iianc INDEPENDENT INSURANCE AGENTS
OF NORTH CAROLINA | Trusted Choice®

10 Ways to Better Secure Your Agency Data

Target. Home Depot. Neiman Marcus. Citigroup. Gmail. Lockheed Martin. PlayStation Network. Health Net. Anthem.

What do these companies all have in common? A significant data breach that has potentially affected millions of consumers.

Data breaches have quickly become one of the most common failures in businesses today. According to IBM, studies have shown that companies are, on average, attacked over 16,000 times per year. Unfortunately, most businesses never even know they have been attacked and their data compromised. It is an alarming statistic, and the numbers are only getting more alarming as hackers and their software get smarter.

And it’s not just the large companies. According to the 2012 Data Breach Investigations Study by Verizon, 71% of the data breaches they reviewed were in a business with fewer than 100 employees!

An informed and proactive approach to data security is vital for all businesses. The IIANC Agency Management & Technology Committee has put together a guide to start you on the path of securing your agency data. While this guide is not exhaustive, we encourage you to review and implement the policies and strategies mentioned. Topics in this guide include wireless routers, employee education, physical security, mobile devices, written security plan, anti-virus/anti-malware software, backups, patches and updates, disk encryption, and passwords. Each topic is discussed and practical information and tips are included to help you better secure your agency data.

Stay cyber safe!

2014-15 IIANC Agency Management & Technology Committee

Debra Ball, CISR
Ascension Benefits & Insurance Solutions

Mathew Brauer
Hawksoft, Inc.

Tom Fisher
Insurance Service of Asheville, Inc.

Rick Heckle, AAI
Dean, Heckle & Hill, Inc.

Justin Litaker, CRM, UACIC
Litaker Insurance

Laurie Mobley
ECM Solutions

Stephanie Pichardo
Burns & Wilcox, Ltd.

George Robertson, CISR,
Rockingham Insurance Agency

Jimmie Robertson, Jr.
IGO Insurance Agency, Inc.

Mickey Robertson
Don Bullard Insurance

Crystal Temple, CISR Elite
Robinson & Stith Insurance

Ralph Whitehurst, Jr., CIC, AAI, CWCA
Whitehurst Strategic Partners

Produced by the IIANC Agency Management & Technology Committee – June 2015

1. Wireless Routers

Wireless routers can be an easy target for any potential hacker. Below is a list of items to help you secure your agency's wireless router.

- **Change Your SSID Name** - When changing the SSID name, do not change it to something like ABC Insurance; instead make it non-descriptive. Try to make it something you and your staff will remember. Selecting your agency name for the SSID lets potential hackers know this router belongs to ABC Insurance.

- **Set the Security Mode to WPA2** - At the time of this writing, this is the best security for wireless routers. Using the older WEP security mode is easier to hack.

- **Set-Up Your Pass Phrase (i.e. Password**) - It is recommended that you use upper and lower case letters as well as numbers and symbols.

- **Set Access Restrictions (if needed**) **-** For additional security, you can prevent your staff from accessing certain sites by putting in the URL under the Block Restricted Sites Section. You can also block the times individuals can gain wireless access. (i.e. You could turn off wireless access after closing. This is completed under the Restrictions Tab.)

- **Change Admin Router Password -** Make sure you do not use the same password as your pass phrase mentioned above. It is recommended that you use upper and lower case letters as well as numbers and symbols. (This is completed under the Administrative Tab).

2. Employee Education

Every office should establish guidelines on how Personal Identifiable Information (PII) or Private Healthcare Information (PHI) is to be collected, transmitted and stored within the organization. Make sure staff members are vigilant when it comes to opening email from an unknown source. With the rise in phishing attacks, staff members need to be careful when opening email. If the email is from an unknown source, do not open it. If an email asks your staff member to click on a link, verify the link is genuine before making the selection. Clicking on the wrong email or link can potentially open your network to viruses and malware.

3. Physical Security

One of the first areas of defense is building security. Make sure you have a list of all access keys and which employees have a key. Install a security system and only give out the security code to those employees with a need to know. If someone leaves your office, make sure you retrieve their key and change the security code. Also, installing security cameras can help to ward off any would be thieves that might want to break into your building. When leaving your office for lunch, appointments or for the day, make sure you lock the door to your office and place all client data in a locked area.

4. Mobile Devices

Mobile devices now have the ability to contain pictures, video, voice recordings and documents. Any staff member that has a company mobile device should have a password and a two-tiered password if possible. Remote-wipe capability is also a good idea just in case the device is stolen or lost. This will allow the agency to send a code to the device and delete the information on the mobile device.

5. Written Security Plan

With the new requirements under the HIPAA/HITECH acts, any agency that is working with PHI should have a written security plan. This plan should encompass physical, administrative and technical security issues within the agency. Even before creating your written security plan, each business should evaluate the collection, transmission, and storage of PII & PHI. Security plans should be updated at least on an annual basis. Some states even require agencies to have a written plan.

6. AntiVirus/Anti-Malware

AntiVirus/AntiMalware security software should be installed on all workstations. As with most software there are dozens of vendors to choose from. Norton/Symantec, McAfee, Avast, TrendMicro and Sophos and are some of the big players. There are some 'free' options out there but often times their licensing model limits the free versions from being used in a corporate environment.

A non-exhaustive list is maintained at this Wikipedia page:
http://en.wikipedia.org/wiki/Comparison_of_antivirus_software

More so than with all other software, it is imperative that antivirus software is kept up to date. AV companies often update their software (definitions) multiple times a day to keep up with the ever changing threat landscape.

7. Backup

Everything we do for our own clients in the insurance industry is about mitigating risk. When looking at how to best secure our own agency's data, we need to do the same thing. A well planned and implemented backup strategy is in essence an insurance policy. In the event of a disaster (be it physical or digital), a good backup plan will indemnify your valuable data. A good backup best practice is to follow the 3-2-1 Rule:

- Have at least **3** copies of your data. One copy is the 'live' data, so you want to have that and at least two more copies.
- Have the data in at least **2** different formats (disk, cloud, tape, etc.). Doing so reduces the chance that your backup becomes damaged or doesn't run properly.
- Have at least **1** copy of the data off site; that is, not in the same physical location as the other backup. The further away these copies are from one another, the better. This reduces the chance of loss in the case of theft or disaster, such as a fire or flood.

8. Patches and Updates

New threats are being created and introduced into the world every hour of every day. Exploitive malware and viruses often infiltrate a system by taking advantage of flaws in various software. The more popular and widespread the software – the more likely it is to have exploited flaws. Windows, Internet Explorer, Adobe Flash, Java and Adobe Reader are some of the most exploited products out there for one simple reason – they're the most commonly used. It is crucial to keep these products updated and patched and most offer a way to automate the process so you don't even have to think about it.

9. Disk Encryption

Apply encryption to all portable drives (USB sticks, portables, etc.) and laptop/portable computers. Encrypting a drive or computer that could easily be lost or stolen ensures that the data on that device isn't readable by an unauthorized person without a special key or password. There are multiple tools available for accomplishing this, including BitLocker which is included with some versions of the Windows operating system. A good list of these tools is maintained in this Wikipedia article:
http://http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

10. Passwords

If there is one single thing any organization can do to better safeguard their data, it is to follow good password hygiene.

- **Use strong passwords/passphrases**. Security research has taught us that the top passwords used year after year are "password", "123456", "monkey" and "welcome". Choose or generate a strong password that isn't in the dictionary and make sure it contains some symbols and numeric characters.

- **Enable two factor authentication where possible.** Two factor authentication (2FA) or two step verification, or multi factor authentication is an extra layer of security that requires two pieces to authenticate. Normally this is something 'known' (like a password) and involves something the user 'has' (like a FOB or cellphone). Normally, one step is your typical password but then also a 2nd piece of information (normally a short PIN) is required. These PINs can be generated on mobile devices via an app, sms/text message or perhaps on a special key FOB. 2FA isn't available everywhere but more and more vendors are making it available to their customers.

- **Do not reuse passwords or use the same password on multiple sites.** The majority of people have between one and a few passwords or password variations they use for every website they visit. This is convenient, yet dangerous. Let's say your favorite online retailer has a security breach. Your email address and password used on that site are now potentially in the wrong hands. Should you be using that email address and password at multiple other sites (say your bank) those credentials too are now in the wrong hands. Using a complex and unique password for each and every site you visit would eliminate this threat. This sounds difficult but really isn't when you implement a password manager properly (see next point).

- **Use a password manager.** Most of the above password practices are almost impossible to follow without the use of a password manager. A password manager is an application (usually a plugin to your web browser and/or mobile app) that assists in storing, organizing and generating passwords. Not only does a good password manager remember all of your passwords but it can be used to save the links/bookmarks to the sites you visit, as well as automatically fill in your email address/user name/passwords and other ‘form’ information like credit card numbers, addresses, and the like. There are a number of different solutions out there but the big names at the moment are: LastPass, Dashlane, KeePass, 1Password and RoboForm. All of these have accompanying mobile apps so even when you’re away from your regular office/home computers you’ll always have access to your passwords and other site data.