Understanding Cloud-based File Sharing Risks for Small and Medium Businesses

Understanding and Mitigating Risks

By Ken Foster
KMBL Security, November 20, 2011

The Cloud offers individuals and businesses a unique opportunity to collaborate and share information. This sharing can be accomplished from a smartphone, personal computer, or work system from anywhere in the world. This provides new and tempting opportunities for increasing business and providing services that help differentiate you from your competitors.

However, it's important you review your business model and take appropriate steps to ensure you meet new online privacy requirements. Failing to do so, will turn a positive to a negative at the speed of light.

Nowhere in the world is online privacy regulated more than the State of California. This is great for consumers living in the Golden State, but can be complicated for those doing business with its residents. This paper will provide you a scenario-based example of how a small business can leverage the cloud, consider the risks, and formulate a supportable solution that is based on the California Standards.

Our Scenario. This papers scenario will be based on a small tax accounting business located in Sacramento, CA. Our entrepreneur will have two employees which work from a single location, the owners' residence. The business will use computers to process the tax returns and files will be retained both electronically and in hard copy. During a normal tax year, clients meet with a tax consultant and deliver hard copy receipts, support paperwork and potentially data files from accounting programs such as Quicken. When a client forgets to provide an item, they must either fax, email, snail mail, or make another appointment to deliver the missing item. In all cases this slows down processing of the clients return.

Identifying your Requirements. Before beginning any technology undertaking, it's important you identify your requirements and the desired outcome. In this case, our entrepreneur is seeking a method to allow their clients send electronic files such as Quicken data files and provide a mechanism to send electronically any required / missing supporting paperwork more readily. The company has received many electronic files in the past several years from their clients. This is partially due to the proliferation of inexpensive copy / scanners found in many of her clients' homes and offices. These files come primarily in one of two methods:

- Delivered on Removable Media such as USB Flash drives, CD / DVD
- Emailed from the clients account (if under the email size restriction limits)
- Faxed if individual receipts

The ability to more quickly associate these files with the clients account would reduce the likelihood of loss or misfile and speed up the processing of their returns. Whatever the solution, it should cause minimal changes or complexity to the client.

Risks. As with any task, there is a certain amount of risk. The introduction of any new process into an established one required a new risk assessment. Let's analyze the potential risks associated with this requirement.

What is PII. When Businesses store information that can uniquely identify a consumer, it is referred to as Personally Identifiable Information or PII (correctly pronounced as P-eye-eye). The State of California, Office of Privacy Protection, identifies "The Social Security number (SSN) has a unique status as a privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential ". Other information considered PII includes Name and Address or Name and Phone Number information when it is combined to uniquely identify a consumer. The state has also passed rules and requirements concerning the formal notification and reporting of exposure of customer PII. Protecting this information both using our current process and any future process requires the client consider how to securely store, share, and destroy PII.

Accessing PII Securely. These are several considerations when it comes to accessing PII. These are broken down based on category.

Electronic File Handling. Any file that is electronic can be moved easily between systems, electronic storage mediums. Unfortunately this can be done insecurely with minimal restrictions. The best practice is to store PII on an encrypted volume which requires password protection (if practical). This helps to ensure that if your systems are compromised by malware or stolen, that the data contained is not accessible. This can be done using either commercially available software, OS provided solutions (e.g. Bitlocker), or third party freeware (e.g. Truecrypt).

Electronic Transmission. In this scenario, our business wants to improve the ease of transmission of client data files and digitized receipts. However, currently clients are sending copies of their PII insecurely. Should a client's email be intercepted, they would never know. In addition, if the business uses email to send the client data, they risk causing a PII breach. So how does this business meet this requirement securely, by using Encryption! Our requirement stated the solution could not be complex and require minimal change. By using cloud-based file collaboration sites that include password protection and SSL encryption, the clients get a method to easily share files electronically and the business get the peace of mind that those files are encrypted from the client to the cloud and from the cloud to their computers. This significantly reduces the risk of a PII breach during transmission.

Finding a Provider. I have been reviewing this space for the past year. While many provides have come and gone, finding the right combination of security, ease of use, and cost

point has been nothing less than challenging. There are many providers who offer both free and fee-based services. However, whatever is implemented, the service must be easy to use by both the client and the Business staff. In this case, the solution I see as the best fit based on research is currently "SendthisFile.com". When reviewing other provides such as Box.com and Adobe - Sendit they lacked a business model that was designed for two-way collaboration or their costs were too expensive for the services offered. A business that were to leverage the

"Business Plan" level service would receive both SSL security while the files were in transit and Encrypted file storage (using AES-128) which awaiting pick-up on the cloud servers. Do not underestimate the importance of encrypted storage in the cloud. It is not simply enough to transmit the file using encryption to the cloud. The recent security breach at DropBox.com underscores the importance of storage encryption as well. For the cost of the business plan and the services you receive, this is the first service I can see as a viable situation to this issue.

Hard Copy Storage. The company business model includes a requirement to retain physical hard copy documents. The current process would include forms with physical signature, hard copy receipts, other source documents provided by the client, and a hard copy of the actual tax forms submitted. The storage of these files within fire-retardant locking file cabinets is a clear requirement. Should these files be stolen or improperly accessed, then a breach report would need to be filed with the state privacy office and all the impacted clients notified.

Destruction of Sensitive Information. This topic covers considerations to take when the retention value of sensitive information is exceeded, or at end of life of computer hardware.

Hard Copy Materials. Hard copy materials should be shredded using a cross-cut shredder with a rated cross-cut size of approximately 5/32" x 1-13/32". Depending on the volume of the materials, it may be less expensive to use a 3rd party shredding service periodically rather than spend the time and expense of buying a shredder. These services can provide on-site destruction of materials and certifications of destruction for your records.

Electronic Storage Media. For many small businesses, this is a mystery. We will cover the four areas most often overlooked and provide recommendations to reduce your overall risk.

Information Systems. Most businesses and consumers use a computer system to process or store sensitive information. It's important that prior to releasing control of the system to a relative, family member, donation to a worthy organization, or outright destruction of the device that you consider the data and its remnants contained on the physical disk drive. Many people do not realize that when you delete a file on a disk, it does not go anywhere. The file space is simply marked for reuse by the computer, but the enact file retains hidden on the drive until it is completely overwritten. Files overwritten can be recovered by hard drive forensics software even when overwritten several times. The best practice is to wipe, then shred the drive. There are several free utilities on the market that can accomplish this task.

The easiest to use is Darik's Boot and Nuke (Dban), which is a free utility disk you boot from and choose the level of destruction. I recommend you choose the DoD Wipe (no less than 7 passes). If it's good enough for the DoD, then it should be good enough for you.

Less Obvious Storage Devices. Did you know most printers, stand-alone copy machines, and fax machines have either flash or miniature hard drives. If your device contains an actual hard drive, then you must remove the drive and destroy it separately using a utility such as File

Shredder. Depending on your level of expertise, this may be best suited for a local IT Pro, as it will need to be mounted to another system prior to wipe. If you are leasing a copier, contact your servicing company to discuss how you can perform a "secure Wipe" on the device prior to return. Make sure you document this step. Often end of life copiers are shipped overseas for reuse in the 3rd world. They are often shipped without any drive wipe processing, exposing the former clients' data to whoever received the device.

CD /DVD Storage. These removable media formats provide a convenient method for off-line storage of information. According to the thexlab.com, the estimated shelf life of a properly stored, recorded CD Rom is between 50 and 200 years. This means that ensuring

their proper destruction is vital to protecting the clients' data. There are two methods for destroying this type of storage medium. The best and easiest method is to purchase a disk shredded. They can be obtained from local office supply stores and in some cases are integrated into medium sized office shredders. If you want to prevent even the most dedicated state-sponsored cyber spook from getting access to the data, use light sandpaper to rough up the non-label side of the disk prior to shredding.

Backup Tapes and Flash Drives. To ensure they are unrecoverable, you have two choices,

degauss using an NSA certified ferrous magnate system or shred them. The best method is direct shredding.

What to do if your Clients' Information is Exposed. If you are reading this portion, then you are already having a bad day. The absolute best course of action and also required by State Law is to report the issue immediately. In California, you are required to notify your affected customers immediately. A visit to http://www.privacy.ca.gov/business.htm will provide you templates for notifications and a list of actions you must accomplish. Consider this; the speed and thoroughness of your response will determine how your customers perceive your business. A sincere and rapid notification is far better received than a story on the local news after some of your clients identities have been compromised and traced back to your company.