Mobile Technology and Your Business SECURITY

by Rob Keene
Chief Operating Officer
Starmount Life Insurance and AlwaysCare Benefits

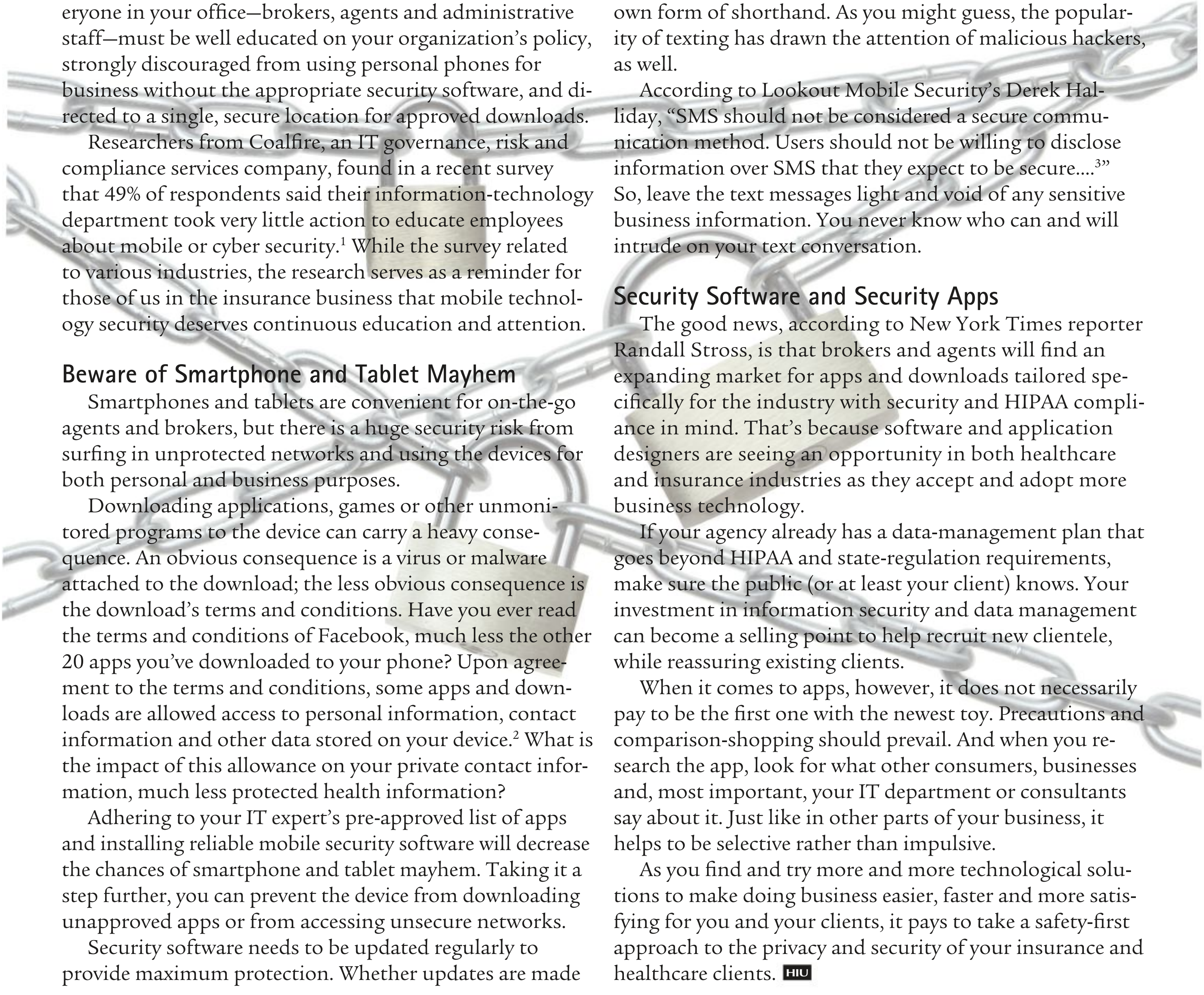
As the insurance industry pushes utilization of modern technology to enhance business, we need a brief overview of why security is a critical and ongoing issue. Here is a back-to-basics explanation of threats for mobile devices that identifies with firms of all sizes.

Smartphones, Tablets, Apps and Security

Advances in communication technology, particularly mobile devices, have boosted efficiencies for many businesses and industries, including the health insurance industry. Smartphones, tablets and various apps can assist an agent or broker in delivering impeccable service to clients with speed and accuracy. However, we must remind ourselves that, with great power, comes great responsibility—in this case, diligence in sustaining the security of client information.

We often think of information security as our defense against hackers and Internet assailants. But as your IT department or vendor will tell you, you have to have a great offense when it comes to cyber security and protected health information. For this reason, it is imperative to stay ahead of the game and go beyond HIPAA's policy and guidelines, such as password protection, data encryption, limited amount of stored messages, and data wipeout capabilities if a device is lost or stolen.

It is also important to establish controls either through your IT policy or automated enforcement of approved applications for your devices. Just because an app is offered in the App or Play Store doesn't mean it is secure. Certain file exchanges, for example, may help you do unsecure things unwittingly, such as upload to data storage services that may not adhere to HIPAA's rules. On the other hand, there are secure apps on the market.



Data-Management Policy and Employee Awareness

HIPAA regulations mandate that organizations and businesses incorporate smartphones, tablets or any device containing protected health information into their data management policy. Your IT team or consultant can control or manipulate devices' capabilities for HIPAA compliance. However, a well-designed data-management plan is not enough to ensure strict following of the guidelines. Everyone in your office—brokers, agents and administrative staff—must be well educated on your organization's policy, strongly discouraged from using personal phones for business without the appropriate security software, and directed to a single, secure location for approved downloads.

Researchers from Coalfire, an IT governance, risk and compliance services company, found in a recent survey that 49% of respondents said their information-technology department took very little action to educate employees about mobile or cyber security.[1] While the survey related to various industries, the research serves as a reminder for those of us in the insurance business that mobile technology security deserves continuous education and attention.

Beware of Smartphone and Tablet Mayhem

Smartphones and tablets are convenient for on-the-go agents and brokers, but there is a huge security risk from surfing in unprotected networks and using the devices for both personal and business purposes.

Downloading applications, games or other unmonitored programs to the device can carry a heavy consequence. An obvious consequence is a virus or malware attached to the download; the less obvious consequence is the download's terms and conditions. Have you ever read the terms and conditions of Facebook, much less the other 20 apps you've downloaded to your phone? Upon agreement to the terms and conditions, some apps and downloads are allowed access to personal information, contact information and other data stored on your device.[2] What is the impact of this allowance on your private contact information, much less protected health information?

Adhering to your IT expert's pre-approved list of apps and installing reliable mobile security software will decrease the chances of smartphone and tablet mayhem. Taking it a step further, you can prevent the device from downloading unapproved apps or from accessing unsecure networks.

Security software needs to be updated regularly to provide maximum protection. Whether updates are made manually through a PC or automatically, take the opportunity to remind yourself and your team that this is a critical step for your business, not just for your sake, but for your clients as well.

There Is No Such Thing as a Secure Text

Short message service (SMS) text messaging remains one of the most popular forms of quick communications between professionals and the public. Texting even has its own form of shorthand. As you might guess, the popularity of texting has drawn the attention of malicious hackers, as well.

According to Lookout Mobile Security's Derek Halliday, "SMS should not be considered a secure communication method. Users should not be willing to disclose information over SMS that they expect to be secure....[3]" So, leave the text messages light and void of any sensitive business information. You never know who can and will intrude on your text conversation.

Security Software and Security Apps

The good news, according to New York Times reporter Randall Stross, is that brokers and agents will find an expanding market for apps and downloads tailored specifically for the industry with security and HIPAA compliance in mind. That's because software and application designers are seeing an opportunity in both healthcare and insurance industries as they accept and adopt more business technology.

If your agency already has a data-management plan that goes beyond HIPAA and state-regulation requirements, make sure the public (or at least your client) knows. Your investment in information security and data management can become a selling point to help recruit new clientele, while reassuring existing clients.

When it comes to apps, however, it does not necessarily pay to be the first one with the newest toy. Precautions and comparison-shopping should prevail. And when you research the app, look for what other consumers, businesses and, most important, your IT department or consultants say about it. Just like in other parts of your business, it helps to be selective rather than impulsive.

As you find and try more and more technological solutions to make doing business easier, faster and more satisfying for you and your clients, it pays to take a safety-first approach to the privacy and security of your insurance and healthcare clients. HIU

[1] Meilach, David (August 17, 2012). "Using Your Smartphone for Work? You're Taking a Big Risk." BusinessNews Daily.

[2] Mobile Security Software Review (2012). TopTen REVIEWS. 08/27/2012.

[3] Mello, John P. (2012). "Spotlight on Security: Don't Trust that Text." Tech News World.