Cloud Security Advice for Law Firms

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

With amazing speed, we've become a very mobile society. Mobile phones are the main computing device for most people. To support a mobile environment, cloud services are growing by leaps and bounds. In the last several years, we can only recall one instance of implementing an on-premises server for a law firm. Just one. And that solution was a non-negotiable demand from the law firm's largest client. Apart from that one exception, law firms are universally accepting a cloud first mentality.

It is one thing to provide technology to support the business function, but many law firms don't pay much attention to securing the cloud environment. They trust the vendor to provide secure cloud applications for the firm. However, many lawyers (especially solo and small firm attorneys) don't know that their own actions can make a secure vendor cloud service very unsecure.

Best Cloud Practices from CISA and NSA

In March of this year, CISA (Cybersecurity & Infrastructure Security Agency) and the NSA (National Security Agency) released five joint Cybersecurity Information Sheets (CSIs) with guidance for recommended best practices for improving the security of the cloud. The five CSIs include:

- Use Secure Cloud Identity and Access Management Practices
- Use Secure Cloud Key Management Practices
- Implement Network Segmentation and Encryption in Cloud Environments
- Secure Data in the Cloud
- Mitigate Risks from Managed Service Providers in Cloud Environments

Even if you are not personally responsible for securing your firm's cloud technology, the CSIs will give you insight into what you should be doing to protect your data in the cloud. Reviewing the CSIs will also help you assess how well your cloud providers are securing your data. We can't cover all the points referenced in the CSIs but will discuss a few that are easy to implement.

Cloud Access

The starting point is getting access to the cloud and the data stored there. Just like accessing any computer system, you should be using MFA to logon. You may be limited by the cloud provider in which MFA method to use. Our preference is to use push notifications via an authenticator app if available. Hardware tokens are better yet, but most firms won't have that as an option unless they have a high level of control for the cloud.

Access to the cloud is usually under the direct control of the firm. The firm defines the users that are authorized and what restrictions may be imposed upon each user. When you hear about cloud data breaches, a very large number are due to mistakes made by the end-user. Weak passwords, lack of MFA and password reuse are just some of the poor security practices that help attackers gain unauthorized access to the firm's cloud environment.

Separation of Duties

Another area to consider is separating out user functions and responsibilities. Think of it as the two-person rule when launching nuclear weapons. Both codes/keys must be valid in order to launch. Separating out duties achieves a very similar function with the cloud. No one person can take complete control of critical aspects of the operation. The end result is minimal damage should one user's credentials be compromised.

Network Segmentation

Segmenting the network means "chopping" up traffic into smaller sections that are isolated from one another. Firewalls are used to restrict which traffic is allowed for each defined section. Not only does this keep authorized usage within the segment, but it also minimizes any negative impact should an attacker land within the segment. The firewalls help isolate any malicious activity to the compromised segment instead of allowing full lateral movement within the network. You can see how critical that defense could be. Another bonus is that network segmentation is part of zero trust architecture (ZTA) which is becoming increasingly mandatory.

Encryption

Another key element in securing the cloud is utilizing encryption. It probably goes without saying that all network traffic should be encrypted. This means not only the traffic to and from the user and the cloud, but also within the cloud environment. Don't forget to encrypt any data at rest too. The CSIs identify various encryption algorithms and standards that should be followed.

Managed Service Provider Risks

In our experience, most firms do not wholly implement and control their cloud environments. Managed Service Providers (MSP) are utilized to provide much of the firm's cloud needs. This puts a lot of trust in the hands of the MSP. There is an entire CSI focused on mitigating the risk with MSPs in a cloud environment.

As firms go through the MSP selection process, consideration of the MSP's security operations is a key part of due diligence. Besides following the best practices recommendations in the CSI, we would also suggest focusing on the responsibilities and liabilities of the MSP when dealing with a security incident and any potential data breach. Many of the MSP contracts we've seen attempt to shed liability for any data breach. Make sure that language does not exist in your MSP contract.

CIS Controls

In addition to the CSIs from CISA and NSA, the Center for Internet Security (CIS) has Critical Security Controls. CIS Controls V8 is the current version. CIS Control 3 and CIS Control 16 are particularly relevant for cloud environments as they deal with application security and data protection.

Convenience vs. Security

You have certainly read about and probably even experienced the movement towards the implementation of single sign-on (SSO). The intent of SSO is to make it a lot easier for you to gain access to multiple systems without having to login to each one individually. In other words, it's convenient. Does it really work? Yes and no. From what we've seen so far, each vendor seems to have its own way of trying to seamlessly integrate application access. The methods and successes vary. It's been a bumpy road for some and smooth sailing for others.

Most of the SSO activity we've seen recently is due to vendor acquisitions. The acquiring company wants its users to access the resources of the new entity as quickly as possible and without a separate login. Rather than migrate the new company application and data, SSO is rolled out to "merge" everything together. Frankly, we think it is more of a bolt-on band-aid than an integration.

Here's where we'll get a little controversial. While SSO can be seen as a convenience, we see it as a security risk and would much rather see separate logins to the data and applications. Something like network segmentation at the application layer. If a user's login credentials are compromised, the attacker has much more access if SSO is implemented. Obviously, the security of the environment is dependent on how well SSO is implemented, but we would rather see true system/data integration as a design goal.

We're also not fans of systems that allow for alternate logins using other system credentials such as "Logon with Google," or "Login with Facebook." Linking across accounts is another way for an attacker to gain access to multiple systems with a single set of compromised credentials. So, what is your firm doing right or wrong? Are you carefully monitoring what your MSP is doing? As we've watched the recent torrent of law firm data breaches, it seems to us that oversight of MSPs by law firms is often lax.

Final Thoughts

It can take a very long time for a law firm to build a solid reputation – and that reputation can be lost by a single cyberattack.

Sharon D. Nelson *is an attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* snelson@senseient.com

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* jsimek@senseient.com

Michael C. Maschke *is the Chief Executive Officer at Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity and digital forensics*

and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.