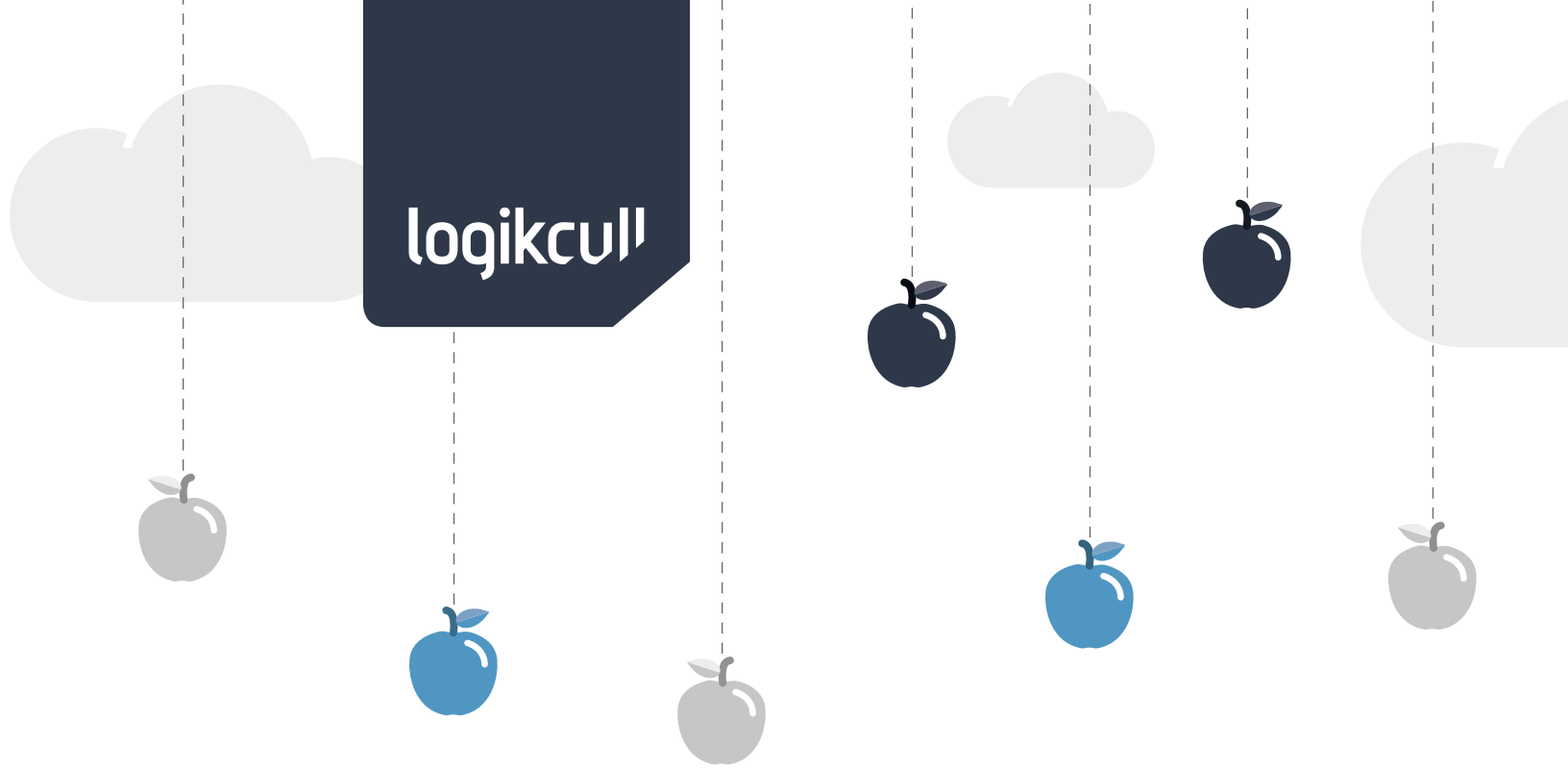


How to Prevent Your Client's Data from Getting Hacked

A useful guide designed to educate legal professionals on the many ways to keep client data safe and secure.

Written by The Data Security Team at Logikcull.com

As cyber-criminals continue to seek new opportunities for their break-ins, law firms constitute low-hanging fruit. Digital espionage is estimated to cost American companies over $50 billion per year, according to Harvard Journal of Law & Technology, and 10% of the advanced cyber-attacks were targeted at law firms. A recent study published by the American Bar Association estimates the average data breach to cost $7.2 million, with an averaged cost of $214 per client record.

Why is your law practice particularly tempting?

There are several reasons:

Concentration of sensitive documents
Large law firms tend to hold significant accumulations of private financial information, including due diligence materials, negotiation strategies, specific details on technological secrets, and many other critical items. In a globalized corporate environment, such materials as these can be worth millions of dollars to foreign intelligence interests.

Law firms have notoriously poor data security
Lucy Thompson, Chair of the ABA, points out that information released to law firms often enters an unguarded arena: "It's possible the information comes from a very secure source, a company with very good security. Then it goes to a law firm, and who knows what kind of security they are going to have."

Information is pre-sorted for value
Large companies accumulate vast quantities of documents, most of which have no usefulness to cybercriminals and corporate spies. A company's outside counsel, however, will only possess materials with the greatest sensitivity and value, so the interested hacker doesn't have to sift through mountains of unrelated material.

Achieving data security is not deeply mysterious, however, and for most law firms it doesn't require an enormous investment. Following a few well-defined steps can go a long way toward protecting your client data. The steps that will be discussed here are:

Minimizing storage locations
Protecting stored data
Protecting data in transit
Securing devices

It's important to keep in mind that the chain of data security is only as strong as its weakest link. Below we will analyze how each link in this chain can be separately protected.

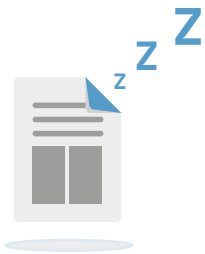
Minimize data storage locations

Each data storage location increases your overall exposure to possible compromise, and multiplies the effort you have to expend to keep data secure. Minimizing the number of storage locations and devices will simplify your data security program and decrease the chances of overlooking a vulnerability.

IComm Security Executive Ian Callens comments that data storage customers often omit due diligence in examining where their data is actually being kept. He says, "With daily cybercrime and cyber espionage having escalated by 24% in 2012, businesses need to be confident they know exactly where customer or employee data is physically being kept." Storing all sensitive data at a central cloud location with strong access controls and monitoring is often better than managing data storage systems yourself.

Step 1: Create a plan for consolidating older data and storing it centrally. Data sets that are not frequently accessed can often hold some of the most sensitive information. Encrypting and storing them on a secure cloud-based system allows them to be protected for as long as necessary, while also keeping them accessible as needed. Cloud-based data systems with datacenter storage are often more capable of providing a higher level of physical protection against catastrophic events than storing data on site. Redundancy in the provision of electrical power and state-of-the-art security monitoring can provide long-term safety for your older files and documents.

Step 2: Remove sensitive information from extraneous storage locations, and from devices that are scheduled for reuse or destruction. It's important to be aware that removing data is not the same as merely deleting files. For performance reasons, when you "delete" a file, you are actually only deleting the reference to that file. It's like crossing out a chapter reference in a table of contents. In order to truly remove stored information from a disk, you must "wipe" the disk clean. There are software products on the market that perform this task. Disk-wiping functionality is also built into operating systems as well. On computers running Mac OS X, the Erase functionality securely cleans magnetic media. On Windows machines, Microsoft's SDelete can be downloaded for safe erasure. The Electronic Frontier Foundation also stays up to date on the best security options for individual machines.



How safe is your "data at rest"?

"Data at rest" is an IT term that simply refers to inactive stored information. There are two approaches to keeping inactive data safe from hacking: Access controls and data encryption.

Access controls

These can take multiple forms, depending on the type of data. Basically they consist of access to specific physical portals, administrator-level knowledge of passcodes, or biometrics such as fingerprint access.

Even devices with single users need to be protected from unwanted file-sharing access. Sharing permissions are easily modified under both Microsoft Windows and MacOS X.

Devices with multiple users demand a higher level of expertise in setting up appropriate permissions. There is no fail-safe way to seal off access to any user who has administrator-level privileges, but file permissions can be set for non-administrative users on Windows or OS X machines.

Data encryption

Encryption is a way of scrambling information according to a certain pattern, so that only the users who have access to that pattern (or "key") can unscramble it and make it readable. Encryption technology is an excellent way to prevent data theft, even if a physical device is stolen, the thieves won't be able to actually use the material they steal without acquiring the key or performing cost and time prohibitive brute-force attacks. It's important to keep encryption keys safe, since the data will be permanently scrambled and unreadable if your key is lost.

Individual File Encryption

Some programs such as "zip" utilities and Microsoft Office provide password protections for individual files. This is the least secure method of encryption, but if you only want to protect the occasional file, make sure you set a strong password.

Whole Drive Encryption

Both Microsoft Windows and Mac OS X offer "whole drive" encryption in their recent versions. Keeping your operating system updated is essential so that you have access to recently updated encryption options. Currently, the best solution on Windows machines is called Bitlocker, which can encrypt all data on an entire drive. Mac OS X offers FileVault 2, which also provides "whole drive" encryption.

Third-party encryption software

As data security becomes more prominent in the marketplace, an increasing number of software encryption products are available to purchase. Utilities such as TrueCrypt can provide whole-drive encryption, but for most users the built-in encryption capacity of the computer's native operating system will prove easier and safer to use.

Regardless of which method of encryption you choose, it's important to shut off your device entirely when it's not in your possession. Certain encryption keys can be accessed by expert hackers if they find your device only sleeping or hibernating.

Protect data in transit

Inevitably, some information has to be downloaded or emailed, and this travel time is fraught with risk. When data is in transit, it can be subject to eavesdropping or tampering at various points in its journey.

Data encryption in transit
Standard web traffic is not encrypted, but there are more secure channels available if you know how to access them. Prior to transferring any customer data, ensure that the site domain name matches what you expect, and that the URL shows "https" instead of just "http".

SSL
These letters stand for "Secure Socket Layer," which is the method banks and online merchants use for handling sensitive financial information. You can purchase a SSL for a modest yearly fee from an authorized certificate authority such as Verisign or Digicert. This SSL page offers full information on how this encryption protocol works, and explains one of the most basic methods of protecting data while in transit. Websites that use https and SSL have a cryptographic certificate that proves the site's identity and authenticity. Site owners must keep this certificate valid, up-to-date, and "chained" from one of the recognized certificate authorities.

Email security
Email should not be considered a secure transport channel unless steps are taken to encrypt the message before sending it. By default, all emails, particularly those which travel outside of your own domain, are unencrypted and are subject to eavesdropping and theft. Configuring secure email transfer is not simple, and requires significant set-up. In most cases, it is preferable to use some other centralized sharing method or encrypt the files before sending them with a third-party software utility such as TrueCrypt.

How secure is your network?
Most people are well aware that using a public wifi network is risky for any personal information. Since business is conducted on a mobile basis now, from smartphones and iPads, it's tempting to sit down at an airport or coffee shop and just log on to get a little work done. If you do this, use your personal 3G connection rather than the public wifi network. If you absolutely must make use of an untrusted network, ensure that all security settings are configured. Make sure that information is cryptographically secure through https / sftp protocols, which provide end-to-end encryption.

For your office network, keep your router software up-to-date, and make sure that the technology is current. Avoid the outdated "WEP" security protocol, and make sure your router uses the newer and better "WPA2" method. Update your router password regularly and make sure it's strong.

If frequent connections to untrusted networks are required, it may be worthwhile to set up a Virtual Private Network (VPN). This will tunnel all traffic over an encrypted channel to a trusted location, such as within a company firewall or to a dedicated cloud provider. This is a complex task, however, and will require the assistance of a specialist.

Secure your device

The final piece in a program of keeping client data safe is to make sure that devices themselves are safe. The Journal of the American Bar Association highlights a survey showing that 36% of lawyers who use smartphones have lost them at some point, and 46% of those lost phones were not even protected by a password of any kind.

Mobile Devices
Use the fingerprint lock function on your iPhone 5S, or make sure to set up an alphanumeric password of at least 12 characters. It is also advised to set the device to wipe its entire information base if a certain number of unsuccessful access attempts are made. This is a good idea, but be sure the phone's information is backed up securely, as pockets and children can pose a danger to a phone with this setting in place.

Desktops and Laptops
Less likely to be misplaced, desktops and laptops are mostly secured through access controls, mentioned above. It's important to make sure, however, that they are fully turned off when not in direct control of an authorized user, and that all their software is kept updated.

Browsers and operating systems routinely issue patches to mend new vulnerabilities that they discover, or to protect against new breaches in their security. Make sure that these patches are installed, and that third-party security software is also kept entirely up to date.

Set up any firewalls or security software on your machines to run at frequent, automatic intervals. Be sure to install virus or malware protection software as recommended by your operating system vendor and update it regularly. There are free and low cost solutions for every operating system.

Summary

Following the outlined principles will help ensure that your law office's client data is only stored in absolutely necessary locations, is protected with access controls and encryption, is transmitted securely, and resides on safe, malware-free devices. Enacting a cloud-based security program will give your clients confidence in the professionalism and discretion of your practice, and will comply with American Bar Association standards for taking reasonable, competent measures to protect client information.

About Logikcull

Logik is the creator of www.logikcull.com - the leading cloud-based eDiscovery platform. Logikcull is ideal for corporations and law firms that want an easy-to-use, affordable, and secure eDiscovery platform without needing to invest in significant hardwar2e and software costs. Logikcull can be accessed using PCs and Macs as well as mobile devices including the iPhone and iPad.

To keep customer data secure, Logikcull.com resides behind an enterprise SSAE16 SOC-1 Type II certified data center. For added security and customer comfort, Logikcull is not hosted in a public cloud like Amazon Web Services (AWS). Some use cases for Logikcull are: eDiscovery & document review, information governance, document archiving, document collaboration, deal rooms, matter mobility, and internal investigations.

Logik is headquartered in Washington, DC and was founded by Andy Wilson and Sheng Yang in 2004.

Visit **www.logikcull.com**
Email **questions@logikcull.com**
Call **1-800-951-5507**
Follow us on Twitter **@logikcull**