utilize the Top Threats report. Gap analysis, risk review, threat modeling, or foundational controls references are some of the few ways in which to lead the direction of thought when diving into this document. Use this as a building block when considering what controls to implement, or perhaps even which threats relate most to your specific situation.