The Top 3 Cloud Risks Facing CFO's Today

By Taiye Lambo and Jordan Flynn

October 2014

In today's continuously changing business world, CFO's are being kept on their toes more than ever before. With technology and business models repeatedly evolving, CFO's also need to evolve in the ways they perceive organizational risks and mitigate against them to avoid both financial and reputational losses for the organizations they are tasked with protecting and overseeing.

Cloud computing is increasingly becoming the go to business model worldwide, with the allure coming from the reduced IT and business costs offered by purchasing computing resources "on-demand" rather than investing in dedicated in-house infrastructure and IT support staff. Yet, while this may be the most attractive advantage for CFO's in moving to the cloud, it has also exposed their organizations to substantial risks by moving too quickly into the cloud without a clear understanding of the risks. This is like jumping off an airplane without a parachute.

Proper education and awareness of CFO's to cloud risks is urgently needed so that they can clearly recognize how the cloud can impact their businesses' top and bottom lines. The risks associated with the use of cloud computing are relevant to both the CFO's of organizations leveraging cloud services as well as CFOs working for the organizations providing cloud services.

While the CFO must be aware of the cloud's impact on profit and revenue, they should also understand control gaps that exist within the cloud and the effects on their businesses if these vulnerabilities were successfully exploited by attackers. As thought leaders charged with the responsibility to lead their organizations, CFO's should be at the forefront of cloud adoption and must understand cloud risks and how to mitigate against them.

Through its independent cloud security benchmark research focused on the Top 100 cloud service providers globally, CloudeAssurance has tracked and identified, over time, the most critical security control gaps for these cloud services, weaknesses that have unfortunately been successfully exploited in high profile breaches. These gaps are critical for CFO's to comprehend and recognize as their organizations consider moving to and operating within a cloud environment, with three in particular that should keep a CFO up at night.

Cloud Control Gap #1 – Lack of Resiliency

The first of these gaps is centered squarely on the cloud service provider's ability to withstand a disaster and continue to provide critical services post disaster. The lack of resiliency for cloud service providers could have a major impact on the business processes that drive major revenue streams for both cloud provider and cloud customer. While this also holds true in a non-cloud environment, it is even more disruptive when the cloud is involved due to its regular use in supporting several organizations at one time rather than supporting just a single organization. A disaster event for a cloud service provider with a centralized data center and no failover capability can put both the cloud customer and the cloud provider out of business completely, destroying top and bottom lines for the provider and causing significant, possibly irreparable harm to the cloud customer's ability to provide services to their own customers and achieve their revenue and profit goals.

Even worse, this scenario is not as unlikely as it may seem at first glance. Our research indicates that many cloud service providers actually lack failover capability in the event of a disaster, with a number of these providers also having centralized data centers located in high-risk environmental areas or hazardous regions. For CFO's relying on Infrastructure as a Service cloud providers (e.g. storage and processing power), these situations can be nothing short of catastrophic. CFO's must ensure the selection of the right cloud providers and also ensure that they have the right exit strategies and migration plans in adverse situations, to protect revenue streams and company reputation from the risks associated with resiliency gaps.

Cloud Control Gap #2 – Improper Management of User Credentials/Remote Multi-Factor Authentication

Another key cloud security control gap lies within the security architecture of providers, specifically in the management of user credentials and effective user access control. This gap is a proven weakness that has been successfully exploited by criminals in high profile breaches throughout 2014. While user access control has always been very important within traditional IT environments, it has typically been easier to manage within the confines of a single organization.

When utilizing cloud services however, the boundaries of responsibilities for the customer's infrastructure and the cloud provider's infrastructure are not always well demarcated, and managing the identity of individuals and accurately authenticating their levels of access in a vast and complex network of intricate relationships can be a daunting task for any CFO. Yet it often takes only one compromise of user credentials and inappropriate use to trigger a nightmare situation with serious financial implications.

This scenario played out in June of 2014, when a malicious attacker effectively put the cloud service provider Code Spaces out of business within a matter of hours. Since Code Spaces was hosted primarily on Amazon Web Services, they heavily relied on Amazon's services to help provide their own cloud services to customers. Unfortunately, an attacker was able to gain unauthorized access to a highly privileged account that provided them with the proverbial "key to the kingdom", in this case access to and control of Code Spaces Amazon console, and therefore its customer's environment.

As typically is the case with criminals, the attacker demanded a ransom in exchange for relinquishing control back to Code Spaces, and when Code Spaces did not comply the attacker proceeded with a calculated deletion of critical resources and customer data, putting Code Spaces completely out of business and leaving the customers using their services without access to their critical data or a way to recover or migrate data from this cloud service.

The Code Spaces incident should serve as a powerful wake up call and example to all CFO's considering a move to the cloud or currently utilizing cloud services. The impact on both the top and bottom lines in these scenarios for both the provider and the customer are severe. The breach at Code Spaces demonstrates that these events are occurring as a result of weak security architecture, with the recent Apple iCloud hack reinforcing this fact as well.

In the Apple iCloud breach, attackers were not locked out after a minimum amount of incorrect password entries had been reached, allowing them to easily perform brute force attacks using password cracking software until login credentials were compromised.

This is a simple and basic password management best practice that Apple did not extend to iCloud's backup and restore capabilities, and it resulted in a major breach of privacy for affected users and a loss of reputation for Apples iCloud service, an event that cyber liability insurers do not typically cover. In both the Code Spaces and Apple iCloud attacks, requiring multi-factor authentication (e.g. requiring not only a password but also entry of a code sent via text message or another factor of authentication such as geographical location) would have either prevented such breaches outright or mitigated risks to acceptable levels. The customer's CFO must be fully confident in both the organization's management of user credentials and the application of multi-factor authentication when selecting a provider in order to avoid a similar situation from occurring at their organizations. Provider CFO's must ensure that these controls are being implemented and actively improved within their organization to avoid incurring serious financial and reputation losses.

Cloud Control Gap #3 – Lack of Cyber Liability Insurance Coverage

Finally, our research also reveals that many cloud service providers have yet to obtain cyber liability insurance and/or do not have adequate service level agreements that compensate their customers for losses they may incur due to outages or security breaches. Since service level agreements vary significantly from one cloud service provider to another, it's important that CFO's consuming cloud services have cyber liability insurance that covers third parties such as cloud service providers and clearly understand both the risk that their various cloud contracts bring and the unique liability issues presented by them. This is vital knowledge that a CFO must utilize in order to ensure that their organization is adequately protected in the event of the breach of the cloud services provider.

Similarly, cloud providers need to proactively obtain cyber liability insurance in order to build trust in their reputation and protect themselves from the growing threat landscape and constant barrage of cyber-attacks. This is a vital aspect of protecting top and bottom lines for businesses providing cloud services, and with the confusion and grey areas lingering in the cyber liability insurance space, CFO's need to push for security beyond compliance within their organizations to clearly demonstrate transparency and maturity of their security processes to their cyber liability insurance underwriters and potentially obtain discounted premiums for demonstrating mature cloud security postures.

About the Authors:

Taiye Lambo is a seasoned entrepreneur with Global Information Security and Governance, Risk Management and Compliance expertise with a focus on Cloud Computing. He is the inventor of the innovative AlertApp! and Founder of USA based CloudeAssurance, Inc., eFortresses, Inc., the Holistic Information Security Practitioner Institute (HISPI) and the UK Chapter of the Honeynet Project.

He can be contacted via E-mail (tlambo@eFortresses.com), LinkedIn (http://www.linkedin.com/in/taiyelambo) or Website (www.CloudeAssurance.com).

Jordan Flynn is the Lead Cloud Security Analyst and Researcher for the CloudeAssurance platform, with a focus on the application of cloud computing best practices, global standards, and enterprise governance, risk and compliance, in particular cloud security framework management and risk assessment methodology. He heads the CloudeAssurance independent cloud security benchmark study entitled "Top 10 Cloud Service Providers", which names the Top 10 Cloud Service Providers each quarter. He also operates as an information security consultant with an emphasis on the NIST Cybersecurity Framework, ISO 27001, and PCI-DSS 3.0.

He can be contacted via E-mail (JFlynn@eFortresses.com), LinkedIn (https://www.linkedin.com/pub/jordan-flynn-ccsk-hisp/2b/1b3/9b8) or Website (www.CloudeAssurance.com).