Is it Safe?

by: Donald G. Carder and James Spencer

Anyone who has ever seen the film Marathon Man can grimly recall a famous scene in which a sadistic former Nazi played by Sir Lawrence Olivier tortures Dustin Hoffman with a set of dental tools, minus anesthesia, while methodically asking the question, "Is it safe?" At this point in the film, Hoffman's character has no idea what the "it" in the question is referring to, and protests his ignorance by saying, "I can't tell you something's safe or not, unless I know specifically what you're talking about. Tell me what the 'it' refers to." Olivier, unimpressed, merely reaches for another pointed probe and in a chillingly business-like manner repeats, "Is it safe?"

Ask any Information Technologist the same question, and they too, like Hoffman's character, will begin squirming uncomfortably in their chair, fully aware that their answers, no matter how thoughtful, are likely to result in some serious discomfort. Like Hoffman, IT folks realize that such questions hinge upon on a very specific definition of what the "it" is, and their internal encyclopedias contain thousands of terms the questioner may not even know exist. The problem stems from the simple fact that computer security is an extremely complex issue, one that the casual user has no desire to explore, or even consider. Ask a non-technical person if their data is secure and your likely to receive a puzzled glance, followed by a noncommittal shrug and an, “I guess so…” Ask an I.T. Worker, and you’re likely to receive something resembling this paper - an examination of multiple variables, scenarios, incidents, and responses delivered in a near overwhelming rush of words.

To the average computer user, technology is little more than electronic magic. They turn a machine on, strike some keys on a keyboard, and lo-and-behold, a world of wonder and productivity appears. While such thinking is common in throughout much of the business world, this attitude is especially prevalent within the legal services community, where decades of low budgets have produced environments where technology use is driven more by outside forces than strategic planning.

Thus we reach the heart of the matter at hand.

Every legal services agency knows that it is required by law to protect its customer or client data, but, for many, the specifics of how to go about doing so are as elusive as a unicorn's horn. For too long, many legal services agencies were playing catch-up with their more well-funded professional counterparts, having non-technically trained staff staple together systems comprised of second-hand or budget-bought equipment, following plans derived from an entirely reactive path to technological progress. Systems were not engineered, so much as cobbled together from pieces acquired via recommendations gleaned from bar journals, slick salesmen, and media-fueled paranoia. Security was, at best, an afterthought, and in some instances ignored out of a misguided belief that, because they are "the good guys," hackers would somehow be less likely to target them. While things have certainly improved in recent years, there is still (and will always be) room for improvement.

The idea for this paper stemmed from an online conversation that occurred a little more than a year ago, in which this author was asked if buying a certain software program would guarantee an organization's data security. More than a bit flustered at the simplicity of the question, an initial response was planned that included links to a comprehensive overview of how computer and data security worked, but, while there was no shortage of articles stressing the importance of good computer security, there was a surprising dearth of information about just how to go about doing it.

So what is computer security? And how does one go about achieving it?

Computer security is a lot more than just making sure your systems don't get hacked, it encompasses a variety of disciplines that include not only electronic security, but physical and human security as well. It is not an easy task - many elements will demand a level of attention far higher than many may be willing to give - but neither is it an impossible one. All it requires is a proper time commitment and a certain level of expense. The key to any good security plan is to start with the best of all possible foundations, then build wisely and efficiently from that point forward. Your goal is to develop a series of inter-connected policies, procedures, and systems, and implement them in a manner dictated not by desire, but genuine need. To do this requires significant preparation and planning, which this document seeks to provide.

PHYSICAL SECURITY

Computer security is not just about making sure your electronic data is safe, but also that the physical assets that house them are equally secure. These include the building you occupy, the equipment you own, and the people you employ. The things being protected can consist of the building itself, and the offices and people within, or interior equipment such as servers, desktops, network equipment, copiers, fax machines, typewriters (yes, they still exist), monitors, keyboards, mice, hard drives, speakers, A/V equipment, and high-value copper cabling. Physical security is both the art of keeping someone else's hands off your stuff, and keeping your stuff safely ensconced inside its very own "Fortress of Solitude" - a place where you, and you alone, control the conditions of access.

Good physical security begins with the design of workplace itself. The primary goal here is to prevent unauthorized human access to facilities and equipment, primarily to prevent theft, tampering, sabotage, or incidents leading to disaster. Over the past 20 years or so, an emerging "scientific" approach to building design called "Crime Prevention Through Environmental Design, or CPTED for short, has emerged that presents adoptees with a set of of environmental considerations designed to improve the security of the workplace. Utilizing three core principles of "Natural Surveillance," "Natural Access Control," and "Natural Territorial Reinforcement," CPTED goes far beyond the traditional approach of "A locked door will keep the bad guys at bay," and looks at ways you can engineer the layout and "flow" of a workplace so that the risk of crime is greatly lowered. Recommendations range from the obvious - install quality lighting at doorways and trim the hedges so that ambush predators lack cover - to more subtle additions like human traffic checkpoints (dividing doorways, pass-coded elevators), clear pathways to exit points, office wardens (and the more controversial "office strongman"), and increased employee awareness and observation of their surroundings. The goal is to construct a workplace where the environment itself reflects an organization's attention to detail and constant vigilance. Most thieves are lazy, and deterrence is often enough to prevent a crime from ever occurring. Make an office appear difficult to "crack" and a thief is likely to think twice about a break-in, and move on to an easier target.

Often the most overlooked aspect of computer security, good physical security begins with an extreme awareness of one's surroundings. The key is to learn how to think like a criminal. Look around your server room and ask yourself how easy it would be to carry an armload of equipment filled with client and case data out a side door? Is it possible for a stranger to roam freely and unchecked by staff? Take a look at your offices, with those lovely new PCs and flat panel displays perched on the corners of desks sitting close to the windows? How easy would it be to heave a cinderblock through the glass and cart the lot off to the nearest pawn shop? Is there anything you can do to prevent that; perhaps a prickly shrub? And what if it's not just thieves you need to worry about? What if the threat is closer to home in the form of a disgruntled or disturbed co-worker? While some may consider the latter a disturbing question, it is just one of a host of valid concerns that need to be addressed when developing physical security policy. Theft can come from any avenue, at any time. Only by considering every possibility, no matter how uncomfortable, can you prepare and defend against loss.

- BUILDING SECURITY

Securing physical access to the building is just the first stage of tightening your organization's security. Other considerations include the safety of the building itself, which can be accomplished by intelligent engineering.

Visit any commercial data center in the United States and you are likely to see something resembling the following: Key-card locked doorways, bright lighting, and clearly labelled access points monitored by a nearby staff member. Equipment rooms will constructed with elevated flooring to aid in both cooling and cable management. Equipment racks will be bolted to the floor to prevent tipping, and power will be provided by twin, yet independent power sources backed by two separately charged battery banks. All electrical wiring will be kept off the floor to reduce the risk of electrocution in the event of flooding. Cabling for the equipment will be carefully threaded through specially designed brackets to eliminate tangling or dangling loops that can lead to accidents. The air within the room will be controlled by an environmental system that keeps it both dry and chilled to an even temperature. Dry-Agent Fire suppression systems rather than sprinklers will be used to reduce the risk of electrocution should a fire break out and the systems activate.   Connectivity to the Internet will be provided by redundant links which, like the power sources, should come from separate vendor circuits to reduce outages. Equipment mounted within the rack will be bolted in, with locking faceplates to prevent tampering by unauthorized staff, and clearly labelled as to purpose. You may even see an armed guard or two.

While such extremes may be beyond the budget of your typical legal services program, they should serve as an indicator as to just how much thought can go into the engineering of your infrastructure to provide safe, and reliable systems for your use.

- LOCKS AND CAMERA SECURITY

Installing door locks on sensitive rooms - such as the offices for your accountant or fundraising staff, server rooms, wiring and storage closets where equipment is kept - ensure that unauthorized personnel, or others, are prevented from deliberately or accidentally tampering with devices that are critical to a company's day-to-day operations. A lock is essentially a “territorial reinforcement” tool - it’s presence letting all and sundry know that behind these doors lie something you wish to protect. They act not only as preventative measures against theft, but also as a means by which accidents, such as an electrician cutting a phone line, or a cleaner unplugging the mail server, can be avoided. Ensure that only people with a genuine need have keys to the doors, and that changes in staffing result in a change of locks.

If you have the budget, and are technically adventurous, you can take things a notch further by installing key-card locks on extremely sensitive doorways. These are doorways that automatically unlatch when a smart-card is swiped, or bumped against a reading mechanism mounted on either side. They are extremely effective at preventing wandering souls from stumbling into areas they need not see, and act as a solid safety barrier to extremely sensitive areas. Most key-card systems also come with the capacity to create and store activity logs, which can be monitored and reviewed if any suspicious activity has occurred.

[Tip: For “bump” card readers, install the device at waist height. That way, a employee carrying an armload of equipment or crate of paper can bump the reader with the card in their hip pocket-saving them the trouble of having to set anything down.]

Security cameras are another strategically useful addition to monitoring sensitive areas. Low-cost web cams can be mounted inside a server room, and hall mounted cameras can be used to observe visitor traffic within the building, recording entrances and exits so that a record of all traffic is preserved fro evidentiary purposes. Some camera systems have built-in motion detection software that can reduce the amount of raw data storage required by only capturing images or video when there is something worth watching or recording.

One last note about locks and cameras: the legal services industry is a high stress environment - clients come because something in their lives has gone horribly wrong, and their emotions are likely to high and fragile. The last thing anyone wants to see happen is an individual give in to his emotional state and lash out in anger, either at the people in front of him, or the furniture and equipment around him. When planning out a building's design, take this risk into account, and establish areas where, should an outburst occur, your staff can take refuge, and the violence be contained.

- OFFICE/ROOM SECURITY

Employee offices are traditionally considered "open" areas within a building, primarily due to a need for ready access and ease of communication. However, there are some elements of office security that merit closer attention. To recall an example from above, consider that rather expensive piece of equipment your employee uses to do their day-to-day work, the personal computer. Contained within its electronic brain is a veritable treasure trove of client confidential information, user personal information, and company secret information that you most definitely do not want the outside world to see. While a closed door may prevent the casual looker from checking out the contents of an employee's office, a lock discourages the looker from becoming an interloper intent on physically carrying the computer (or anything else, for that matter) away.

Glass windows are problematic - everybody wants one, but they are the single most fragile entry point a building can posses. Items sitting too close to a window, be they computers or an employee's purse, can act as a theft magnet. All a thief need do is pick up a brick, heave it through the glass, then reach in to carry the device away. Some of the risk here can be mitigated by taking steps to reduce the ability for a person passing on the street to take a visual inventory of a room. Installing blinds or reflective film will help reduce the exterior visibility of an office, while simultaneously preserving a staff member's ability bask in the light of day.

While we'll get into methods to securing the electronic contents of the computer here in a bit, one of the easiest ways to prevent the theft of a desktop is to anchor it to the desk itself. Cable-locks are high tensile steel cables that can be attached to a PC and/or monitor's case, then anchored to a more immovable object such as the desk itself, much the way a bicycle chain is attached to a bollard. The cables are extremely difficult to cut, thus presenting a far more daunting task to a criminal mind.

Another thing to consider with office PCs is visibility. Office PCs should be positioned so that an employee has a full view of his nearest surroundings, including the doorway and any windows. Employees should never have their backs to an open doorway as this reduces their awareness of their surroundings, and the goings on within their office. Furthermore, by positioning the desk in this manner, you position a PC's monitor so it is not readily visible by anyone other than it's owner. Neither a casual observer in the hall, or our man in the street, will be able see the contents of a user’s computer screen, further protecting the confidentiality of the data displayed upon it.

Additionally, users should be trained and reminded regularly, to close out of sensitive materials when away from their desks. This includes short trips to the water cooler, to a copier, or co-counsel. Man is a curious animal - wandering eyes are easily attracted - and you never want someone seeing something they shouldn’t. Make sure your users understand the importance of never leaving their offices unattended without either closing down any applications displaying sensitive materials, or shutting and locking the door. Should they need to step out while a client is present, a quick activation of a password protected screen saver acts as a simple and effective snoop deterrent. Longer trips away from the office should demand a formal log-off (or an automated one, if necessary) so that an unsupervised visitor cannot awaken the machine and take advantage of something as simple as a browser’s “Back” button to tour previously visited sites such as online banking services.

Speaking of online banking, many user may have set their browser to automatically remember and provide authentication credentials for such sites. This, while convenient, is a monumentally bad idea. While the above example of using the browser’s “Back” button to regain access is increasingly rare, there are still a number of online sites that do not clear a login cookie properly, thus making the trick all too possible. Furthermore, depending on the browser, such passwords are trivially recovered - in some instances by a handful of mouse clicks. Make sure your users are aware of these dangers, particularly how they relate to any personal sites they may visit.

PERIMETER AND NETWORK SECURITY

Perimeter security refers to the boundaries between an internal office network and the wild west of the Internet. Perimeter security should be perceived, and constructed, as a layered defense, with no single mechanism considered a perfect solution. There is no such thing as a “universal security system,” nor will there ever be. Attacks, and the attackers that launch them, are on an evolutionary pace that far outstrips any one person’s ability to keep up, so it has become necessary to deploy defenses designed to assist in as many ways possible. Nor is it just the “bad guys” that you are defending your network from. When an organization decides to become a part of the Internet community, it implicitly agrees to be a "good neighbor", and not allow its systems to abuse the resources of others. Such abuse can occur either maliciously, in the form of a rogue employee, or inadvertently, in the form of an infected machine under the control of an outside agent.

Firewalls, intrusion detection systems, antivirus, anti-spam, connection monitors, log monitors, and data loss prevention systems are all just single elements designed to deal with specific tasks. A solid defense perimeter will consist of a marriage of multiple elements, carefully configured to interact with one another seamlessly, in a manner that is both understandable, and communicative of valuable and useful information.

The most commonly found components of a basic perimeter defense consist of an intrusion detections system (IDS) and a firewall. Both serve not only to prevent attack from hostile sources, but to collect and analyze data from the attacks for investigative purposes and reporting in the event of a successful breach. The primary difference between the two is that where a firewall serves to stop overtly hostile traffic from entering or leaving a network, an IDS seeks to examine traffic for covertly malicious behavior. Remember too, that the perimeter must be protected against threats coming from either direction - defenses should not only keep the bad guys out, but also contain anything bad within.

- FIREWALLS

A firewall has a pretty straightforward responsibility – it prevents unwanted traffic from ever seeing the inside of your networks. In simplest terms, firewalls are traffic wardens that examine network packets destined to specific ports, and allow them pass provided they meet certain conditions. Firewalls operate by riding herd over the 65,535 numbered ports that comprise the core of the TCP/IP protocol, ports used by assorted software programs and services to establish communication between networked machines both on and off the Internet.

So, that is what a firewall is supposed to manage, but how does one go about doing that? This simplest and most effective firewall configurations start by denying everything except activity on ports necessary for your network to function as expected. Smart administrators build their firewall rules by applying allowances one at a time, and examining logs of blocked connections to see if they contain references to traffic that should be allowed. As new services come online, new rules can be added with a minimum of fuss.

Deployment of firewalls had been traditionally reserved for the outer edges of business networks, as they were initially seen as devices designed to keep unwanted network traffic out. Thanks to the rise of the computer worm, however, it has become standard procedure these days to use firewalls as a secondary layer of defense within a network to contain and prevent locally infected machines from targeting other network segments.

- INTRUSION DETECTION SYSTEMS

An IDS system monitors all network activity in real-time, looking for suspicious traffic patterns that may signify the presence of an active attack. They accomplish this by examining network packets the same way an anti-virus program examines software, checking all traffic against an internal library of known attack patterns. Vendors of IDS devices update their databases of attack patterns regularly, and updates are released with enough frequency to keep customer comfort levels high.

One thing to look for when choosing a good IDS system is the presence of what is known as “deep-packet inspection,” a method by which the device searches for malicious payloads contained within what would normally be considered acceptable traffic. Deep-packet inspection has become increasingly important in the last decade as many of the more modern computer worms have shifted to concealing their activities within benign packets used for other purposes. A typical example might be a program requesting a web page while simultaneously passing along a command-and-control exchange to a hacker controlled bot-net.

There are two types of IDS systems that can be deployed: passive systems - which work by detecting intrusions and alerting an administrator for further action - or reactive systems - which can be configured to stop an attack in its tracks (Note: the latter is more commonly referred to as an “Intrusion Prevention System,” or “IPS”). Intrusion detection systems can also act as a policy enforcement tool; ensuring that an organization’s computers are properly configured, deterring rogue programs from launching attacks against others, and ensuring that sensitive information does not “leak” outside an organization’s boundaries without explicit approval. This latter aspect is a relatively new feature currently being marketed under the term “Data Loss Prevention” (DLP). DLP systems actively examine content entering and leaving the network, looking for elements that may compromise confidentiality and/or company secrecy. This can include scanning documents attached to e-mail for language resembling sensitive data such as Social Security numbers, bank account numbers, passwords, or language that may violate an organization’s protocols for acceptable communications.

SERVER SECURITY

Servers are the backbone of any enterprise. They are the equipment that enables e-mail to be delivered, files to be served, and client case management systems to be accessed. They provide remote connectivity to mobile workers, defend the perimeters, perform backups, and log network activity. An awful lot of responsibility, and an awful big target for those pernicious hacker-types. There are number of approaches to server security, but the core principles are relatively simple to grasp, if not always so easy to execute.

- SERVER HARDENING

Hardening a server refers to the internal locking down of services and processes so that they execute with the minimal amount of privileges necessary to perform their tasks. For brevity’s sake we’ll only discuss a handful of techniques here, but suffice it so say that server hardening should begin at installation. Obvious starter tricks include setting a BIOS password (to “freeze” hardware settings and prevent unauthorized modifications), installing only the services dictated by the device’s purpose (i.e., if your organization is not using FTP, don’t bother installing it), and creating a limited number of administrative accounts. Once these accounts have been created, and passwords assigned, the password file itself can be set to a “read-only” state to eliminate the risk of a remote attacker modifying its content. Log files for each critical service should be required, and either kept indefinitely, or rotated on an acceptable schedule with archives retained in case of an emergency. Log file attributes can be changed to only allow additions to the file, rather than deletions, which will be the first thing a successful hacker tries to do to hide his tracks. Utilities to aid in log file analysis can also be installed, provided they send their results to an administrator fully responsible for fully examining their content (Remember: should a breach occur, preserved log files will serve as the primary source of evidence). Remote connections to servers should be handled by services such as “Secure Shell,” or SSH, which encrypts the entire communication channel, thus preventing eavesdropping on commands. SSH has some additional capabilities, such as defining a set number of failed login attempts before a potentially malicious connection is dropped or fire-walled, enabling the use of an encrypted key exchange in lieu of passwords, and even defining a time-frame for when remote connections are allowed.

Within many commercial enterprises, individual services such as mail, web, and database are often located on separate systems to add virtual "fence" around their processes, reducing the risk of one compromised service carrying others down with it. Regardless of whether you take this approach or not, get familiar with the methods of hardening the services themselves to reduce the risk of a vulnerability in one leading to compromise of others via the granting of elevated privileges. Placing services within a protected environment (such as a UNIX/Linux "chroot" jail) will further restrict the amount of damage possible from breach. Finally, use encryption wherever possible, both for securing communications, and the data residing on the server itself.

- SCHEDULED MAINTENANCE

Just as desktop computers require the occasional update, so do servers. Unlike desktops, however, server updates should only be undertaken on special scheduling conditions so that downtime can be kept to a minimum. While a desktop update may affect only a single piece of software, most server updates will consist of updates to core files, libraries, front-end components, and utility code that that are all inter-connected in some way. Because of this, the risks of unexpected behavioral side-effects are increased.

Probably the best way to handle server maintenance is to adopt two simple approaches: the establishment of a development system, and a plan for regularly scheduled maintenance. A development environment is essentially a twin of a deployed server (called a "production machine"), where all the experimentation, testing, and playing around can occur without the risk of damaging critical systems or live data. By deploying updates to a development system first, and administrator can be sure that all server updates go as planned before applying them on a production machine. An alternative approach is to upgrade the development machine to state-of-the-art status, then migrate it as a drop in replacement for the production device. Whatever the approach, try to schedule all maintenance for periods of time when user demand is low. Evenings, weekends, and long weekends around holidays are the best times, but note that some upgrades take longer to complete than others. When you have a schedule in mind, notify all staff of the impending changes by explicitly stating what services will be offline, and how long you expect them to be gone.

- DATA SECURITY/AVAILABILITY

All the security in the world does little good if something as simple as a power outage takes your equipment offline, prohibiting your users from accessing your services and their files. You can avoid extensive downtimes by trying to build as much redundancy in place as possible into your computer and network architecture as possible. Typical forms of redundancy include secondary power feeds to each server (one per power supply if the server supports it), a backup ISP in case your local telco decides to do a little line cutting on a Monday morning, and battery backups for those times when the power company decides to do the same.

Mechanical redundancies are essentially mechanical backups - secondary devices that can assume the identity of a failed element in the event of a catastrophic loss. For servers, redundancy is most often provided by a "mirror," an identically constructed machine containing regularly synchronized data pushed on a schedule from its primary counterpart. Other network hardware such as switches and routers can be purchased in matching pairs, so that should one cut out in the middle of a day, the other can act as a plug-n-play replacement on a moment's notice. For workstations, the use of an imaging system to perform the initial construction of the machine gives you ready access to a rapidly deployed operating system that can be dropped on a spare hard-drive to bring a user's computer back online in a matter of minutes.

Do not overlook the importance of providing redundancies for your user's files as well. Backups are the key strategy here, with a number of approaches available to provide the best possible coverage. The standard model for file backup consists of a multi-tiered approach consisting of capturing full backups of a user's machines or server stored files at the beginning of the month, the beginning of the week, and incremental backups of new or changed files every single business day. Files backed up should be both compressed to preserve server disk space, and encrypted to protect their contents. By following this model, there will never be fewer that NINE copies of a data file in existence at any given time. However, the one shortcoming of this approach is that it does not account for a catastrophic disaster striking the facility that houses the servers hosting the backups. In order to prepare for such an eventuality, steps should be taken to ensure that the data being backed up is also pushed, mirrored, or physically carried offsite on a daily basis. If your organization resides on a wide-area network, and the amount of data needing to be moved a manageable size, nightly pushes of backups from one office to another can scheduled to occur in the wee small hours, when bandwidth demand is at its lowest. Branch office data may also be pushed around in a "round-robin" manner, with data from Office #1 going to Office #2, and Office #2's data going to Office #3, etc. Should the data being moved prove too much for a nightly push to process, portable hard-drives can be used to offload daily backups for physical removal from the office by trusted personnel. Finally, no backup plan would be complete without regularly tests to verify both the integrity of the backups, and your ability to restore them.

WORKSTATION SECURITY

Employee workstations, like the servers they connect to, should have strong controls in place to prevent end users from accidentally, or deliberately, bypassing security policy. We've already discussed methods by which you can protect the physical aspects of the machine itself, but what about the software and data contained within?

For an administrator, trying to keep a Windows workstation secure is a bit like playing a perverse game of whack-a-mole. A sad fact of the Windows operating system is that it grants the user far too many privileges by default; including the ability to install software detrimental to the performance of the machine. Part of the reason for this is Microsoft's desire to make using Windows as painless an experience as possible. In order to do so, Microsoft enables a lot of services and features that it feels users desire, rather than limiting things to what users need. When constructing a machine, a wise administrator will set about disabling unnecessary services and functions that have no practical use within his or her business environment. This not only increases the security footprint of the machine, but also frees up resources that can provide performance increases for the actual tasks that matter.

Another thing to look at is the security of the applications installed for everyday use. Due to flaws within the way Microsoft chose to implement its web browsing capability, it is possible, though difficult, for web sites to install software without any user interaction whatsoever. Browser settings should be tweaked to close as many loopholes as possible. Things to look for here include execution of web-based scripts, particularly those written in ActiveX, which has a history of allowing malicious code to execute without controls. Vulnerabilities also exist within common file formats, such as those used by Word and WordPerfect, which both allow the inclusion of coded macros that can compromise machine security. Further complicating matters are a number of other vulnerabilities that exist within the programs designed to run under Windows (we'll go more into these a little later in this document). See the "Resources" section below for a listing of guides on how to tighten up and tweak a typical Windows configuration.

Finally, make yourself familiar with the many options available found within Microsoft's Group Policy editor. Group Policy Editor enables you to customize the Windows operating system to your needs, modifying, enabling, or disabling elements to increase the security profile of the machine. Things like disabling the "Run" command (to prevent rogue installations of software), clearing caches and "history" logs (to protect privacy), enforcing password policy - including lockouts for failed attempts (to make them more secure), and securing access or modifications to key system files are all possible within this utility. Furthermore, many of these adjustments can be set at the server and pushed down to client desktops with the click of a button.

- ANTI-VIRUS/ANTI-MALWARE

It's a fact of modern life that computer viruses and malware are here to stay - hacking, it seems, has become a capitalist enterprise. In the "good old days" a computer virus was little more than a nuisance; infecting files for the purpose of spreading itself to other files. Rarely did any of these early infections possess any sophistication beyond the ability to propagate themselves. With time however, viruses evolved into complex code more closely resembling their biological counterparts in their desire to grow and thrive. Modern computer viruses now regularly contain a multi-pronged approach to infection, with the initial infection agent dropping additional installers and reactivation code in other areas of a computer's hard drive and operating system. Hackers now use these tools to harvest data off victim machines, or, in extreme cases, use those machines to launch attacks against others. Both of these newer approaches merit concern, particularly from a legal services perspective, as they can lead to breaches of client confidentiality, and the destruction of a program's reputation.

Because of this, it is necessary to provide some form of protection against such threats, and the installation of a solid anti-virus/anti-malware utility is strongly recommended. In the past, an anti-virus program by itself was enough to provide a modicum of peace of mind, but as newer, blended threats have become common, advanced features such as anti-spyware, anti-spam, and personal firewalls have become crucial companion components. Taken together, these applications make up the heart of what are called "security suites" - software devoted solely to protection. Such applications work by monitoring files, e-mail and Internet focused activity within a desktop computer, seeking known patterns of embedded code or behavior that may signify malicious intent. When such behavior is detected, they seek either to clean the files, restrict access to messages, or prohibit the activity by terminating or fire-walling any suspicious connections.

While the majority of these programs can be run with little to no user interaction - administrators can pre-configure many settings, saving the software the trouble of having to “learn” the difference between valid and invalid behavior - there are times when end users will be presented with alerts advising them that something is up. It is here that a lot of organizations fall into the common trap of failing to communicate expectations. Unless users are given a framework of reference detailing what kinds of alerts to expect - what they mean, and how to respond - there is a risk that they, the users, will only be confused by what they see and refuse to respond (or worse, ignore the messages). When faced with a cryptic message asking whether or not they wish to allow a program called “internet.exe” to execute or access the web, they are likely to agree simply because they have never been given instruction on when to say “yes” and when to say “no.” Additionally, some users may feel that the simple presence of anti-virus software means that their computer is automatically safe, and this false sense of security can lead to a weakening of defenses.

- PASSWORDS

While it may be true that no one likes being forced to remember multiple passwords, the reality is that the passwords exist to protect company resources, not employee comfort levels. No one wants to see their firm’s spokesman on CNN explaining how client confidentiality was breeched because someone found their password too difficult and reset it to their Social Security number, which they then posted on their monitor as a reminder. A password that is easy for an employee to remember is equally as easy for a hacker to crack, and employees will need to accept the fact that the needs of the organization outweigh the needs of the individual.

The key to a good password is to make it a mix of letters, numbers, and symbols, and then change them regularly. Password lengths should be no fewer than eight characters, with ten to twelve being an acceptable middle ground. The recommended lifetime for a sensitive password, such as those used for servers is no longer than 90 days, with the preferred minimum being 30 days. Try to ensure that users know they are not to share them – with anyone - or post them to, or in, any visible location. There will be wails and screams at this, with many pointing out how difficult they’ll be to remember.

This need not necessarily be true.

Here’s a little trick to password generation that can help your users more readily recall a complex combination of characters: Make them look like words. For example, let’s take a generic 10-letter word such as “Nailbiters” and convert it from a trivially cracked dictionary word into something far more difficult to break. By replacing certain letters with numbers or symbols that resemble letters, we can convert “I”’s to “1”’s, “A”’s to “@”’s, “S”’s to “5”’s, and “E”’s to “3”’s to get something like “N@1lb1t3r5.” What was once a password crack-able in a matter of micro-seconds is now something that requires a much more significant amount of time and effort to break. The more time a cracker spends guessing, the better your chances of catching him in the act. Furthermore, your users now need only remember their word of choice, and the formula for character replacement, making recall much easier for them and peace-of-mind possible for you.

[Note: Stress to your employees that the recommendations for password strength within the confines of the office, are equally applicable without. As we'll explore in a few minutes, good passwords can protect an office and its employees in more ways than one.]

While an end user may only be required to memorize three or four passwords, administrators get stuck with the unenviable task of having to remember not only their own day-to-day passwords, but also those of other users, server accounts, management interfaces, device web interfaces, business account logins, etc. Keeping track of these on paper is possible, but not advisable from a security perspective, so help comes in the form of utility software such as utility software such as "Password Safe" or "KeyPass." What these programs do is create an encrypted storehouse for account information and passwords that can be accessed readily by the provision of a single, "master password" that unlocks the application. Most modern versions of these programs allow a user to create classification systems for different types of passwords (i.e., "Web Passwords" or "Desktop Passwords") so that rarely used passwords can be more readily recalled.

- USER AND PROGRAM PRIVILEGES

One of the single most effective ways to keep unwanted software off an organization's computers is to eliminate or restrict an end user's capability to install them. Within Windows this can be accomplished by setting all user accounts to be "Restricted," which prohibits the user from installing any software without providing administrative credentials. This is useful for two important security reasons: license compliance, and anti-malware defense.

The long and short of license compliance is this: no organization should ever allow an unauthorized individual to install any software on an office computer without the express knowledge and support of administrative staff. Given free reign, some users will cheerfully install just about any program they can get their hands on. While this may be acceptable behavior within the confines of their home computing environment, it should be discouraged within the walls of an organization. Software licenses come with legally binding restrictions on use, and an organization failing to recognize the binding nature of these licenses is asking for trouble. Most software licenses, even those for so-called "free" software, come with explicit instructions on acceptable use, and terms of limitation of liability should something go horribly wrong. Some contain language stating that monitoring will occur as part of an effort to deter piracy. Other, more frisky, licenses may even contain language claiming things from full access rights to a computer's contents (which introduces privacy risks) to demands for constant connectivity (for license validation checks). All, however, contain prohibitions on how the software may be installed and used within an office environment, and these must be reviewed, understood fully, and accepted by an organization's leadership.

From an anti-malware perspective, if a user does not have permission to install software at will, neither will a rogue program inadvertently downloaded via a spoofed web page or e-mail link. Users running under restricted privileges have their software set (for the most part, anyway) to run in the same manner, greatly reducing the risk of what have come to be called "drive-by infections." The one exception to this can be found in the default configurations of many browser-based applications, which sometimes require the ability to launch external applications (ones completely separate from the browser itself) in order to complete certain functions. Some malware authors have caught onto this "feature," and have begun exploiting holes in these applications to bypass installation restrictions (more on this later). In order to combat this disturbing new approach to viral distribution, some vendors have begun releasing "sand-boxing" utilities for web browsers. A sand-box allows externally launched code to run in a protected environment that prevents permanent, and potentially dangerous, changes from being made to any files or the operating system of a computer.

- REMOTE ACCESS

If they haven't already, your end users will eventually discover an overpowering need to connect from remote locations to your organization's resources - either the company network, or their personal desktops. Whenever this occurs, a whole new avenue of security issues arises that you, as the administrator, and they, as a responsible user, will need to address.

First and foremost of these is the security of the user's remote machine. As this will typically be someone's personal equipment, an administrator should go to great lengths to make sure the user understands that, just as office computer security should be taken seriously, so should personal computer security. Anti-virus/Anti-malware applications should be present, machines should be kept up-to-date, and the same policy guidelines followed within the office should apply.

Then there is the security of the actual connection itself. Remote connections can be accomplished in a number of ways, but the most secure method is an encrypted virtual private network (VPN). VPN's use the public Internet infrastructure to establish secure connections between computers residing on separate networks by encapsulating network packets traveling between the two inside a encrypted "envelope." This prevents any machines those packets may travel through from being able to "snoop" the contents. Furthermore, VPN's can be configured to take advantage of any perimeter defenses established by an organization thus providing a little more peace of mind to both sides of the connection.

Wireless connections from remote computers should be monitored carefully, and only occur over well-known, and approved networks. While a remote worker may be tempted to accept the first wireless network their laptop detects, that does not mean should do so blindly. It has become increasingly common for unscrupulous people to set up freely available wireless networks for the sole purpose of harvesting any data traveling across them for later, more detailed analysis. This can include capturing encrypted data, which can be forcibly cracked at a later time. Be sure to let your employees know this, so that they are aware of the risks.

- HARDWARE CONTROLS

Another layer by which to provide physical security is to restrict methods of use on the actual devices themselves. Portable devices and media such as CDROM's, DVD's, USB keys, and smart-phones have the ability to contain files that can auto-execute upon attachment to a desktop computer. Consider the venerable application setup disk: when inserted into a computer's

CDROM tray, the operating system detects the presence of an “auto-run” file on the disk and executes the instructions to launch the software installer. Under supervised conditions, this would be expected behavior, but from a security standpoint, this is a dangerous event. Should a user insert media from a questionable source, or attach an un-vetted device, it may be possible for malware to be installed without your knowledge. Because of this, it is recommended that auto-run functionality be completely disabled. To take things a notch further, many computer’s system BIOS contain settings that can be set to enable or disable automatic access of removable devices such as USB keys. If your policies prohibit such devices, consider disabling this feature for an extra layer of protection.

Unauthorized devices such as laptops, wireless access points, and smart-phones should also be monitored carefully. No user should ever be allowed to attach any device capable of network communications to your systems without a thorough checking-out beforehand. Laptops may contain computer viruses and worms that could traverse the network. Wireless access points are open doors into your already secured systems, granting a clever hacker an unsecured entryway into your data and devices. Smart-phones can introduce both dangers, either by sneaking viral files onto a user’s computer, or by introducing the equivalent of a server device able to launch attacks with impunity.

APPLICATION SECURITY

Application Security is where the majority of your efforts will be directed, and where the biggest headaches will occur with regard to protecting your program’s information. There are hundreds of thousands of software programs available in the world, each with multiple versions, in multiple languages, for multiple platforms. The key to managing application security is, simply, awareness. However, when you take into account the number of applications currently in use throughout your organization, and the number of vulnerabilities and attacks released almost daily, keeping up with the latest developments for each becomes a Sisyphean task. Thankfully, there is help available for the latter, in the form of mailing list notifications provided by security minded organizations such as the SANS Institute and Carnegie Mellon’s CERT Team. Both bodies issue regularly released messages on the latest security vulnerabilities for mission critical, commonly used, and rather obscure software products and utilities. [On a side-note, both organizations also present excellent resources for CIO’s, CTO’s, and administrators in the form of trainings, seminars, conferences, and certifications.]

The best approach to handling application security is to create what is known as a “development system” somewhere off the company network. A development machine is essentially a test-bed computer whose sole purpose is to act as a guinea pig for any software trials and evaluations. Before performing any rollout of any new software addition, be it an application, an update, a browser plug-in, or minor utility, make sure you have tested the code thoroughly against any software you may already have in use.

Additionally, make yourself familiar with the option, or preferences, settings within the software already in place. Just because an application vendor thinks you may need a certain feature enabled, doesn’t mean it’s necessary. Two features imminently suitable for slaughter include useless “lurker applications” (such as “speed launchers” and “monitors”) that sit in the task-bar eating system memory better reserved for other apps, and options that enable unnecessary network or Internet chatter. Also be on the lookout for privacy violations in certain programs that wish to send "usage data" back to the vendor so they may "improve their products." Whenever possible, take a look at the support queues or mailing lists for the applications you use - these often contain useful guidelines on how to eliminate many of the nuisance aspects of the software in question.

- SOFTWARE DEPENDENCIES

Many programs are inter-dependent on others, meaning that you not only have to be aware of the security issues for your primary tool of choice, but also the plumbing that enables them to run. There are two types of dependencies present in most computer software: shared libraries, and co-dependent code. On machines running the Windows operating system, most software dependencies are hidden from the end user in a morass of interconnected files called "Dynamically Loaded Libraries," or DLL's. The purpose of these files varies; from presenting a common visual interface to end users, to enabling passage through Microsoft's core code for controlling access to a machine's hardware. During development, multiple software companies will make modifications to these DLL's to enable support for their needs. What is supposed to happen, is that these companies will collaborate with Microsoft in the creation of a "master" DLL to be released for distribution. Things don't always go as planned, however, and some companies will release modified versions of these DLL's that introduce behavior that has a negative impact on other software. This condition has come to be known as "DLL Hell," and is one of the principle avenues by which software vulnerabilities are introduced.

UNIX-based operating systems, such as Linux, have a similar shared code approach, wherein common functions needed by system services are stored in linked libraries. Unlike Windows, however, most UNIX dependencies are visible to an administrator during installation, typically via a package management system such as Debian's "apt-get," BSD's "ports" or RedHat's RPM Manager. A package management system is essentially a software database that contains not only a list of program you might wish to install, but also a library detailing the necessary, or recommended, dependencies for each. Whenever you select one piece of software for installation, the package manager will examine it's database and report back a list of any additional programs or libraries the software may require. While a little more informative than the Windows DLL approach, UNIX systems possess the same problem where one developer's desires may run contrary to another's. For example, an administrator who may wish to build a "headless" server (one not requiring a monitor), may find that a utility program he's selected for installation demands additional code designed to utilize a monitor. This unnecessary code then becomes an additional administrative burden, requiring attention and updating that was never initially desired.

Co-dependent code is separate software that is activated or accessed by a parent program in order to perform a specific function. In the old days of the BASIC programming language, most programs performed a single function. Nowadays, however, it is not uncommon for one program to have multiple sub-functions that trigger the execution of an external "child" program. The difficulty then becomes one of keeping the parent program's requirements in sync with those of the child, and making sure both can securely play well with each other. Probably the single best current example of this is the ongoing vulnerabilities in Adobe's Acrobat Reader, an application initially designed to do just one thing: display PDF files. Over the years, however, Adobe has added additional features to the application to enable support for things such as animations within PDF's (something this author is still scratching his head over), and scripting (which makes filling forms possible). In order to trigger these functions, however, the Reader application must make use of the Java programming language, which is developed by a different company. Either due to lack of communication, developer ignorance (or arrogance), Adobe's programmers failed to code functional support for Java in a secure manner, and the end result was/is a series of monstrously persistent security holes that enabled attackers to infect PC's by getting a user to simple open a poisoned PDF. These "zero-day" vulnerabilities (called that because there were no immediate defenses capable of preventing them) not only damaged the reputation of the once venerable PDF, but sent administrator's into a mad scramble to try and mitigate damage to their systems and networks.

- PROGRAM UPDATES AND PATCHES

Unfortunately, software is never static. As technology is released it is nearly inevitable that flaws be found and updates created to address the newly discovered problems. Such updates are called "patches," and they can address anything from a gaping security hole to adding new functionality to improve inter-operability with other technology. Whenever a new technology gains a foothold in the public consciousness, Microsoft has a tendency to enable it before an administrator has time to evaluate it and prepare. Because of this, it is important that administrators keep an eye on patch management just as they would application distribution.

Patch management can be handled in several ways, either manually by updating individual machines one at a time (often feasible in environments where a mix of hardware both old and new demands careful application), or via a centralized patch management application that can "push" updates to an entire network's worth of computers in matter of minutes.

However handled, patch management should not ever be left to its own devices. Going back to the previous example of a mixed environment of older and newer machines, a patch that works well with one set of equipment may have disastrous side-effects on another, crippling or even disabling functions that may, at first, appear totally unrelated to the issue addressed by the patch. Past examples include print driver updates that obliterated envelope formatting in a prominently used word processor, and a recent Windows security update that removed the ability for Microsoft Outlook to archive old e-mail. For this reason, all patches should be tested on a development machine before being widely distributed to staff computers. The trick becomes one of timing versus need. A patch for a zero-day vulnerability for a widely used program such as Adobe's Acrobat Reader may demand a shorter testing interval due to the severity of risk present, while a patch for a printer driver can be forced to endure a little more scrutiny and testing abuse.

- UPGRADES

Eventually, though, only so many patches will be released and applied before a developer finally reaches the point where he's had enough of the old and wishes to ring in the new. Upgrades generally introduce new features to programs designed to capitalize on user demands and emerging capabilities. Like patches, upgrades require significant testing before deployment, as new features usually come with a new look, and new things for your users to learn. The best most recent example of how an upgrade can seriously alienate unprepared users comes to us courtesy of Microsoft, whose recent modifications to its office suite completely replaced a previously well-known and understood interface with a maddeningly complicated interface that forced user to re-learn many things they had previously internalized as second-nature.

Upgrades also frequently introduce new functionality that has to be evaluated against existing abilities for suitability of purpose, inter-operability, and security concerns. To reuse Microsoft as an example, the release of Windows 2000 introduced the default addition of Windows Messenger, a program that provided chat capabilities. Messenger became a major nuisance for organizations that did not wish to provide chat services to their end users, as the software proved well-nigh impossible to keep off a machine. Administrators would disable, or uninstall the service, only to see it pop right back up on user desktops with the next Windows “Critical” update. Users already familiar with chat through personal use outside the office, would notice its return, and if unchecked, cheerfully sign up for the service with a personal account and begin sending unmonitored communications through the company firewall.

From an interoperability perspective, Microsoft once again gets a special mention for modifying its default file format for Microsoft Word on almost every single release, requiring early adopters to adjust their file save behavior lest they find no one else able to read their documents. True, an observant user could spot the change and force Word use a more commonly acceptable format, but that’s an assumption that the organization purchasing the product should make, not Microsoft.

But this is only the tip of the interoperability iceberg. Remember earlier, when we were talking about software dependencies? There are many programs on a computer that depend upon other programs to complete specific tasks. Upgrade one piece of software and chances are you will also need to upgrade these other utilities as well, a process by which you will find yourself continually returning to the starting point of evaluation and additional testing.

Therefore, before undertaking any software upgrade, it is considered best practice to perform a pilot rollout to either a test machine or a small group of technically savvy, and tolerant, users who are willing to put the software through its paces, while simultaneously noting any changes, or new, odd, or buggy behavior. Administrators can then collect these notes, and after removing or resolving the nuisances issues, deliver the software to remaining staff with a prepared list of caveats and training materials that explain the benefits and differences of the new program in language that eases employee fears and encourages experimentation and exploration.

- BROWSERS

Thanks to the popularity of the Internet, web browsers have now become one of the most co-opted pieces software on the planet, containing soft-coded links to dozens of other utilities that also have their own system requirements and further dependencies. The advent of thousands of assorted plug-ins and add-ons that can be installed without administrative privileges creates a whole new level of application management that can rapidly become a nightmare. As sites seek newer and flashier way to “trap eyeballs,” more and more plugins will come into demand, and the level of complexity of the once lowly web browser can rise to a level approaching that of the most expensive office suite.

The key to successful browser security is the development of a complete understanding of how all these optional features interact, not only with each other, but the sites your users may visit on a daily basis. The former can be accomplished by careful study of the software in a controlled environment (such as a development PC), while the latter comes down to pure grunt work. Contact your users to get a feel for the types of sites they visit regularly, then record these in a log, or bookmark them on the development machine. Whenever a new version of a browser or plug-in is released, test things on the development machine by visiting these site to make sure they still render properly. For those that don’t, you should contact the developer (via a webmaster’s e-mail address) and ask for a status update on when the new software will be supported, or if there are any known usable workarounds that will produce the desired results (also, feel free to strongly suggest changes be made for the betterment of all involved). If a web developer has no plans to support the new software, however, you are faced with a difficult choice: you can either hold off upgrading, or you can make an attempt to find similar services elsewhere, or you can make arrangements to provide a “sand-boxed” copy of the older browser for when the need arises. The danger here is that the longer the developer waits to update his code to play nice with modern browsers, the longer he is forcing his site’s visitors to expose themselves to completely unnecessary security vulnerabilities. Old code is just that: old, and as such, unworthy of defense. Any developer refusing to modernize out of some perverse preference for the “way things were” does not need to be gainfully employed.

EMPLOYEE SECURITY

Finally, all of the above will have no effect if employees do not buy into the organization's philosophy of precaution. Security is not just a collection of rules and guidelines, but a mindset that must be adopted by all. Like life itself, education is the key to any successful security strategy. It is not enough to inundate your employees with ream after ream of paper policies detailing ideal behavior for within the office walls; the lessons must be presented in a way that encourages employees to believe in the policies because they are the right thing to do. Strong and persistent training is a must, and should serve not only to define the conditions of a security policy, but to explain why it came into being and why the organization felt it was necessary for adoption. Only by continually reinforcing an attitude of security awareness, can a program achieve security awareness.

- POLICY

Policies and procedures are important; anybody saying otherwise is delusional. If your organization has not already developed acceptable use policies for technology resources, do so immediately, and give them teeth. Security is the one truly non-denominational aspect of any business and best practices must be followed by every single member of an organization, from part-time interns to executive directors. No one should be immune. While many like to think of their office as a home-away-from-home, the simple fact of the matter is that this is a business, not an extension of the living room.

As an administrator, you want to strike a balance between protecting your program from liability, while not making things so rigid your employees feel stifled. Policies should be developed with full employee participation, taking their needs and desires into consideration, and measuring them against what is best for the program as a whole. They can address thing such as how a server should be constructed, to how often the locks on the doors should be changed. Essentially, everything you will read in this document constitutes some form of policy recommendation. By documenting these recommendations, you have a framework of reference that serves not only to lay out a set of guidelines for acceptable procedures and behavior, but also a survivability mechanism that serves to explain to your successors how things got to be the way they are.

- HOME EQUIPMENT

While the majority of an administrator's job will rightfully focus on protecting the organization's resources and assets, you should also take the security of your employee's home equipment into account as well. Like it or not, employees are going to carry their work home with them, copying files from a properly secured office computer to a machine that may or may not be in the best shape. While the company cannot be expected to dictate the terms of its employee's household purchasing decisions, it can offer useful advice on how to keep their personal computer's from becoming a danger to themselves, and, by extension, the business.

Make sure that staff understand that if they intend to carry work-product home, that their personal computers should be kept up-to-date and secure as possible. Potential dangers include un-patched or outdated programs or absentee anti-virus software - which can lead to viral infections being passed to files carried back into the office - and un-secured home network configurations that can lead to captured credentials - bad for both the employee and the business.

- TRAINING

Just as with any business, it is important that a comprehensive training regimen be put into place to ensure that staff are aware of the need for strong security protections. As stated before, security is a tough subject, requiring a deep understanding of multiple variables. While staff cannot be logically expected to understand the "how" of computer security, they should be ready to accept the "why" as necessary part of their business life. The best way to accomplish this is by continual reinforcement of the message through an ongoing program of training. Technology training has another key benefit as well: it increases user familiarity with the systems the use, which leads to greater levels of both comfort and productivity.

Technology training should begin on the first day of employment. Just as you would take a new hire around the building to introduce them to their co-workers and coffee rooms, so should you introduce them to your information systems. Before any employee is allowed to use an organization's computers and networks, they should be given a formal orientation by I.T. Staff. This orientation should include not only demonstrations of how the systems work, but also how the employee is expected to behave while using them. Employees should be given copies of the company's technology policies, and time should be spent making sure that they understand the content and the logic surrounding them. They should be encouraged to ask questions, and an effort made to give them an answer they can understand. Any policies provided should also be signed by the employee, as an acknowledgment of their acceptance of content.

Beyond orientation, training can be accomplished in a variety of ways. As I.T. is a business unit, it should already be included in program staff meetings, and these can also be a place where I.T. announces any emerging developments in the computer security realm, and explains any implications. Classroom sessions on application use should also include coverage of known vulnerabilities and any mitigative steps staff can take to reduce their security profile. Administrators should also monitor technology news sources (see the "Resources" section below), relaying important bug alerts and announcements in a way that puts them into an everyday context the users can grasp. One thing to keep in mind when sharing technological information with staff is to try and refrain from using as much "geek speak" as possible. Non-technical staff are easily intimidated by jargon, and you do not want to alienate readers with a litany of technical terms they have no need, or desire to learn. By putting things simply, in terms they can understand, you not only gain their trust and confidence in your abilities, but also their curiosity, which will keep them intellectually involved in the organization's efforts to keep them safe.

- MINDSET

Which brings us to the final aspect of computer security, a character trait that Bruce Schneier calls "The Security Mindset." The best computer security experts, if there can ever be such a thing, got that way not because they possess a higher intelligence or deeper understanding of a particular technology, but simply because they have developed a particular way of looking at the world with a highly analytical eye. Part of it involves learning to "think like a criminal" - looking at the world with an eye attuned to getting around obstacles rather than erecting them. As Schneier himself puts it:

> Security professionals -- at least the good ones -- see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it.

While this kind of thinking can lead to some pretty depressing thought experiments (as well as a deep-seated cynicism) there is a hidden gift within such talents: the ability to see things as they are rather than as we fear them to be. The field of security deals with threats that are based on both objective experience and subjective speculation. It is the observed that can be studied and prevented, but the speculative requires a more cautious and analytical approach. As mentioned at the beginning of this paper, a proper security mindset is the product of both an intellectual and financial investment. Within the legal services community, the latter is always cause for considerable concern because there will always be times when the money simply isn't there. While it may sound ironic coming from the author of a paper devoted to electronic defense, be very wary about letting fear of a speculative threat drive a purchasing decision. Take a step back, look at the problem from a different angle, and ask yourself, "Is there another way I could accomplish this goal without spending fantastic amounts of money?" Going broke is the worst way to defend an enterprise.

CONCLUSION

While the above would make it seem as if computer security is an overly complex subject, it should be stressed that this does not automatically make it an impossible subject to grasp. Like anything business related, it simply requires a little investment, concentrated effort, and attention to detail. In recent years, many organizations have taken great strides forward in learning how to handle the complexities of information security, and thanks to the continuing spirit of innovation, curiosity, and support of others within the legal services community even greater strides are sure to follow. It is the authors's sincere wish that this document can, in some small way, contribute to these efforts, and any future successes.

ONLINE RESOURCES:

Ars Technica (http://arstechnica.com/) - Technology News, Reviews, Law, Etc.

Bruce Schneier's "On Security" (http://www.schneier.com/) – Looks at security from a variety of angles, from the obvious to the subtle. Excellent resource for developing the "security mindset."

CERT (http://www.cert.org/) – Carnegie Mellon/Homeland Security's Computer Emergency Response Team. Provides technical information and alerts about cyber-security issues and events.

Crime Prevention Through Environmental Design (http://www.cpted.net/) – Building design with an eye to crime prevention. Feng Shui for Facilities.

IANA (http://www.iana.org/) - Internet Assigned Numbers Authority controls lists of the root DNS zones, top level domain assignments, port assignments and other useful information.

List of TCP/UDP Ports (http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

SANS Institute (http://www.sans.org/) - The SysAdmin, Audit, Network, Security Institute provides training and certification on a variety of aspects related to computer and network security. Not cheap, but an excellent learning resource.

Securing Your Web Browser (http://www.us-cert.gov/reading_room/securing_browser/) – Covers Internet Explorer, Firefox, Safari and others.

Slashdot (http://slashdot.org/) – News for Nerds, Stuff That Matters

The Register (http://www.theregister.co.uk/) – Technology news with a warped sense of headline humor; also hosts the "Bastard Operator From Hell" diaries, which look at business and tech operations from a sadistically skewed point of view.

BOOKS:

CISSP® All-in-One Exam Guide Fifth Edition (Shon Harris)

Database Nation: The Death of Privacy in the 21st Century (Simson Garfinkel)

Hacking Exposed: Network Security Secrets and Solutions (Stuart McClure, Joel Scambray, and George Kurtz)

Linux Security Cookbook (Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes)

Microsoft Windows Security Resource Ki (Ben Smith, Brian Komar)

Network Security Hacks (Andrew Lockhart)

Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning (Gordon “Fyodor” Lyon)

Penetration Testing and Network Defense (Andrew Whitaker, Daniel Newman)

Practical Cryptography (Niels Ferguson, Bruce Schneier)

Practical UNIX and Internet Security (Simson Garfinkel, Gene Spafford)

Protect Your Windows Network: From Perimeter to Data (Jesper M. Johansson, Steve Riley)

Securing and Optimizing Linux: The Hacking Solution (Gerhard Mourani)

TCP/IP Network Administration (Craig Hunt)

TweakGuide’s “Tweaking Companion” (Kharoush Ghazi) - http://www.tweakguides.com/TGTC.html