How Leasing Assists Your Firm to Make Your Information Security Processes Bulletproof

By Scott McFetters

Security issues are cited repeatedly as the number one concern for law firms and most recently topped all other current trends. The 2015 ILTA TechSurvey revealed that nearly half of the 420 law firms surveyed identified security as the number one concern—and with good reason. As recently reported in Legaltech News, 80 of the 100 biggest law firms have been hacked since 2011. This year, firms are estimated to spend more than $6.9 million or 1.92 percent of their gross annual revenues on information security.

Security concerns are a game changer. Not only are clients mandating increased security measures, they are requiring that these security measures be absolute and transparent. Management of your firm's technology and equipment assets now falls under the mandate of these security standards to which law firms must adhere.

Every firm is now beholden to know exactly what technology and equipment it has in its possession, its location, its lifecycle stage, and the established processes required to securely return and dispose of the assets at the end of its useful life. As security measures evolve, so will the rate of technology equipment refresh alongside it-- firms cannot afford the risk of deploying technology beyond its useful life.

Two vital components of your pragmatic information security policy are IT asset management and a refresh program that ensures your law firm is equipped with the most current updated hardware and software. Leasing, as it turns out, is a financial tool which parallels your firm's goals to achieve both, assisting your efforts to make your information security program bullet proof.

Asset Management: The Key to Safe Practice

Prior to the new normal regarding security concerns and data breaches, organizations in general may have been reluctant to dedicate staff/overhead hours to tracking assets; it was on the bottom of the list. However, that has all changed—asset tracking is now a key feature of all organization's security protocols and compliance programs.

An "asset" can be defined loosely as any object that your firm owns, or will be leasing in the foreseeable future. Most, if not all, firms have hundreds or thousands of assets in its possession at a given time—and it's not just your proprietary software, company-issued smartphones and laptops but also used servers, desktops, tablets, SAN, copiers, printers and the client files currently sitting in storage. Asset management simply means knowing where those objects are and to whom they are accessible.

Headline breaches of celebrity smartphones and financial hacks at major retailers and now even law firms are a reminder of how exposed our information can be. We live in a world where each employee may have several devices (smartphones, tablets, and laptops) and data is often synced across all devices. Of course we don't carry all of our devices at the same time so it's imperative for your firm to take the proper steps to ensure employee data has been safeguarded.

Even something as simple as losing a file folder or confidential letter can make your firm vulnerable to security breaches; needless to say, it's even easier and far more dangerous to lose a smartphone. With no way to track--or an unwillingness to do so--what you have or where to find it, it can take far longer for such losses to be detected, which gives bad actors a much larger time window in which to damage your firm.

There are too many anecdotes of empty offices storing old/out of date hardware, unknown locations of loaner laptops, or employees leaving with their computers. These assets have not been secured by proper returns and compromise information security exposures.

IT asset management begins with cataloguing all of the hardware and software currently in use throughout your firm, and, in best-practice scenarios, moves forward to "asset tracking." Through the use of GPS-trackable RFID (which uses an electronic circuit to automatically identify and track tags—attached to objects—which contain electronically stored information), bar codes, or other tools, you create a continually updated database of what you have, where you have it, and who is responsible for it.

Firms and companies often store old hardware in offices and computer rooms that are accessible to employees, office maintenance teams and janitorial workers. Old hardware can come back to haunt you. Most of us hear stories where, for instance, a storm causes a power outage –and when the power is restored, it restarts the old servers—that was powered off but still connected— and it infects the entire network. This type of neglect leaves your firm exposed to security breach consequences.

Too many firms begin to put their information security plans in place during a crisis – which is to say, after there is an active breach or loss. Beginning with good IT asset management allows you to prepare for problems before they happen – and detect potential problems in time to prevent them.

Asset Tracking Basics: The "Lost Dog" Theory of InfoSec

As previously noted, IT asset management begins with a catalogue of all IT assets in your possession, including both hardware and software. This will not be a catalogue of the types of hardware and software you own (for example, "iPhones" or "Microsoft Word") but of each individual piece of hardware and software throughout the organization (for example, "Steve's

iPhone, Jenny's iPhone, Steve's Microsoft Word, Jenny's Microsoft Word," and so on).

Once these assets have been catalogued, they can then be tracked with asset management software. Internally, this can be provided by tagging each hardware or software asset with its own radio frequency identification (RFID) tag or other options.

When RFID-enabled tags are applied to your law firm's IT assets, they render each piece of hardware or software in your organization uniquely identifiable and trackable, so that any loss or theft can be found out and remedied quickly.

RFID technology has come to largely replace bar codes because it allows owners to locate lost or stolen items. Although barcode is less expensive in the short term, the RFID is 15-20 times faster than barcode processes and more durable, making it more cost-effective over time due to potential increases in efficiency and decreases in errors.

Bar codes, the previously preferred standard, identifies the item but does not provide unique identification of the tagged asset – the asset in question must be located and scanned. RFID chips do not have to be in the owner's line of sight in order to work; they only need to be in the read range which is large. Their radio frequency can be picked up remotely, and used to identify their precise location, unlike barcodes which mostly require a human to scan it. Several RFID-based asset management programs, such as WiseTrack and Radiant RFID, have evolved in recent years. The best programs will integrate a continually updated database with GPS tracking and software assets at any given time.

This solution provides law firms with both flexibility and security. Assets such as laptops can be "checked out" of the office at any time, answering the increasing demand for mobile and remote working arrangements. The RFID technology keeps track of those assets, thus preventing data breaches before they occur. Furthermore, the real-time results and databases built by this practice provide the sort of clear,

transparent evidence of due diligence that clients increasingly demand in the new legal market.

The right leasing partner assists your firm in its needs to track its assets. CoreTech has an online asset tracking, system which allows firms to:

- Track assets by schedule
- Order and sort by any field
- User defined fields available for custom tracking
- Search on any field by description and serial number
- Export to Microsoft Excel to upgrade your internal asset tracking tools
- Secure online access from anywhere in the world

Online asset tracking capabilities enhance your firm's ability to identify the location and disposition of its technology and equipment simultaneously – from anywhere, anytime.

Technology Lifecycles: Newer is Smarter

Knowing what you have – or even knowing where to find it – is only half the battle when it comes to InfoSec. In order to fully perform due diligence, you must also ensure that you are disposing of your hardware correctly, and that you are not using hardware or software beyond the end of its useful life cycle. The less frequently your firm updates its software, the easier it will be for hackers to access your information. In order to fully execute due diligence, you must ensure that lawyers and support personnel are working with the newest software available, and complying with all security updates.

For hardware, this is true simply because older equipment tends to break down – a worn-out server is at an increasing risk to crash, potentially wiping out crucial data. Old software is at an even greater risk. The older any given piece of software is, the less likely it is to receive security updates, making it more likely for a hacker to access, for example, a lawyer's e-mails in Outlook if the lawyer is working on an outdated, unsupported software version that can't repel newer modes of attack.

Leasing: Your Silver Bullet Asset Management Partner

It is oftentimes overlooked that law firms—as businesses—are successful based on their use of equipment and not from the ownership of that equipment. It is clear that the useful lifespan and the security lifespan of your firm's technology and equipment are decreasing. This means it may not be strategic in the current environment to own, as the depreciable life most likely will outlast the equipment's useful life as well as security protocols. In the past, many firms objected to leasing and preferred to own the assets as they did not have the staff and time to track the equipment and monitor their location. Those days are over.

Your firm should put together a workable disposition plan combined with a technology refresh program that will protect the firm from keeping outdated equipment in use that doesn't adhere to new and increasingly high security standards—as well as deploy rigorous asset tracking processes. Many firms have committed to current technology by means of leasing it over its useful life; at the end of the lease term, these organizations are just replacing hardware with a new monthly expense and have the security of knowing their hardware is correct.

These are in fact all benefits of leasing. If your firm is inclined to leverage leasing to assist with its asset tracking or other information security benefits, choose a partner you can trust, choose a lessor who:

• Knows your industry and is known in your industry.
• Has a long-standing reputation for both transparency and responsiveness.
• Communicates openly about terms and conditions in the master lease documents that can affect your total cost of ownership.
• Has the flexibility to meet the firm's needs through the entire lifecycle of the lease process.

As with most things—but especially when dealing with technology and equipment—the end is just as important as the beginning. Partner with a lessor who builds best practices throughout the lifecycle of the lease, including the end of terms—your information security compliance requirements will thank you, and so will your PR team.

Whether or not the firm leases, it still has to dispose of the hardware at some point. It is imperative that all equipment is data wiped to at least DOD data erasure standards level before leaving the premises. You have no control once it leaves the door.

—❖—

Scott McFetters, a member of this newsletter's Board of Editors, is President of CoreTech Leasing, Inc. CoreTech is an independent leasing company working in strategic partnership with over 100 law firms. For more information, please visit www.coretechleasing.com, follow on Twitter@CoreTechLeasing, or connect on LinkedIn at https://www.linkedin.com/company/coretech-leasing-inc-.