About this article: *Kate Gluck & Paul Fuller provide nine great tips for agencies to follow to protect against data breaches, which can destroy an agency's reputation and cost a lot of money to remedy. The article also points to resources the agency can access to get further information and to implement the recommendations. The authors seek to simplify an increasingly complex subject – laying out a series of manageable steps – in the hope that agencies will take action now to bolster their current agency security procedures where needed.*

Keeping Agency Data Secure

By Kate Gluck & Paul Fuller, Strategic Insurance Software

Benjamin Franklin once said that distrust and caution are the parents of security. The expression seems remarkably fresh and relevant in today's world, especially when it comes to protecting sensitive client data.

In fact, this caution is becoming more and more necessary. In an age of highly portable data (and of increasing identity theft)[1], independent agents have an ever-increasing responsibility to keep a lock on their client data. State and federal privacy and data breach notification laws and regulations (e.g., Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA)) put pressure on you to keep your clients' sensitive personal data safe. Even more important, if a data breach were to occur, your company's reputation would take a nosedive.

In an attempt to simplify a complex area, this article will touch on nine things – some basic and some not-so-basic – that an agency can do to mitigate risk of a data security breach.

1. - Keep data in a password-protected, encrypted space

Because so many of us these days carry our computers around with us, there is always danger of them being lost or stolen. While most people are honest, unfortunately the same cannot be said for everyone, and precautions must be taken to store client data in a way that is inaccessible to unauthorized users. The best way to do that is to encrypt and password protect it. There are three easy ways to do this:

- ***Store data in your agency management system*** – Because your agency management system is password protected, and data it sends over the Internet can be encrypted, data that is saved in your system or sent via Real Time, secure email or a Virtual Private Network has some measure of safety from prying eyes as long as the proper protocols are followed. Data retained on most agency management systems, however, is not encrypted, so it is extremely important to keep your server in a secure location if housed within your agency, or if you use your vendor's online

[1] Kristin, Finklea M. "Identity Theft: Trends and Issues." *Federation of American Scientists*. Congressional Research Service, Feb. Web. 22 Oct. 2012.

system, to have confidence in the security measures practiced by your vendor.

- ***Encrypt a folder on your hard drive*** – While your agency management system is a good location to store most client data, it is almost inevitable that you will have things saved outside of your system, such as on a laptop or USB flash drive. We recommend that the agency strictly limit the employees and instances where client personal data can be kept on such mobile devices and then only for a specific use, after which time the data is deleted from such devices. The trick is to keep this data secure as well. The first option for securely storing confidential information outside of your agency management system is to encrypt space on your hard drive. While this may sound complicated, in reality it is rather simple, so long as you know what to do.
    - To create an encrypted space—essentially a password-protected folder that you can save files to "on the fly"—our recommendation is that you use the very good (and free) TrueCrypt software. The open-source software is available for download at (http://www.truecrypt.org/), as is a step-by-step *beginner's tutorial on how to create and use a TrueCrypt container.*
    - Once you get the system installed and in use, the beauty of encrypted space is fourfold. First, in many cases it's free. Second, the simple step of creating and saving to a single file provides an added layer of protection. Because you and you alone decide where you want to file your encrypted folder, anyone trying to gain unauthorized access would not only need the password, they'd also need to know where to look. Third, it's mobile. You can copy and backup the password-protected file anywhere. Lastly, it won't slow down your machine.
    - *Summary: creating encrypted space on your machine is a convenient and controllable way to protect data that doesn't cost performance.*

- ***Encrypt entire hard drive*** – If you'd prefer not to worry about having to remember to save confidential information to one specific folder, another option is to encrypt your entire hard drive. From a user standpoint, essentially all this would mean is an extra login. From a security standpoint, it is about as secure as you can achieve, short of prohibiting that such data be kept on such portable devices. So secure, in fact, that if you were to forget your password, the likelihood *you'd* even be able to get back in is slim.

  One option to do this is BitLocker. (Available in the Ultimate and Enterprise editions of Windows 7 and Vista and in the Pro and Enterprise versions of Windows 8.) Another is the aforementioned TrueCrypt.

  Something to consider when deciding whether to encrypt your entire hard drive, or just space on your hard drive, is that in some cases, particularly with older computers, encrypting the hard drive may slow the performance of your machine somewhat.

  Summary: *The beauty of encrypting your entire hard drive is that if your machine gets stolen, without the password, no one can make sense out of it – the whole hard drive becomes a puzzle.*

- ***Smart phones and tablets*** – Agent use of these devices is growing exponentially and they pose additional security risks. Personal data might be contained in emails received from the client. Agency employees should take care to delete these emails promptly and not transmit this kind of data from these devices via unsecure email. In addition, the agency should make sure their employees have activated the password protection on these devices and should employ a remote wiping technology, so that if the employee loses or misplaces the device, the agency can restore the device to its original manufactured state with all of its data removed. In addition,

some larger agencies are starting to employ software on the mobile device that walls off and secures business applications and data.

2 - Create "Strong" Passwords and Keep them Secure

Because your password is the first line of defense in preventing unauthorized file access (whether to your agency management system, your encrypted file or your entire encrypted hard drive), it is important to create strong passwords and store them in a safe place. Best case scenario would be not to write them down at all. If you must write them down, don't carry them around with you or leave them in an easily accessible place.

Microsoft offers the following suggestions for creating a strong password[2]:

- Make sure it is at least 8 characters long
- Make sure it does not contain your user name, real name, or company name
- Make sure it does not contain a complete word
- Make sure it is significantly different from other passwords you have used
- Make sure it contains at least one uppercase letter, one lower case letter, one number and one symbol.

3 - Change Passwords Often

Experts have different opinions as to how often passwords should be changed. Our best advice on this is to set a standard for your agency (whether it be every month, every three months or every six months) and enforce that policy agency-wide. Of course, if you ever have any reason to believe that your password has been compromised, it should be changed immediately.

Many systems require this from you, and do so for good reason. It is much harder to hack systems that require frequent password resets. It adds a level of complexity for the hacker that can be both a deterrent and a safeguard if there is a breach. As you know, carrier portals continually request password changes from all of their users to ensure fraudulent access is minimized. Make sure your agency management system has password management capabilities – so when you change your password on the carrier site, you can change your password in the agency management system and retain your Real Time access.

Changing these passwords for multiple employees, carriers and other entities is cumbersome. The good news is that there is an industry movement underway to streamline these processes. The ID Federation (http://idfederation.org/) is a not-for-profit group dedicated to creating the Trust Framework to enable agencies and others to use a digital identity provided by a trusted Identity Provider to authenticate themselves with carriers and other business partners in place of passwords. Look for vendors to emerge to start to provide these digital identities to agencies in the coming year.

4 - Keep User Permissions Tightly Controlled

Unfortunately, one of the biggest password related problems we've seen across the board is that many agencies not only share their agency management system passwords among staff members, they leave the user permissions wide open. Because of the sensitivity of the data stored in the system, the only ones who should have access are those who use it day in and day out.

---

[2] "Tips for Creating a Strong Password." *Windows.* Microsoft, n.d. Web. 22 Oct. 2012. http://windows.microsoft.com/en-US/windows-vista/Tips-for-creating-a-strong-password .

Use your user permissions well. The better systems will have fairly comprehensive permission lists that are assignable by individual user. Make sure you:

- Understand the levels of permission you can set within your system.
- Understand the access that each of your team members needs to your system to perform their job optimally.
- Implement based on your agency's best practices.
- Make sure employees understand that they should not share their passwords with any other employee or person.

For example, many agency systems have permissions to dictate who can pull data in a mass fashion from your system. Take the time to understand these permissions, and who needs to have access. Do your producers need to be able to export a client list with sensitive data? Do your CSRs? If not, consider implementing this permission to restrict their ability to do so.

5 - Remember to Log Out

While it may seem simplistic, remembering to log out is one of the more important steps you can take towards keeping your data secure. As long as you are signed in, it doesn't matter how many layers of security you have or how good your password is – anyone who can get their hands on your computer or mobile device can access your data.

Most systems will have an automatic log-out feature that you can set. For example, if you are not active on a computer for 10 minutes, you will be logged out of the system. Make sure you are using this effectively. If you walk away from your office with your system left open and this auto log-out feature is not active, you essentially give the keys to your kingdom to anyone that walks in the door.

6 - Protect Outbound Data

While everything we've discussed up until this point has related to the data residing on your computer, protecting your outbound data is just as essential, if not more so. Here are a few quick tips:

- **Use Real Time** – As emphasized in the ACT article, Agency Strategies to Send & Receive Personal Data Securely, Real Time offers a much more efficient and secure method to handle transactions with carriers than email. When you send a file using Real Time, communications are automatically encrypted and kept within both the agency's and carrier's management systems.[3]

- **Secure your email with TLS (Transport Layer Security) email encryption**. ACT has published a number of articles outlining the basics of TLS encryption. Rather than duplicate these efforts, we suggest the following reading:
  - Protect Your Clients with Secure Email Using TLS
  - TLS Email Encryption--Frequently Asked Questions
  - Insurance Carriers Enabled for TLS Email Encryption for the Agencies

  TLS is the industry recommended secure email solution for business partners where there are frequent email communications going back and forth, such as between agencies and carriers. TLS is an open standard that is transparent to end users, but it requires that it be activated in the email servers of both partners.

  Most agencies are also likely to need to employ a proprietary email solution for use with

[3] Yates, Jeff. "Agency Strategies to Send & Receive Personal Data Securely." *Independent Insurance Agents & Brokers of America*. ACT, Agents Council for Technology, n.d. Web. 22 Oct. 2012.

their clients (or set up a secure client portal on the agency website), for those instances when sensitive personal data is transmitted to the client, such as that contained in the insurance policy.

- When storing/saving client emails, attach them to files within your password protected agency management system instead of saving them in the Outlook application.

7 - Use Security Software

If you are using a reputable online hosted agency management system, the data in your system should be protected with Internet and server firewall data protection, malware & anti-virus protection, as well as weekly security patch updates to Windows and Internet and server firewall data protection. You should be receiving maintenance window updates from your agency management system provider that let you know these things are being kept up-to-date. If your agency management system is housed within the agency, you should make sure similar security hardware and software are employed.

To protect data saved outside your agency management system, we also recommend that you use one antivirus program, a spyware scanner regularly, and keep your PDF reader (usually Adobe Acrobat Reader) updated and on the latest version.

While this paper will not recommend one particular vendor, below are a number of vendors that supply both a standalone anti-virus package, along with a suite of security software for your machine.

- McAfee
- Symantec
- Sophos
- AVG
- Microsoft Security Essentials

In addition, it is recommended that you update your Microsoft operating system with the latest patch levels on your machine. For more information on the latest patch levels for your operating system, visit www.microsoft.com.

8 – Be Careful when using Public Wi-Fi

While free public Wi-Fi is certainly convenient, if you don't protect yourself against data thieves and hackers, that convenience could well come at a price. Steve Anderson put it quite succinctly in his *Tech Tips* article, Free, Public Wi-Fi Can Be Dangerous to Your Health when he wrote, "You go to an airport or other hot spot and fire up your PC, hoping to find a free hot spot. You see one that calls itself "Free Wi-Fi" or a similar name. You connect. Bingo -- you've been had! The problem is that it's not really a hot spot. Instead, it's an ad hoc, peer-to-peer network…" [4]

Fortunately, there are things you can do to protect your data, yet still access the Internet while you are on the road. Here are a few suggestions:

- NEVER pick a "free" wireless network that is not identified clearly as a usable network by the provider. For example, most hotels and all *Panera* restaurants have clearly named networks and written instructions for accessing. Be careful not to use the network that advertises itself only as "FREE-WIFI!"

[4] Anderson, Steve. "Free, Public Wi-Fi Can Be Dangerous to Your Health." *Steve Anderson.com Tech Tips*. Ed. Steve Anderson. n.d. Web. 22 Oct. 2012.

- ALWAYS select the Public Network option when prompted. This uses Windows technology to make your device as undiscoverable as possible on the network. This can be hacked, but it is a critical first step.
- Read the terms and conditions that come up if prompted (e.g., at *Panera*); make sure you are familiar with the security the specific Wi-Fi network is offering, and the associated liabilities.
- Use a Virtual Private Network (VPN) when accessing your agency's system. A VPN is a relatively inexpensive way to ensure secure online access wherever you are. Three examples of providers offering VPN solutions designed to provide a secure online experience – even in a free public Wi-Fi environment include: *HotSpot Shield* (*http://www.hotspotshield.com/*); *GoTrusted* (*http://www.gotrusted.com/*) and *Witopia* (*https://www.witopia.net/*)
- Purchase and use a Wireless Internet Card. In very non-technical terms, a wireless Internet card is a small device you attach to your computer that will provide access to the Internet over a wireless carrier's cellular network. These are available, for a fee, from the major cellular providers. Many 3G and 4G smartphones can also substitute for the wireless card for a small extra fee per month, and data charges.

9 – Create a Security-Minded Agency Culture

You want to have a clear understanding throughout the agency as to the major information security risks facing your firm, grounded in a written security plan and written procedures implementing the plan that are consistently applied. It is also critical for you to have a good understanding of the information security requirements imposed by the state and federal privacy and data breach notification laws and regulations that are applicable to your agency. A common requirement of these laws, in addition to having and implementing a written security plan, is to appoint a Security Coordinator who takes ownership of the information security issue within the agency.

Most important of all, it is essential for you to train your employees so that they have a good awareness of the security risks facing the agency, or in the words of Franklin, a healthy sense of "distrust and caution." Many avoidable security breaches result directly from employee mistakes, because they are unaware of the risks. Agencies should ask their employees to commit to the requirements of the firm's agency's information security plan and procedures, and the agency should regularly audit for compliance.

ACT has created a prototype agency information security plan that agencies can use as a starting point in creating their own plan. In addition, see the Security & Privacy section of the ACT website for a wealth of additional security-related information.

Summary

Some of these tips can easily be implemented; others will take a bit more time. When it comes to file and hard drive encryption, setting up VPN security measures or TLS email encryption, and standardizing security software across your agency, we highly recommend you get your IT consultant or department involved in the planning and implementation. The important thing, however, is to start: define and outline security measures and make them a standard requirement for everyone in your office.

Note: products mentioned in the above article should not be considered product endorsements, just suggestions for where you can go to learn more.

This article was written for ACT by Kate Gluck, Director of Marketing, and Paul Fuller, EVP – Product Management, of Strategic Insurance Software (SIS). Kate and Paul can be reached at kate.gluck@sisware.com and pfuller@sisware.com. *This article reflects the views of the authors and should not be construed as an official statement by ACT.*