“Servers, Hackers, Clouds and Eggs”

Defending your Law Firm against Information Technology failures and Cyberattacks

brought to you by LEXSERVO
YOUR DEFENSE NEVER RESTS

The implementation of Information Technology (IT) in the Law Practice has been the single greatest force of change in the industry since the 19th century establishment of Bar Associations. Starting with word processing, and then rapidly continuing with transformative tools such as data storage, spreadsheets, accounting systems, practice management solutions, and culminating with email, websites, and a cornucopia of Internet applications, the impact on the field of law has been nothing short of revolutionary. It is impossible to imagine a law practice nowadays attempting to function without the requisite IT capabilities and data backbone. In fact, the proliferation of LegalTech businesses, estimated by some to eventually mushroom into a $400 Billion industry, has created entirely *de novo* segments, such as Do It Yourself (DIY) legal solutions and Legal Marketplaces[1].

Unfortunately, this disruption to the traditional ways of practicing law contains within it a constant threat to disrupting a firm's operations, at times with catastrophic results. Data has become the lifeblood of the industry, across all areas of specialization. In the earlier days of technology implementations, practices had to deal with a myriad of hardware failures, software bugs, continuous operating system "patching" and ever-present network "gremlins" affecting access to peripheral devices such as printers and document scanners. Most importantly, nightly data backups were erratic and often unreliable, resulting in irreplaceable data loss when, say, a local hard drive would fail.

And then came the Internet.

Suddenly, everything became connected. And immediate. Colleagues and clients started communicating via email, to which data files were commonly attached. Now defensive measures had to be taken against computer viruses which crippled PC desktops and destroyed high value data. Online browsing introduced all sorts of Malware: Adware, Bots, Rootkits, Spyware, Trojan Horses and Worms all became part of our day-to-day lexicon, with our IT assets

1 "Legal Tech Startups Have A Short History And A Bright Future" - TechCrunch, 12/6/2014

seemingly under continuous attack.

And then came the Hackers.

Ill-intended operators, located anywhere from around the corner to around the globe, seeking to wreak havoc on your IT operations and data for fun and profit. Confidential documents routinely accessed by unauthorized users, privileged information continuously compromised, ongoing projects at constant risk of derailment, vulnerable employees being exposed to "phishing attacks", in an attempt to extract private information from them, and cyberattacks on law firms in which the aggressors are seeking to extract clients' trade secrets and insider financial information are very much on the rise. Clearly, battle lines have been drawn and a war is being waged. Two terrifying examples from Osterman Research:

> *An attorney in the greater San Diego area opened an attachment in a phishing email that he thought was sent to him by the US Postal Service. The attachment installed malware on his computer, and shortly thereafter he found that $289,000 had been transferred from his firm's account to a bank in China.*
>
> *A law firm in Charlotte, NC transferred $387,000 to a bank in Virginia Beach, VA after it closed a deal. Shortly thereafter, cybercriminals transferred most of this amount to a bank in Charlotte, which transferred the funds to a bank in New York and then to a bank in Moscow. The victim organization believes it had been infected with keystroke logging software from a phishing email that captured all of the critical information necessary to initiate the wire transfer.*
>
> *These are all examples of the types of the phishing and malware threats that are becoming more commonplace as cybercriminals become more adept, stealthier, and more able to penetrate corporate security defenses. The consequences of even a single such attack can be enormous, resulting in the potential loss of millions of dollars from corporate financial accounts, the loss of sensitive customer data, the loss of intellectual property like trade secrets or marketing plans, and possibly the dissolution of a business.*[2]

---

[2] Best Practices for Dealing with Phishing and Next-Generation Malware – Osterman research, April 2015

Not only are legal practice data repositories and networks under continuous threat from cyberattacks, the sheer complexity of hardware, software, data storage, routers, firewalls, backup appliances and peripherals can create an extremely high maintenance IT environment that is typified by numerous, concurrent points-of-failure. Stated otherwise, the IT environment requires constant monitoring, costly ongoing maintenance, yet still many things can (and do) go wrong, causing expensive disruption to the practice, with user downtime being the least of its worries; potential loss of data or confidentiality breaches can devastate an otherwise thriving firm.

While the aforementioned scenarios are germane to all legal practices, they are of particular significance to small- and medium-sized firms. Often lacking the human and financial resources to acquire and maintain secure, well-defended IT infrastructures, many entities find themselves woefully under-protected and exposed, unable to proactively invest in continual hardware upgrades and software updates, limited to putting out fires and playing catch-up, while critical data assets beckon hackers and other malcontents.

The good news is that the same Internet which had created all these headaches is, at the same time, the cure. Cloud Computing, which essentially is a set of converged infrastructure and shared services, facilitates the deployment of remote, ubiquitous, on-demand technology solutions that greatly reduce operational costs through economies-of-scale and improved efficiencies.

As Mark Twain famously wrote: “Behold, the fool saith, "Put not all thine eggs in the one basket" - which is but a matter of saying, "Scatter your money and your attention"; but the wise man saith, "Pull all your eggs in the one basket and - WATCH THAT BASKET.”[3] Thus, more than a century before the emergence of the Internet, America's preeminent humorist had succinctly defined the value proposition of the Cloud.

---

3 “Pudd'nhead Wilson's Calendar” ---Mark Twain, 1893-4

The advantages of Cloud-based IT implementations to a law firm are legion: First and foremost, the ability to effectively secure an entire legal practice by limiting application and data access to Secure Cloud Desktops. Under this methodology all applications are located centrally, continually monitored, updated, and protected, with extremely strict user authorization and data privileges. A centralized infrastructure allows a firm to enjoy the most robust possible environment, with multiple redundancies, eliminating most points-of-failure. By virtue of the remote access nature, authorized employees may enjoy application and data access from alternate locations, such as a home office, court room, or client site, utilizing mobile devices, yet do so in an entirely encrypted, secured manner. The firm no longer has to attend to costly, unpredictable hardware and software upgrades, and data backups occur on a continuous basis, insuring no losses. The inherent economies-of-scale and typical monthly subscription model facilitate the highest level of data security, integrity, and privacy, while keeping costs low and predictable. Lastly, the scalable nature of Cloud Computing empowers the addition of users at a moment's notice.

Clearly, when it comes to protecting a firm's core IT assets, opportunities abound.

To learn more about how Secure Cloud Desktops can help your law firm meet the emerging Information Technology challenges, please visit us online at www.lexservo.com, or call us at +1.800.986.4375.

LEXSERVO
YOUR DEFENSE NEVER RESTS