The Dark Side of Cloud Computing

by Sharon D. Nelson, Esq. and John W. Simek

We have said for many years that the cloud will generally protect a law firm's data better than the law firm would itself. As more and more law firms adopt Microsoft Office 365, thereby moving to the cloud, we have come to the conclusion that a few words of caution are in order when law firms entrust their data to the cloud.

With huge volumes of law firm confidential data (and data from other verticals) moving to the cloud, it is no wonder that the bad guys are taking aim at the clouds. And there seems to be a shift afoot, in which the main responsibility for protecting corporate data in the cloud belongs to the cloud customer rather than the cloud provider.

The Cloud Security Alliance (CSA) recently issued the latest version of its Treacherous 12 Top Threats to Cloud Computing Plus: Industry Insights report.

While there are many security concerns in the cloud, CSA's list focuses on 12 concerns specifically related to the shared, on-demand nature of cloud computing. CSA conducted a survey of industry experts to gather professional opinions on the greatest security issues involving cloud computing. In order of severity, here are the 12 risks.

1. Data breaches

Data breaches can result from humor error, application vulnerabilities, poor security practices – or they can be the result of a targeted attack. The data uncovered might be personally identifiable information, health records, financial information, trade secrets, intellectual property, etc. In our judgment, this is consistently the major concern for law firms.

2. Insufficient identity, credential, and access management

Criminals pretending to be legitimate users, operators, or developers can read, modify, and delete data; issue control plane and management functions; snoop on data in transit or release malicious software that appears to originate from a legitimate source according to CSA.

3. Insecure interfaces and application programming interfaces (APIs)

Cloud providers expose a set of software user interfaces (UIs) or APIs that customers use to manage and interact with cloud services. Provisioning, management, and monitoring are all performed with these interfaces, and the security and availability of general cloud services depends on the security of APIs. Clearly, they need to be designed to protect against accidental and malicious attempts to circumvent policy.

4. System vulnerabilities

System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a system to steal data, taking control of the system or disrupting service operations. Vulnerabilities within the components of the operating system put the security of all services and data at risk. When there are multiple tenants in a cloud, systems from various businesses are placed close to each other and given access to shared memory and resources, creating a new attack surface. Not a great idea for law firms.

5. Account hijacking

Cloud services add a new threat to the landscape. If attackers gain access to a user's credentials, they can watch activities and transactions, manipulate data (truly, the manipulation of data may be scarier than a data breach), return falsified information and redirect clients to illegitimate sites.

6. Malicious insiders

We have seen this time and again in law firms. A malicious insider such as a system administrator can access potentially sensitive information. Now imagine that malicious insider working for your cloud provider . . . systems that depend solely on cloud service providers for security are at greater risk.

7. Advanced persistent threats (APTs)

APTs are a form of cyber-attack that infiltrates systems to establish a foothold in the IT infrastructure of target companies, from which they steal data. APTs work stealthily over extended periods of time, often adapting to or eluding the security measures intended to defeat them. APTs can move laterally through networks and appear to be normal network traffic to realize their goals.

8. Data loss

An accidental deletion by the cloud service provider, or a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of customer data unless the provider or cloud consumer takes adequate measures to back up data, using best practices in business continuity and disaster recovery. Multiple backups tested regularly are a requirement.

9. Insufficient due diligence

Executives need to develop a good checklist for due diligence when evaluating cloud providers. Many rush aboard without a considered study of the cloud provider.

10. Abuse and nefarious use of cloud services

Poorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups via payment instrument fraud expose cloud computing models to malicious attacks. Bad actors might leverage cloud computing resources to target users, organizations, or other cloud providers. CSA cites examples of misuse of cloud-based resources including launching distributed denial-of-service attacks, e-mail spam, and phishing campaigns.

11. Denial of service (DoS)

DoS attacks are designed to prevent users of a service from being able to access their data or applications. By compelling a targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space, or network bandwidth, attackers can cause a system slowdown and leave all legitimate service users without access to services. This is not a theoretical threat – it has happened time and again in spite of good faith efforts to defend against such attacks.

12. Shared technology vulnerabilities

Cloud service providers deliver their services scalably by sharing infrastructure, platforms or applications. In general, this is a good thing, keeping costs down and allowing customers to scale up or down as needed. Cloud technology often divides the “as-a-service” offering without substantially changing the off-the-shelf hardware/software. Underlying components that comprise the infrastructure supporting cloud services deployment may not have been designed to offer strong isolation properties for a multi-tenant architecture or multi-customer applications. Shared technology vulnerabilities present a serious cybersecurity risk.

We are not trying to scare law firms away from cloud computing (just to be careful!), but it’s worth noting a study from last summer. A post in *RCRWireless News* said that a cyber security incident that takes a top three cloud provider offline for three to six days could cause anywhere between $6.9 to $14.7 billion in economic losses and between $1.5 and $2.8 billion in industry insured losses. That is one among many findings in a report published by Lloyd's of London in partnership with the American Institutes for Research (AIR), which explores the impact a cloud failure could have on the economy.

The results of the report were based on the top 15 unnamed cloud providers in the U.S., which together constitute a 70% market share. In the event of three to six days of cloud downtime, the report found that Fortune 1000 companies will carry 37% of the ground-up losses and 43% of the insured losses. This is, obviously, particularly meaningful to very large law firms.

Businesses outside the Fortune 1000 are potentially at the greatest risk, carrying 63% share of economic losses and 57% of insured losses. Right out of the gate, we know that law firms consider being out of business 3-6 days unimaginable.

The corollary to a cloud disaster is mitigating your risk through cyber insurance. As the report says, "Organizations large and small are investing in risk and loss mitigation, including preventative security and post event recovery measures. The continued expansion of the cyber insurance market is both necessary and inevitable. Taking proactive measures now to build a risk-based cyber insurance ecosystem, ahead of the next truly catastrophic event, is essential to establishing more resilient communities and businesses."

Bottom line, the cloud is generally a good place to be for law firms, but it is not without its threats and complications. For solo/small firms, we prefer a hybrid cloud, where law firms own their own equipment which is secured by their IT provider in a datacenter where they have the assurances of redundant power and Internet connections. This environment does require more work in order to properly configure and secure the systems, but leaves access to the data in the hands of the law firm and not the cloud provider.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com