On Premise Standards Working Group
International Legal Technical Standards Organization

Kim Brand
January 16, 2011, updated February 13, 2011, added Google password tips 2/16/11
Updated 2/19/11, 8/2013
Updated 10/15/2015

Preface/Background

In the ‘On Premise’ standards, we consider the means practitioners employ to create, safeguard and share their work product using digital technologies inside the ‘four walls’ of their offices. Our emphasis is on the dual missions of data safety and security. (Bruce Schneier, noted security technologist, summarizes ‘safety’ concerns as related to unintentional acts, and ‘security’ concerns as related to intentional acts. Loss or compromise of data due to lapses in either safety or security can lead equally to ethics and malpractice liability for attorneys.)

The definition of ‘on premise’’ is in flux so our work here impinges on standards developed by ILTSO groups focusing on mobile and cloud technologies.

Server rooms/Data Closets

When viewed schematically, the premises of a law firm typically comprise offices, meeting spaces, public spaces and utility spaces. Somewhere within the premises a space (or data closet, server room, etc.) is generally reserved for technology equipment like telephone systems, Internet access, servers and central cabling terminations (sometimes call the demarcation Point or demarc) and equipment like switches, routers, firewalls, modems (DSL, Cable,) etc. There may also be power line conditioning equipment like Uninterruptible Power Supplies (UPS) and Surge Suppressors. (Those may be also installed at each PC or server.)

Large offices may have more than one data closet or server room. And if a firm grows to multiple locations, there may be such rooms dedicated to technology services and equipment at each.

Caution should be exercised to restrict access to the data closet and/or server room. It should remain locked with access limited to authorized employees and contractors. Some firms may choose to keep entry logs, but this may prove impractical for a smaller firm.

The practitioner should be aware that physical access to nearly any technology equipment and facilities makes security far more difficult. Passwords are impotent if an attacker can boot up a server with a ‘Live CD’ and browse the system’s hard drives; casually making copies on local media or transporting files over the Internet unhindered by firewalls or the access control lists (ACLs) carefully configured into the server’s operating system when it is operating normally.

We have also seen server rooms where backup media have been carelessly stored. Pilfering backup media is among the easiest ways to steal confidential information. Usually, this might be done by an employee, but backup media left unprotected in public places expose a similar threat. One solution is to encrypt backups, but simply keeping backup media in a separate/secure location is an effective deterrent to data compromises.

Edge devices

So called ‘Edge devices’ are equipment that face the outside world and which typically are employed to protect the IT assets operated within the four walls of the office. These include routers, firewalls, proxy servers and modems (DSL, Cable.) Each presents an avenue through which an attacker may gain access to sensitive information. Also, each represents a single point of failure that could ‘take down’ a law firm’s ability to send or receive e-mail, access cloud based services, conduct research or access other critical services. Internet access has become a vital element in the conduct of law - interruption of that access can have substantial negative consequences.

We recommend that, at minimum, a firm document the various access code, login/passwords, service provider contacts, account numbers, morel numbers and configuration details for every edge device they operate. Temporary interruptions to Internet-based services should be expected and plans should be made for work-arounds in the event access is interrupted for longer periods. This would include consideration of the impact if access to internal IT assets from the outside were cut off as well: remote workers and/or partners and/or other offices via VPNs, RDP/Terminal Services or other means (GoToMyPC, LogMeIn, etc.) Some firms way wish to consider redundant equipment/services with fail-over capabilities.

Hardware Firewalls

Hardware firewalls (as opposed to software, or personal firewalls,) are designed to prohibit access to internal IT assets by outsiders. They may also be used to prohibit outbound connections originating from inside a firm’s network. (Such as to restrict access to certain websites or transmission of information using certain protocols.) Their use is particularly important if a firm hosts services like a website or e-mail on servers which have access to their internal network and data.

Reports available from some firewalls may be useful in detecting inappropriate Internet usage or simply to measure Internet bandwidth consumed to understand where bottlenecks may be occurring.

We recommend that any service hosted on the internal network which requires inbound connections and/or port forwarding programmed into the firewall/router, be documented and approved by the firm’s management and periodically reviewed. (Such services should only be accessible using rigorous passwords or an alternative secure means. See: Updates, OS)

Firewalls operate software which requires configuration and periodic maintenance. A trained consultant should be employed to perform such administration, and monitoring, where needed. A poorly configured firewall can easily defeat any protection it might otherwise provide.

Penetration Testing

In cases where particularly sensitive data is stored and/or regulation requirements demand it, Penetration (PEN) Testing may be conducted to assure the effectiveness of a firm’s public Internet facing defense systems. For example the Payment Card Industry Security Standards Council (PCI) publishes the Data Security Standard (DSS) testing protocol and awards certifications based on a testing regimen conducted by trained ‘attackers’ who attempt to gain unauthorized access to a computer network.

Passwords

Among the most common means to secure information is the use of passwords. Typically, passwords are combined with account (or user) names to authenticate persons and ascertain their filesystem permissions or rights to services provided locally or remotely. Logins/passwords are often stored in devices and software to allow automated access to information and services within or between computer systems. Since account names often conform to predictable patterns, for example John Doe’s login name might be jdoe or john.doe, hacking a user’s account on a local file or mail server may simply be a matter of guessing his or her password.

Due to the sensitive nature of nearly all information managed by a law firm, and considering lawyers’ ethical obligations, it should institute a password policy, and assure its employees are trained on and conform to the policy.

Rigorous password policies sometimes lead to their own undoing. We have seen cases where passwords were written on Post-It notes and stuck to displays. Password sharing in a small office is not uncommon. At bottom, a relaxed attitude about passwords is a symptom of a lack of respect for client data and should not be tolerated.

Meanwhile, password management is frustrating and time consuming. We have been seen cases where access to systems has been delayed for hours or days due to a password lost or forgotten. Passwords used to protect backups or encrypt data can be problematic - when the data is needed, will the person who knows the password may be available? Do they still work for the firm? The loss of a password can be as great a danger to the illegitimate compromise of information as to the denial of appropriate access to information.

Password complexity may be adjusted to suite the individual environment, but we recommend the following minimum requirements:

> *Passwords must be 8 to 12 characters long composed of the following character types:*
>
> > *Uppercase Alpha (A, B, C, etc.)*
> > *Lowercase Alpha (a, b, c, etc.)*
> > *Numeric (1, 2, 3, etc.) or the following Special Characters (!, @, #, $,*, +,-)*
>
> *Each password must contain UPPERCASE AND LOWERCASE ALPHA CHARACTERS, and at least one character that is either a Numeric or a Special Character.*
>
> *Passwords should not contain parts of the user's login name, common words, common numbers (like birthday, age, SSN, address or telephone number,) or predictable sequences like 12345, qwerty, abcde, etc. (Note: The 250 most common passwords uncovered in a recently compromised system are listed here.)*

In high security environments, or where data is accessed remotely, passwords should be changed regularly to defend against the risk that a password was communicated improperly and may be used by a third party, former employee or contractor. The rules to change a password are generally comprised of the following elements:

Period: the number of weeks or months a password will remain valid

> *Repetition: the number of cycles of password changes that must elapse before a password may be reused.*

Further, specific rules about passwords should be a part of every firm's employee manual, training and culture. For example:

> *Passwords should never be shared.*
> *Passwords should not be posted in a visible place or kept in an easily accessible location*
> *Passwords should be unique to each system - different passwords should be used on each system: file server, e-mail, cloud service, banking, e-commerce, etc.*

Finally, a central repository of passwords should be maintained by the firm's management and protected appropriately: in a locked drawer, a password protected file and/or at another location. The inventory of passwords (and other authentication credentials - many systems now require answers to multiple 'challenge' questions to gain/regain access,) may typically include:

- *Administrator password for key computer systems: servers, security, telephone, etc.*

- *Encryption keys for wireless access points, VPNs, etc.*
- *Internet access, firewalls, router, proxy servers, switches, remote access servers, etc.*
- *Domain name registration accounts, web-site maintenance, DNS administration, etc.*
- *Backup media/on-line access password and/or encryption codes, etc.*
- *Cloud services administration passwords and account details, voicemail, e-mail, etc.*
- *Banking, broker and other financial service password and account details*

Note: Firms should assure that they have access to e-mail accounts to which password reset and administration messages may be sent

An increasing number of system may forego passwords altogether and rely on alternative means of authentication. These may include biometric systems which validate a user by retinal scanning, finger or palm prints and keycards or security tokens which require a user to carry a device. Some are quite sophisticated and expensive. Hybrid systems may combine technologies for added security.

Restricting access to confidential data should only be considered one layer of protection. We recommend that every firm conduct a periodic review and, if appropriate: third party audit, of the permissions which are extended to every employee and contractor. Only through persistent diligence will the confidentiality of privileged material be assured.

Remote Access

Controlling security within the four walls of a law firm is difficult enough. Offering remote access to internal IT assets is far more risky. However, the desire to work from anywhere at anytime is so compelling that these risks are overshadowed by the gains. We recommend that any firm that allows remote access to on-premise IT assets establish additional rules and procedures to protect the confidentiality and safety of information thus made available.

As we have mentioned before, allowing physical access to key resources in the server room, networking closet or even to desktop PCs presents its own challenges to data security and safety. We can predict, short of a break-in (which must be allowed for,) that those entering our offices are employees, guests, contractors, or at least persons which know our office exists, how to get in, and take the trouble to do so. Allowing remote access opens our virtual doors, albeit locked doors, to any one of the millions of people who need spend no more energy than to download hacking software that can scan for vulnerable systems automatically and then attempt to ‘pick’ our virtual locks while they sleep.

The most common type of remote access is gained using a free feature built into modern Windows Pro or Server operating systems, (but lacking in their Home versions,) called Remote Desktop Services, (formerly known as Terminal Services;) sometimes call RDP for Remote Desktop Protocol.

Terminal Services, if enabled, can present a virtual desktop to any client PC running compatible software. It offers good performance, remote printing, media redirection (so you can hear sound from your office PC on your home PC,) and access to both local and remote devices (including support for multiple monitors.) Later versions include encryption which prevents a 'man in the middle' from observing the activities taking place between the Terminal Services host and client.

There are several third party programs that offer similar features to Terminal Services: PC Anywhere (sold by Symantec) and Virtual Network Computing (VNC - orginally developed by Olivetti and released under the GNU General Public License and available free,) are popular. These programs are installed on both the host and client PCs and allow remote control of a PC, remote printing, etc.

We recommend that if Terminal Services, or any type of remote access is employed, that an encrypted connection should always be used. An encrypted connection may be created, despite using an older version of Terminal Services, if the office and home are first connected using a Virtual Private Network (VPN) which creates a virtual 'tunnel' through which the remote connection is established.

What is common among these remote access solutions is their requirement to allow an incoming connection initiated from a PC located outside the office over the Internet. This is enabled by forwarding a port at the router or firewall to the internal device hosting the remote access service. This requirement creates a vulnerability: unless care is taken to secure the service which is 'listening' for the connection, a hacker may attempt to enter login credentials to masquerade as a legitimate user or exploit defects in the remote access software or other services to otherwise gain access to the remote system.

We recommend that if remote access by one of these methods is enabled, that additional diligence be exercised to be sure that:

1. All Internet accessible services implemented in either software or firmware are updated as soon as possible after updates become available. This requires knowing when updates become available for affected systems by monitoring vendor announcements.

2. The log files for all Internet accessible systems are monitored for suspicious activity regularly.

3. A higher standard of complexity for login names and passwords is applied.

4. All remote access permissions and configuration details (such as port forwarding rules,) are documented and kept in a safe place. Should circumstances change, (such as the termination of an employee or contractor,) revocation of remote access rights should be made swiftly or, if possible, *before* the termination is effected to prevent installation of

‘back door’ access by the terminated party. Note: There is *no guarantee* that the terminated party didn’t configure unauthorized back door access at some prior time.

In addition, there are ‘brokered’ remote access solutions like LogMeIn, GoToMyPC and TeamViewer. These programs install software on hosts and clients which connect to a central server that brokers the connection between the two. In this way, no inbound connections to a firm’s systems are required. While these systems are more costly and the performance may suffer, they are inherently more secure and easier to manage.

Redundant Hard Drives

For any system on which client information or critical data is stored we recommend the use of redundant hard drive storage systems, commonly known as RAID arrays. Likely systems to include RAID subsystems include servers and desktop PCs which act as servers or which have been designated as so critical that the costs and consequences of a failed hard drive outweigh the rather modest expense of installing a RAID controller and additional hard drives.

The purpose of RAID arrays is to allow the hard drive storage subsystem to continue to operate, without data loss, after a hard drive failure. This feature is called: fault tolerance. The intention is to give the operator time to replace the failed hard drive and thus restore fault tolerance. In practice, we have seen systems with a RAID array that suffered a hard drive failure but went unnoticed, (that is the point, after all, of having a RAID system,) until another hard drive failed, at which point the hard drive subsystem failed and all the data was lost.

We recommend that every RAID subsystem be configured to report failures via an alarm, or better yet by e-mail, when their status becomes degraded. The e-mail address (or addresses) to which the report is sent should be monitored regularly. Procedures should be documented that include whom to call and the steps to take to replace the failed hard drive. For particularly sensitive systems, consideration should be given to adding a ‘hot spare’ to the array so that rebuilding the array may progress even before a service technician is called. This reduces the time to restore fault tolerance and reduces the risk of data loss.

Note: Maintaining a fault tolerant hard drive system is an important element of data safety, but should not be considered a sufficient backup solution.

For more background on backup issues visit:
http://datasafetyseminar.pbworks.com/w/page/16880667/FrontPage

Servers

As their name implies, servers are purpose built and dedicated (i.e. not used as a workstation,) to deliver one or more specialized services to a network of PCs. This may include file services, e-mail services, databases services or other services that the firm may require. A single server may be configured to host multiple services. Today, a server typically has one or more multi-core processors, additional memory and fault tolerant hard drive storage subsystems, robust internal power supplies with a filtered electrical service and/or uninterruptible power supply (UPS,) an integrated backup system and an operating system, like Microsoft Windows Server, Mac Pro Server or Linux, designed to deliver those services to dozens or hundreds of users together with the more complex security architecture to maintain data safety and privacy.

Law firms, like any small business, that operate five or more PCs, soon discover that sharing files, controlling access to those files and protecting information from loss or corruption is a job for which a desktop PC is poorly suited. In those cases we recommend the purchase and installation of a file server.

Firms which choose to host their own e-mail may implement an e-mail server. Despite the widespread use and familiarity of e-mail programs, e-mail servers remain one of the most complex, resource consuming, security challenging and maintenance hungry applications any business can deploy. In general, we recommend against firms with fewer than 25 employees hosting their own e-mail. Today, economical and reliable third party hosted e-mail solutions exist that outsource the operational risk and support for e-mail services. Dozens of vendors, including Microsoft, offer Exchange hosting. Google, among others, offer e-mail solutions and alternatives to traditional collaboration platforms..

Other common types of servers include database servers, (typically SQL servers,) document management/indexing servers, web site hosting servers, Internet acceleration and filtering servers, Intrusion detection, DNS proxies among other application specific servers.

As with remote access, caution should be exercised when hosting any server with inbound connections from the Internet. Vigilance is required to assure that hackers are blocked from accessing internal IT assets - and so we recommend that most small firms outsource deployment of services not required for performance, integration or security requirements to be located on the internal network.

Ideally, servers should be located in a secure area of the office and physical access to them limited.

Administration rights to servers should be limited to as few employees and contractors as possible. A [confidentiality policy] should be maintained with any contractor who has access to any server. Server administration logins and passwords, and the users who have them, should be documented and kept in a safe place.

Access to information and services should be controlled based on the dictum: the less access the better. Generally, groups are defined based on their collective need to access a type of information (e.g. client matter, personal files, e-mail, databases, accounting records, etc.) or service provided. Users are then assigned to groups and permissions are then granted to users and/or groups to access the file storage areas (*shares*) and services. The system of defining users, groups and the permissions with which each have access to information and services is collectively known as the Access Control List (ACL.) ACLs should be documented.

Windows servers support Domain Controller functions which centralize the administration of user accounts, including setting passwords. They are used in conjunction with the Pro versions of Windows operating systems: Windows XP Pro, Vista Pro and Windows 7 Pro. We recommend such features be employed to enforce and administer password policies if a server is used.

Many servers incorporate software firewalls and other configuration settings to limit access to the server based on the IP address or service port number. For example, e-mail servers may be configured to only accept connections on port 25, SMTP, from upstream e-mail filtering services. The general rule is to prohibit all connections and then 'open' services/ports on an exception basis. All exceptions should be documented.

For additional security, the files on the server may be encrypted. A number of systems are available: TrueCrypt and WinMagic are popular. Backups may also be encrypted. An important element of any encryption policy is password or key management. Care must be taken to assure access to encryption keys for data recovery. A lost key or password may be as catastrophic as a total system failure.

Proper server operation and maintenance includes:

1. Regular updates to all operating and application software
2. Installation and regular updates to Anti-Virus and Anti-Malware software
3. Multiple generations of backups to local media *and* offsite backups. (See infra: Backup)
4. Disaster recovery procedures (See infra: Disaster Recovery)
5. Periodic review of relevant system and application logs
6. Periodic review of user accounts, group memberships and share management (ACLs)
7. Periodic inspection of fans, filters and the general operating environment of the server

While it may be tempting to operate a server until it fails, we recommend that the useful life of a server is defined by the warranty period available from its manufacturer and the life cycle of the operating system and key software applications, whichever is shorter. It is not responsible to operate a server past its useful life.

PCs

PCs have become ubiquitous in every business. They represent both a source of increased productivity and risk.

We recommend that every employee of the firm execute an Acceptable Use Policy (AUP) that defines the ownership of the information technology equipment, data and services provided by the employer, the standard of care which should be exercised by the employee in the use of same, privacy obligations with respect to information processed by the employee, accommodation for reasonable personal use, restrictions on installation of unauthorized software, and training or proficiency required.

Every PC should be configured to require a login and password to start-up. We recommend Pro versions of Windows PC operating systems. When joined to a domain controller hosted by a Windows server, they support more secure password policies administered from the server.

To the extent possible, all information processed at the PC should be stored on a server if available, or in folders or libraries on the PC which is backed up regularly. (See infra: Backup.)

All things being equal, data stored on a PC is less safe than if it is stored on a server. In an environment without a domain controller, the assumption must be made that any and all information stored on a PC will be accessible to any user able to gain access to the PC. In other words, it is *not* appropriate to share access to a PC with non-employees. Further, if a PC is being used to host (share) information with other PCs on the network, the security of the information on the host can be no greater than the restrictions imposed for access to the PCs connected to it.

PCs should be configured to automatically logout or display a password protected screen saver after 10 minutes or less of inactivity.

A common threat today is the installation, wittingly or unwittingly, of unauthorized software on PCs by employees. These may be installed from CDs, or more likely downloaded from the Internet. Sometimes the software is as harmless as Weatherbug, but often it carries performance, productivity or privacy stealing payloads which the firm can ill afford.

Malware, delivered via compromised websites and exploiting security faults in browsers, is an epidemic that may compromise the most carefully protected PCs. Viruses, while less common than they once were, can still create havoc. Any *virtual intruder* must be considered dangerous to client matter confidentiality.

We recommend a multi-layered program to protect against PC infection and maintain maximum productivity and data safety:

1. Adequate training of all employees to alert them to common computer exploits and effective defenses; emphasizing the appropriate use of their PC to reduce the potential that ‘recreational browsing’ will land them on a compromised website
2. Internet filtering to restrict/prohibit access to inappropriate websites
3. Selection of ‘safe search’ features of Google or Bing.
4. Regular updates to all operating and application software
5. Installation and regular updates to Anti-Virus and Anti-Malware software

As with servers, PCs have a limited life. Desktop Operating Systems and hardware become obsolete more quickly than servers and their use makes them more vulnerable to evolving malware threats. We recommend that a firm ‘turn over’ their PC inventory at minimum every five years to remain protected.