CYBERRISKS&LIABILITIES

Cloud Security Management Explained

Cloud computing refers to a pay-per-use service that equips users with on-demand access to a range of IT resources (e.g., databases, software, servers, networking and analytics tools, and artificial intelligence applications) via the internet. By leveraging cloud-based platforms, organizations can minimize the need to purchase and maintain physical data centers and servers, ultimately streamlining their digital infrastructures and allowing for greater IT flexibility.

Although cloud computing can provide a number of benefits, it also carries unique cyber exposures. Specifically, without proper safeguards in place, organizations could be susceptible to cloud-based cyberattacks and associated losses. To limit the potential risks stemming from cloud computing, it's imperative for organizations to adopt effective security management measures. This article provides more information on cloud security management, explains why it's necessary and offers related best practices.

What Is Cloud Security Management?

Cloud security management consists of various techniques, tools and tactics that organizations can implement to ensure they can utilize cloud services to their full potential, all while defending their data and operations against possible cyberthreats. By adopting sufficient cloud security management measures, organizations can host essential workloads and information on cloud-based platforms without compromising their digital assets and IT infrastructures.

Cloud security management differs from traditional IT security management in several ways. Since cloud services are accessed online, they often present a wider array of attack surfaces for cybercriminals than those found in a physical IT environment. Cloud-based platforms are also constantly evolving, with new risks following suit. Considering these complexities, cloud security management typically requires a different approach and more specialized strategies than traditional IT security management. Yet, seeing as organizations generally utilize both physical computing resources and cloud-based services within their operations, it can be beneficial for them to incorporate a mix of traditional and cloud-specific security solutions.

Why Is Cloud Security Management Necessary?

When organizations decide to invest in cloud services, they can't afford to ignore cloud security management. These specialized risk mitigation strategies are necessary for the following key reasons:

- **Cloud-based cyberthreats are on the rise.** As cloud services become more prevalent and advanced, cybercriminals have started targeting these services through a variety of sophisticated attack methods (e.g., data breaches, malware infections, phishing scams, ransomware incidents and distributed denial-of-service attacks). Because such services often store organizations' most valuable digital assets, cloud-based cyberattacks can result in considerable damage. With ample cloud security management, organizations can better navigate these rising cyberthreats and avoid devastating losses.
- **Organizations have certain cloud security obligations.** Many organizations falsely assume that their cloud service providers are solely responsible for ensuring proper cloud security management; however, organizations must share these security obligations with their service providers. This concept, known as the shared responsibility model, requires organizations to openly communicate with their service providers to determine and delineate each

BITNER HENRY
INSURANCE GROUP

party's specific cloud security roles. In most cases, service providers are responsible for securing their overall cloud infrastructures, whereas organizations are in charge of safeguarding the digital assets stored within these environments.

- **The consequences of poor cloud security can be severe.** Organizations with inadequate cloud security management are more likely to experience costly cyberattacks. In addition to the serious financial ramifications of these incidents, cloud-based cyberattacks can lead to significant operational disruptions and major reputational damage. If these attacks result in compromised files or leaked stakeholder information, organizations may also be subject to compliance violations under applicable data privacy legislation and, subsequently, face hefty regulatory penalties.

Cloud Security Management Strategies

Here are some cloud security management practices for organizations to consider:

- **Understand the shared responsibility model.** First and foremost, organizations should be fully aware of the shared responsibility model and understand how it applies to their cloud security obligations. In particular, it's important to note that while cloud service providers are responsible for ensuring the security of the cloud itself (e.g., establishing proper network and server configurations), organizations should take steps to maintain the security of cloud-based workloads, data and endpoints.
- **Perform routine security audits.** Organizations should conduct regular cloud security audits to assess their unique cyber exposures and identify possible vulnerabilities. This may entail documenting the types of digital assets stored within cloud-based platforms and reviewing which parties can access such assets. By conducting these audits, organizations will be better equipped to address their specific cloud security needs and comply with relevant data privacy laws.
- **Ensure proper access controls.** To limit the risk of cybercriminals compromising digital assets stored within the cloud, organizations should implement effective access control policies and procedures. These policies and procedures are intended to only permit approved users to utilize the cloud resources they need for essential tasks (also called the principle of least privilege) and prevent unauthorized access to sensitive workloads and data. For example, organizations may leverage multifactor authentication policies that require users to input two or more credentials to verify their identities before accessing cloud-based platforms.

  Additionally, organizations may also utilize identity and access management (IAM) systems. These systems record which users have been granted access to the cloud and the types of digital assets those users are allowed to handle, updating such information as users' roles and projects change. IAM systems then use this information to monitor cloud access attempts and only permit approved users to pass through, thus keeping cybercriminals at bay.
- **Encrypt sensitive data.** Encrypting confidential files and information stored within and transported through cloud-based platforms can help organizations keep this data concealed and secure, even if it ends up in the hands of cybercriminals. Organizations may be able to leverage data encryption products offered by their cloud service providers or through other third-party vendors. Regardless, organizations should ensure their data encryption processes involve keeping private files and information protected both at rest and in transit, as well as maintaining proper management of encryption keys.
- **Secure cloud architecture.** Since cloud services include access to containers—which refer to software packages and related codes, settings and libraries—and applications, it's best for organizations to safeguard these major elements of their cloud architecture. Container security typically consists of deploying technological solutions that continuously monitor for suspicious activities and enhance the visibility of potential cyberthreats, namely malware. Such solutions should also help detect and decommission compromised containers.

On the other hand, application security generally entails implementing cloud security posture management (CSPM) tools that scan for any misconfigurations that could impact cloud-based workloads. CSPM tools evaluate an organization's cloud service deployments against company-specific standards, industry guidelines, and applicable security and compliance benchmarks to assign a score that represents the current state of its cloud-based workloads. From there, the organization can determine whether any corrective actions are necessary to improve its score and remedy possible workload concerns.

- **Educate staff.** Employees are often considered organizations' first line of defense against cyberthreats, including those found within the cloud. As such, organizations should be sure to incorporate cloud security management tactics in their routine cybersecurity training programs, thus giving employees the education and resources needed to properly identify and mitigate cloud-based cyberattacks. Key topics to cover during such training include digital exposures stemming from the cloud, common cloud-based cyberattack methods, and incident detection and response protocols.
- **Monitor and address cyberthreats in real time**. Organizations should leverage advanced threat detection tools to maintain consistent monitoring of cloud-based platforms and any digital assets stored within these environments. In doing so, organizations can establish a baseline for typical cloud interactions and activities, making it immediately evident when unusual events arise. This will allow organizations to promptly investigate any emerging cyberthreats in the cloud and address these concerns before they cause widespread damage.
- **Have a plan**. Creating cyber incident response plans can help organizations ensure necessary procedures are taken when cyberattacks occur, thus keeping related losses at a minimum. These plans should be well-documented and practiced regularly, and address a range of cyberattack scenarios (including cloud-based incidents).
- **Purchase sufficient coverage.** Finally, it's critical for organizations to secure adequate commercial insurance policies to ensure ample financial protection against losses that may arise from cloud-based cyberattacks. Organizations should consult trusted insurance professionals to discuss their specific coverage needs.

Conclusion

While cloud services can certainly benefit organizations, they also pose some substantial cybersecurity challenges. By understanding the risks associated with the cloud and taking steps to minimize these concerns, organizations can maintain a strong security posture and prevent large-scale losses.

Contact us today for more risk management guidance.