Understanding Cloud Security, Vulnerabilities and Internal Controls

In today's digital world, "the cloud" has revolutionized the way organizations, store, manage, and process data. However, as more organizations utilize cloud technology, the vulnerabilities surrounding that technology have grown exponentially. Failure to adapt and prevent these vulnerabilities from impacting your business can have major consequences, including significant financial losses, reputational damage, and operational disruption. Therefore, it is imperative that organizational leaders take cloud security very seriously.

Common Cloud Vulnerabilities

So, how and why do problems usually arise?

1. Data Breaches and Unauthorized Access: Since the cloud stores vast amounts of sensitive data, it is a prime target where attacks will be centered. The prospect of getting financial or operational information from an organization is too tantalizing to pass up for cyber criminals. Traditionally, issues like employee passwords, compromised credentials or misconfigured access controls often lead to unauthorized access and data breaches. Thankfully, these areas of concern are the easiest to secure with proper education and policies in place.

2. Misconfigurations: For many organizational leaders, cloud misconfiguration often falls under the responsibility of IT professionals or your third-party vendor. However, it is imperative that you ensure your team is on top of your cloud configuration to keep misconfigured cloud storage, databases, or applications away from the public eye.

3. Insider Threats: Of course, the biggest threat for a data breach comes from outside your organization but never underestimate the possibility of employees or third-party vendors trying to monetize your data for their own benefit. Those with legitimate access to cloud systems can unintentionally or intentionally compromise data security.

4. Denial-of-Service (DoS) Attacks: Once such an attack is underway, the goal may not be to extract valuable information. Instead, attackers may wish to flood cloud systems with traffic, which disrupt operations and cause downtime. This can be just as debilitating for an organization as the actual loss of vital information.

How to protect your data

When advising our clients on cloud security, COMD looks to leaders like Joe Saracino, President and CEO of Cino Security Solutions (CSS). CSS recommends implementing, at a minimum, the following six security measures to better protect your nonprofit and to keep your operations running while using cloud technology:

1. Implement Robust Access Controls: For all employees and users of your digital systems, nonprofits should use multi-factor authentication (MFA), and strong password policies to prevent unauthorized access to cloud systems. The days of your staff member using his DOB as a password are officially over.

2. Encrypt Data: No matter where data is in your system, ensure it is encrypted. By utilizing strong encryption protocols, your nonprofit will protect sensitive information from unauthorized access and save you from having to explain why your business didn't do what is now the most basic thing in data protection.

3. Train Employees: Minimize outside and inside threats by providing employees with the training they need to understand cybersecurity. This isn't an extremely exciting thing on which to spend money, but if you don't then how do you explain to your donors, benefactors or members that information was lost because an employee didn't recognize phishing attempts, had simplistic passwords or failed to securely manage his credentials?

4. Monitor and Detect Threats and Conduct Regular Threat Tests: Part of any IT budget must be the purchase of cloud monitoring tools and threat detection systems to identify and respond to suspicious activity. At the same time, organizations must test their cloud systems for vulnerabilities. This will allow issues to be addressed before they become critical (and often public) failures.

5. Cloud Configuration Management: Though a bit more "technical," ensuring regular audits and updates of your cloud configuration systems will help prevent cloud problems.

6. Third-party Vendor Risk Management: Since many nonprofits use multi-cloud or hybrid-cloud strategies, evaluating the security practices of your third-party providers is essential to protecting your data.

Conclusion

In the end, organizational leaders no longer have the luxury of just hoping that their data storage systems won't be attacked or disrupted by something. In today's world, cloud computing offers unparalleled flexibility and scalability, and its use is expected – even in the smallest of organizations, but it comes with its own set of risks. Without doubt, organizations must take a proactive approach to identify and mitigate cloud vulnerabilities. By implementing robust security measures, fostering a culture of awareness, and working closely with cloud providers, your organizations can build a resilient cloud infrastructure and protect critical assets from these clear and ever-present threats.

Kim McDonough, Director of Operations at COMD