Suggested APA style reference information can be found at http://www.counseling.org/library/

Article 39

Digital Confidentiality: A Holistic Security Model for Counselors

Paper based on a program presented at the 2011 ACES Conference,
Nashville, TN, October 26-30.

Timothy D. Baker

Baker, Timothy D., is a counselor educator at St. Cloud State University. In his current role and former position as a K-12 school counselor, he has worked in the design of secure data collection and storage systems for counseling accountability and outcome measurement, and collaborated with information technology security professionals to address issues of concern to professional counselors.

Counselors use technology widely (Cabaniss, 2002), for such purposes as training (Berry, Srebalus, Cromer, & Takacs, 2003; Chandras, 2000), and assessment (Lundberg & Cobitz, 1999), as well as communication with clients. The potential for technology to improve treatment services exists, but substantial barriers exist to the successful implementation of information technology (IT) principles in clinical settings (Wisdom, Ford, & McCarty, 2010). Indeed, these challenges are not unique to the counseling profession, but are faced by practitioners in the allied health professions (Briscoe et al., 2006; Curry, 2011). A general threat is the possibility of a malicious agent causing breach of information, known as "hacking" (Saporito, 2011). Hacking attacks have been sensationalized in the news media, with breaches suffered by the financial industry, sophisticated entities such as weapons contractors, military forces, and national governments (Albanesius, 2012; Goodin, 2011a; Goodin, 2011b; Schactman, 2011;). And yet, counselors who use electronic tools while serving clients have ethical and legal obligations to keep confidentiality (American Counseling Association, 2005; Health Insurance Portability and Accountability Act of 1996). Before entering into a counseling relationship, a client reasonably might ask: What security measures are in place to safeguard private data?

A Security Model for Counseling

A security model for the counseling profession should build on counselors' natural strengths: systems thinking, relationship-building, and effective communication. Keeping records confidential is not the work of a single professional, but the result of procedures and practices across the workplace. A team effort, guided by IT "best practices," can reduce the odds of a breach.

Such practices are well-understood and based on industry guidelines (e.g., Garfinkel & Spafford, 2002; Hope & Walther, 2008; Hunt, 2002). These practices have high "face validity." To make an analogy, consider how police advise motorists to lock the doors of their parked automobiles and keep valuables out of sight: The linkage to theft prevention is evident. Likewise, IT best practices are direct and reliable, and computer experts have attributed some high-profile breaches to the failure to follow industry norms (Summner, 2011). Best practices are well-defined, so in almost any setting, technical assistance can be found to help implement them. But best practices also are holistic: No part can be separated from the whole without a loss of synergy. All parts must be in-tune and in-balance to achieve harmony and the ultimate goal: digital security and confidentiality.

Five-Point Holistic Model

This model identifies five key components of the digital security "system:" You (the counselor who uses a computer), your computer, the network, servers, and storage devices. The purpose of this model is to create a conceptual framework for non-technical users who may be unfamiliar with the particular risks affecting each part of the model. However, effort has been made to present information that is technically-informed and accurate (Garfinkel & Spafford, 2002; Hope & Walther, 2008; Hunt, 2002). This model is also harmonious with the National Institute for Standards in Technology (NIST) guidelines for HIPAA compliance. The specifications described in the NIST checklist generally can be related to the framework of this simplified model (Scholl et al., 2008).

You

As the professional who uses a computer to maintain client records, you play the central role in data security. Perhaps the most important task in this role is the selection of effective passwords. Computer hackers have used electronic dictionaries containing up to 300 million words and pseudo-words, trying each in rapid sequence. Thus, any password composed of any known word from any language (including person, place, or pet names) is categorically unsafe. To build a strong password, start with an easy-to-remember amalgamation of words (e.g., "TheRaceIsNotToTheSwift" which can be reduced to an acronym (yielding "TRINTTS"). Include a mix of upper-case and lowercase characters as well as numbers (thus, "TR1NttS"). Passwords should be long – 8 characters as a bare minimum, but 15 or more is ideal (expand to "TR1NtoTheSwift", a very strong password). Note that any password is ineffective if it can be observed in plain sight, hand-written on a note taped to a monitor, or in an unlocked drawer. Also, a password saved in a web browser can be retrieved by anyone with access to that computer.

As a professional, you have responsibility for working with your client. But keeping data secure requires the trust, coordination, and discipline of an entire team. Many hacker attacks involve so-called "social engineering" techniques, which use deception; typically an attacker (one whose goal is to steal confidential information) places a telephone call or e-mail impersonating someone else, especially an authority figure (Greenburg, 2011). Professionals should always follow the written security procedures of their institution, whether a clinical practice group or university. For

example, many universities strive to educate students and staff that legitimate help desk technicians will never ask for a password. But it may help also to understand how trust is affected by incoming vs. outgoing information.

In general, incoming information should always be viewed with skepticism, because its apparent source easily can be falsified or "spoofed." E-mail sender addresses are easy to counterfeit, and the Federal Communications Commission warns that telephone caller IDs are also susceptible to spoofing, advising the public never to divulge sensitive information to an incoming caller (2011). In contrast, outgoing information can more reliably be directed to the intended source. The implication is that an incoming request for information should be followed-up with an outbound phone call or e-mail of confirmation. The case study detailed in Figure 1 describes the dangers that otherwise may be faced.

Your Computer

Your role in confidentiality and security is foremost, and the second most important consideration is your computer. The most critical aspects of computer security are operating system (OS) updates and anti-virus protection. In some cases, personal firewall protection may be beneficial, and some applications or programs have unique security aspects as well.

OS updates. A simple procedure to ensure that your computer has up-to-date safety features is to enable OS updates. For privately-owned computers, you may need to adjust the security settings for this to happen, while university-owned computers typically have OS updates enabled by design. A simple work habit can help make updates reliable and convenient: At the end of each work day, save your work, close all applications, re-start your computer, and leave it running (but not logged-in) overnight. This has three benefits. First, mid-size institutions usually have a local server that "pushes" out updates, usually overnight on a scheduled basis. Your computer must be powered on to receive the update, and may need to re-start itself after. In the case of your own personal computer, you can schedule it to check for and install updates during non-business hours. This minimizes the inconvenience of having updates run during the day, when you need your computer for work. Second, some non-OS programs only prompt to install updates after your computer has been restarted, for example Adobe Flash and Acrobat. Flash player updates install quickly and are important given their frequent interface to the Internet. Web browsers (e.g., Firefox, Chrome) also require periodic updates for security. Third, re-starting the computer frees up memory that applications may "request" and not always return, resulting in a slowdown of other programs. This is true of most computers and even smartphones. Re-starting your computer may improve its performance. In some rare cases, an OS update or software update may cause a program to quit working, but usually this occurs with highly-specialized applications; check with the vendor for details.

Anti-virus protection. The purpose of Anti-Virus (AV) protection is to prevent virus damage, which is not always apparent (as Figure 2 explains). AV protection serves two functions: "real-time" protection against a virus trying to enter the system, and periodic scans to locate a virus in storage. Real-time scanning relies on frequent virus definition updates (i.e., specifications of new, "zero-day" viruses being discovered continuously by security researchers). Your computer can be configured to download virus definition updates during the night. Scanning is a process that requires a few hours;

on a university computer, routine scanning probably has been scheduled to run during the night. By re-starting your computer each evening and leaving it powered on overnight, you provide a convenient time for the daily scan to run without affecting workday performance.

Also note that most universities make available to all students and staff, free of charge for use on their home computers, an industrial-strength version of an anti-virus product such as McAfee or Symantec. If you are not affiliated with an educational institution, you can purchase a product from a major retail store, or download a free program such as Avast, AVG, or Kaspersky anti-virus. Mac computers need virus protection, too, but know that fake anti-virus programs abound on the Internet, so download only from a reputable source such as CNET.com.

Personal firewall protection. A personal firewall is a system that determines how much a computer will "trust" and interact with other computers on the same network. Most workstations owned and maintained by an institution are part of its local computer network, computers that can "see" each other and share resources, such as a laser printer or networked storage (e.g., a "file share" or hard disk with documents that everyone in the office can access). On a home network, these shared resources may consist of a music library or streaming video and/or television. But if you connect your computer to wi-fi at the neighborhood coffee shop, those conditions of safety no longer exist. Recent versions of the Windows operating system ship with a built-in firewall which, beginning with Vista, displays a park-bench icon after connecting to a wi-fi network, giving you the option to set the network location as public. This helps protect against other wi-fi patrons intruding on your computer's contents. You also can adjust your firewall manually, and if you do not plan to share a resource (such as an attached printer or scanner) it is best not to enable them for sharing at all. This approach, called service pruning, helps prevent a variety of vulnerabilities.

A word on logon passwords. It may surprise you to know that a logon password, in most cases, does not actually protect the integrity of files on your computer. An attacker can still view your files by restarting your computer using a Linux boot disk, which will list and open your computer's files, or by stealing and removing its hard drive and installing it as a secondary drive on another machine; thus, physical access is critical to security. Even if it does not protect your files, a logon password should be used anyway, because it discourages casual snoops. It also prevents an attacker from operating the machine using your password identity, which can access resources, such as a network or a program, where other kinds of confidential information may be stored. Your computer should have a screen saver which "locks" the machine after a period of inactivity, typically 10 to 15 minutes (Scholl et. al., 2008). Note that a logon password may protect files securely when used in conjunction with full-disk encryption, a feature of some "professional"-version operating systems.

Linkages. In this holistic model, every point is connected to every other point. The second most important factor in security is connected to the most important factor – you. Your computer is safest when you are knowledgeable of security risks and have received training in your institution's procedures. You are able to create strong passwords for your accounts, and to assess accurately the strengths and limitations of using a logon password to access your computer.

The Network

In the Internet age, the network is the means by which most threats propagate. If you access the Internet through your institution, such as a university or office, you can help keep the network safe by creating a strong logon password, thereby preventing an attacker from stealing your identity credentials. By following best practices, a network can be made so secure that community agencies gain trust in their intranet, a private network complete with e-mail system – though as Figure 3 explains, sometimes it is difficult to know when the contents of an e-mail message are being quietly downloaded onto your computer.

If you set up a wi-fi network at your home, you should take steps to secure it against unauthorized use, because of the danger that a "free wi-fi surfer" may commit criminal acts online using your internet connection, which is traceable to you and can result in your being investigated by authorities (Walsh, 2011). As a professional counselor, even a fleeting moment of suspicion might harm your credibility. To reduce the risk, you should configure the "control panel" that is typical of wi-fi routers sold at big-box consumer stores. The exact instructions will vary, but usually the first step is connect the computer to the router with a networking cable, open a web browser and type an address like http://192.168.2.1 or http://192.168.100.1; these are not Internet addresses, but exist only on the local network, reserved for such devices as home wi-fi routers and modems (the exact address will be found in the owner's manual). Recommended options for the control panel are as follows:

- Assign a password to the control panel itself – usually consumer-grade routers ship with no password, or a generic password like "admin."
- Disable remote administration of the router. This helps prevent potential attackers on the Internet from tampering with your router.
    - Special note: Until you change these first two options, anyone, anywhere in the world, potentially can take control of your home wi-fi connection.
- Enable connection encryption security. This restricts who is allowed to connect to your network. At the time of this writing, "strong" algorithms include WPA2 and/or PSK with AES or TKIP encryption; these choices should appear in a list from which you can choose. An older protocol, WEP, is now considered weak. "Open" security means no security.
- Set a strong password for the encrypted connection. (This is a separate password than the control panel password.) In the case of a wi-fi network, consider a longer password of at least 20 to 25 characters, such as a phrase including spaces. You will only need to enter it once per computer.
- Change the default network name, or SSID. By default, routers ship with a generic name reflecting manufacturer and model (e.g., "Linksys router"). This can invite a hacker to probe its specific vulnerabilities. The Payment Card Industry's data security standards recommend that organizations change the SSID in a way that does not advertise the company identity. For a household, "the Smiths" might be a poor network name, while quirky "Chez Moi Cafe Americain" is better. (Early PCI guidelines required that the SSID be made invisible, but this is no longer encouraged.)

- Block ping responses to the WAN port. In plain English, a "WAN ping" is like an interlude from a stranger with unknown intent. To visualize a "ping," imagine that you are in a large city, and a stranger who walks up says "knock knock" to gauge your reaction. Will you respond "who's there?" Blocking the ping response helps your router stay "invisible" to the Internet, thus not posing an invitation to curious passers-by.
- Enable the network firewall (if not already enabled).
- Consider restricting MAC addresses, the ultimate security feature, though tedious to implement. A MAC address is a 12-digit alphanumeric code that uniquely identifies your computer's wireless adapter, a sort of serial number. Restricting MAC addresses increases security at the cost of convenience; the procedure how to do so exceeds the scope of this guide.

Linkages. Your skill as a counselor in creating good passwords will help keep safe your network (either a work network or home wi-fi network). Even if no client data is stored on your personal computer or home network, you will help protect your good name and trustworthy reputation.

Servers

Servers are the computers on the internet that give us information, entertainment, or vital services such as client scheduling and advertising contacts. For most people, our control over a server is limited to consumer choice – either use it, or choose a competitor. When choosing, consider such characteristics as security. The encrypted connection protocol for the web is https, often (incorrectly) called a "secure server." In fact the https connection only protects data in transit, and servers boasting secure connections can still become infected with viruses (Finkle, 2011). Still, https is an essential feature. Less obvious is the need for secure file transfer (sFTP). If you will be uploading files, is a secure FTP connection available? If not, logging on over an unencrypted wi-fi connection could put your password at risk, especially if you are using a public hot spot.

Because of the danger of a password breach, think about security in terms of "zones." Some zones, like your work e-mail, are critical. Others are trivial (e.g., login to post a comment on your hometown newspaper). Do not store in any trivial zone information that could be used to breach a critical zone, such as the answer to a biographical "password re-set" question required by another web site. Such questions introduce many risks, because they are too easy to guess, and because only a few are used – including some used by financial institutions for verification. Finally, Figure 4 discusses some of the reasons it is important to debate whether the company that operates the server is, itself, worthy of your trust.

Linkages. As always, your management of passwords is critical; keep separate passwords for different accounts, especially those with different levels of importance. Know your computer and how it interfaces with the server; does it use a browser (http) or file transfer (ftp) connection? If the connection is not encrypted, is that risk moderated or exacerbated by the characteristics of your local network, such as a wi-fi hotspot?

Storage Devices

Portable storage devices that can be attached to a computer, such as USB or "Flash" drives, seem to pose a great security threat because of the ease of losing a pen-

sized device, which can fall out of a pocket without being noticed. A preliminary step might be to attach them to a key fob or index card for visibility. Generally, it is difficult to protect against sensitive documents being copied onto such media by authorized persons for unauthorized purposes; such methods even have been linked to national security breaches (Leigh, 2010). More can be done to secure Flash drives as well as computer hard drives. Even if full-disk encryption is not available, "vault"-style encryption often is feasible; a vault is a large, encrypted file that resides on a hard drive. If opened with any conventional program, its results would appear as gibberish. But when opened with the encryption program using the password, the vault appears as a separate, virtual drive, to which one can drag and drop files.

Vault encryption utilities making use of strong algorithms are readily available. Many Flash drive vendors offer a free utility pre-installed on the media itself (such as Lexar Secure™ for PC and Mac, included on Lexar USB drives). The free application TrueCrypt (www.truecrypt.org) has undergone years of development and is well-regarded; before installing on an employer-owned computer, check with your IT department. Whatever the product selected, it is important for counselors to take an active approach: As Figure 5 explains, once a Flash drive has held client data, it might forever be treated as holding client data, even after it has been deleted.

Increasingly, "cloud" storage is gaining popularity. This entails file storage on a server over the network. While your ability to manage the server is limited, your ability to ask questions of a vendor is unlimited. Cloud storage can be described as "secure," but who has access? It is critical that every employee of the cloud storage facility be trusted, including the manager, IT staff, even security guards. Recently, a well-known cloud-storage company was the subject of a Federal Trade Commission complaint because of its terms of service stating that staff "cannot" access the confidential files, implying they lacked the capability. A computer scientist who felt this was misleading demonstrated the company used an encryption algorithm that stored the "key," a two-way encoding/decoding tool, on a server employees could access, implying they actually must have the capability to access clients' confidential files. Soon, the company's written policy was revised to state (emphasis added) that employees "*will not* access your files" (Hickey, 2011; Hood, 2011; Singel, 2011). Ultimately, you as a professional consumer may judge a vendor trustworthy and decide to trust them; but the decision begins with a fair assessment of risks.

Linkages. Are you able to manage encryption vaults and create strong passwords? Are you able to interview and assess data storage vendors? Are you able to research the nuances of cloud storage and understand the nuances of what vendors are telling you – and not telling you? At what point can you decide that a risk is "acceptable?" How, and when, should you communicate that risk to your clients?

Evaluation

Fortunately, or unfortunately, successful security procedures ultimately may be evaluated in terms of what does not happen: a breach of information. If no such breach has occurred, counselors can take a breath – but also maintain a pro-active approach to security by reflecting on their own use of security procedures. Do counselors consult with knowledgeable IT staff? Do counselors become educated in the security ramifications of

using a particular technology for storing client information? Do counselors have written policies describing what will be done if client information is leaked? How are backup or archival copies being made and stored? Most importantly, how are these facts communicated transparently to clients? Do counselors adhere unfailingly to their statements and promises in this regard? If all these conditions are satisfied, then the professional counselor truly has implemented a security model that is consistent with the values, tools, and ethics of the counseling profession.

Figure 1: A Social-Engineering Attack

In 2011, security consultant Aaron Barr, CEO of HPGary Federal Security, revealed in a news interview that he had obtained names of some of the leaders of hacking group Anonymous, and would soon reveal them to the FBI. Anonymous retaliated swiftly: Within days, hackers breached security at Barr's firm, posted thousands of his personal e-mails online – including a message from his wife threatening divorce – and erased several of the firm's servers. Discredited, Barr resigned (Greenburg, 2011). It was reported that the hackers' initial access to the firm's network began with a social-engineering attack; someone impersonating a senior executive contacted a clerk and demanded a password re-set. The enduring message is that even for high-tech companies, staff members throughout the organization who are properly trained and supported continue to be the greatest asset.

Figure 2: Myth or Fact?

"Many people's Facebook accounts are getting hacked, so I can be more secure by not signing up on Facebook."

Status: Myth. Many cases of Facebook accounts being hacked are only a symptom. The cause might be a virus on the person's computer which is able to intercept the Facebook password as it is typed; such a virus is called a "keylogger" and causes real concern (Shachtman, 2011). Often the best preventive measure is a functioning anti-virus program.

Figure 3: Myth or Fact?

"Someone once sent me a Word document as an e-mail attachment. I read it, but then deleted the e-mail. I need it back. Is it true the Word doc is still on my computer?"

Status: True. Microsoft Office applications must download a file to a "Temp" folder before it can be opened. The file remains on your computer indefinitely. To view the temp folder location, open a document from e-mail and then (in Word 2010) select the File tab, then Info. The file's path (the folder where it is stored) is displayed at top.

Figure 4: Myth or Fact?

"I heard that web sites can track people's movements across the web, and 'spy on' what you are shopping for."

Status: True, with qualifications (Potter, 2011). Web sites can do this by sharing an image file and a "third-party cookie," if all these sites tracking your movements have an existing agreement, typically through contract in a research firm (Perrin, 2009). Usually the mechanism is used for targeted advertising; when least expected, an advertisement is displayed promoting a product you recently viewed. This may be embarrassing,

especially for clients who need to keep their shopping for medical or behavioral health services private from an employer or spouse. You can educate your clients how to use a modern web browser such as Firefox which has a "private browsing" feature, which temporarily disables the browser's internal history log and acceptance of cookies. Private browsing does not, however, provide web browsing anonymity, and all clients should know that the owner of a computer (such as an employer) usually has a legal ability to "spy" on the person's web browsing habits (Lorentz, 2006; Mandak, 2011; Rothstein, 2000).

Figure 5: Myth or Fact?

"When you erase a file, it's not really 'gone.' It's still there; you just can't see it anymore."

Status: True. Even when deleted from the Recycle Bin (or Trash), most of the file persists on the hard drive for a time, and may be restored with a utility program. Before donating an old computer, consider using a "disk scrubber" utility to permanently erase the entire hard drive. Also, some encryption utilities have file "shredder" programs that will securely delete a single file. Finally, this risk does not apply if the file was stored in a secure vault initially.

References

Albanesius, C. (2012). Massive 'Flame' malware stealing data across Middle East. PCMag.com. Retrieved from http://www.pcmag.com/article2/0,2817,2404951,00.asp

American Counseling Association. (2005). *Code of ethics*. Alexandria, VA: Author.

Berry, T., Srebalus, D. J., Cromer, P. W., & Takacs, J. (2003). Counselor trainee technology use skills, learning styles, and preferred modes of instruction. *Journal of Technology in Counseling, 3*(1). Retrieved from http://jtc.columbusstate.edu/vol3_1/Takacs/Takacs.htm

Briscoe, G. W., Fore Arcand, L. G., Lin, T., Johnson, J., Rai, A., & Kollins, K. (2006). Students' and residents' perceptions regarding technology in medical training. *Academic Psychiatry, 30*(6), 470-479. doi:10.1176/appi.ap.30.6.470

Cabaniss, K. (2002). Computer-related technology use by counselors in the new millennium: A delphi study. *Journal of Technology in Counseling, 2*(2). Retrieved from http://jtc.columbusstate.edu/vol2_2/cabaniss/cabaniss.htm

Chandras, K. V. (2000). Technology-enhanced counselor training: Essential technical competencies. *Journal of Instructional Psychology, 27*(4), 224-227.

Curry, D. G. (2011). Selection and implementation of a simulated electronic medical record (EMR) in a nursing skills lab. *Journal of Educational Technology Systems, 39*(2), 213-218.

Federal Communications Commission. (2011). *Caller ID and spoofing.* Retrieved from http://www.fcc.gov/guides/caller-id-and-spoofing

Finkle, J. (2011). Nasdaq hackers spied on company boards. *Reuters,* Retrieved from http://www.reuters.com/article/2011/10/20/us-nasdaq-hacking-idUSTRE79J84T20111020

Garfinkel, S., & Spafford, G. (2002). *Web security, privacy and commerce*. Cambridge, MA: O'Reilly Media.

Goodin, D. (2011a). RSA breach leaks data for hacking SecurID tokens. *The Register*, Retrieved from www.theregister.co.uk/2011/03/18/rsa_breach_leaks_securid_data/

Goodin, D. (2011b). Stolen RSA data used to hack defense contractor. *The Register*, Retrieved from http://www.theregister.co.uk/2011/06/06/lockheed_martin_securid_hack/

Greenburg, A. (2011). HBGary Federal's Aaron Barr resigns after anonymous hack scandal. *Forbes,* Retrieved from http://blogs.forbes.com/andygreenberg/2011/02/28/hbgary-federals-aaron-barr-resigns-after-anonymous-hack-scandal/

Health Insurance Portability and Accountability Act of 1996, 45 CFR § 160 (1996).

Hickey, A. R. (2011). Dropbox cloud authentication bug sparks class action suit. *CRN Technology News,* Retrieved from http://www.crn.com/news/cloud/231000593/dropbox-cloud-authentication-bug-sparks-class-action-suit.htm

Hood, J. R. (2011). Cloud site dropbox drops the ball. *Consumer Affairs,* Retrieved from http://www.consumeraffairs.com/news04/2011/06/cloud-site-dropbox-drops-the-ball.html

Hope, P., & Walther, B. (2008). *Web security testing cookbook: Systematic techniques to find problems fast*. Cambridge, MA: O'Reilly Media, Inc.

Hunt, C. (2002). *TCP/IP network administration, third edition.* Cambridge, MA: O'Reilly Media.

Leigh, D. (2010). How 250,000 US embassy cables were leaked. *The Guardian,* Retrieved from http://www.guardian.co.uk/world/2010/nov/28/how-us-embassy-cables-leaked

Lorentz, K. (2006). Is your boss spying on you? *CNN,* Retrieved from http://edition.cnn.com/2006/US/Careers/03/24/cb.boss.spying/

Lundberg, D. J., & Cobitz, C. I. (1999). Use of technology in counseling assessment: A survey of practices, views, and outlook. *Journal of Technology in Counseling, 1*(1). Retrieved from http://jtc.columbusstate.edu/vol1_1/assessment.htm

Mandak, J. (2011). Suit against PC renter raises privacy questions. *ABC News,* Retrieved from http://abcnews.go.com/US/wireStory?id=13523926

Perrin, C. (2009). Paranoid cookie management. *TechRepublic,* Retrieved from http://blogs.techrepublic.com.com/security/?p=2335

Potter, N. (2011). Facebook privacy: Lawsuit charges facebook tracked users even after they logged off. *ABC News,* Retrieved from http://abcnews.go.com/Technology/facebook-privacy-mississippi-woman-sues-facebook-tracked-online/story?id=14754964

Rothstein, L. E. (2000). Privacy or dignity? Electronic monitoring in the workplace. *New York Law School Journal of International and Comparative Law, 19*, 379. Retrieved from http://cyber.law.harvard.edu/privacy/PrivacyOrDignity%28Rothstein%29.htm

Saporito, B. (2011). Hack attack. *Time, 178*(1), 50-55.

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C.D., & Steinberg, D.I. (2008). *NIST special publication 800-66 revision 1: An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule*. Gaithersburg, MD: US Department of Commerce.

Shachtman, N. (2011). Computer virus hits U.S. drone fleet. Retrieved from http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

Singel, R. (2011). Dropbox lied to users about data security, complaint to FTC alleges. *Wired,* Retrieved from http://www.wired.com/threatlevel/2011/05/dropbox-ftc/

Summner, S. (2011). Microsoft blames recent Sony and RSA hacks on 'rookie mistakes'. *Computing,* Retrieved from http://www.computing.co.uk/ctg/news/2083236/microsoft-blames-recent-sony-rsa-hacks-rookie-mistakes

Walsh, J. (2011). 18 years in prison for Blaine hacker next door. *Minneapolis Star-Tribune,* Retrieved from http://www.startribune.com/local/north/125444928.html

Wisdom, J. P., Ford II, J. H., & McCarty, D. (2010). The use of health information technology in publicly-funded U. S. substance abuse treatment agencies. *Contemporary Drug Problems, 37*(2), 315-339.

Note: This paper is part of the annual VISTAS project sponsored by the American Counseling Association. Find more information on the project at: http://counselingoutfitters.com/vistas/VISTAS_Home.htm