Information Security Strategies for Healthcare: Part II

Noam H. Artz, PhD

As a consultant, staying in touch is one of the most important elements of a successful business. And boy, do I have lots of ways to stay in touch. I travel with a mid-size laptop weighing four pounds, complete with a wireless Internet service that almost always succeeds in connecting, no matter what obscure city I happen to be visiting (and it works great on the train, too). For those moments when I am literally on the run, my Palm-based PDA provides IMAP e-mail and instant messaging to clients that are especially useful in airports (and, I hate to admit, at red lights, too). I have an alphanumeric pager that can accept e-mail messages (I always feel odd when the thing starts vibrating while landing at an airport) and a cell phone with nationwide roaming and walkie-talkie.

You must think I'm insane for carrying so many devices. For me, it's a question of redundancy (any one of these can fail at any moment) and spreading out the most valuable commodity of all—battery life! But it's all worth it when I am asked a question while sitting with a client and find the answer by the end of the meeting by e-mailing a colleague or surfing the Web.

Defining the Agenda

In my first column (Summer 2003 *JHIM*), I identified a set of important information security realities for healthcare IT leaders. They were: security starts with principles and policies; continue your move to the Web; keep your basic infrastructure healthy; if you're not already doing so, start worrying about portable devices and the three A's—authentication, authorization and accounting.

Last time, I talked about basic infrastructure. Today's topic, as evidenced from the above anecdote, is portable computing.

Laying the Groundwork

Consider the following facts:

- A recent study in Pediatrics concluded that at least a third of the pediatricians surveyed used PDAs in their clinical practice. This trend will only likely increase as health plans and facilities increase the availability of handheld applications, often at little or no cost.
- Wireless networking, while not quite ubiquitous, is proliferating as well. And there is a flavor for every need: LAN-based Wi-Fi for use within organizations; public Wi-Fi "hotspots" that support roaming across many metropolitan areas; and wireless Internet services that, while slower in speed, offer improving performance at reasonable cost wherever most cell phones work.
- Notebook computers finally have operating systems that exploit their features while offering more stability that ever before.
- Portable computing has the potential to bring much-needed efficiency to the healthcare enterprise, as well as significant risk if not managed properly.

> *"Portable computing has the potential to bring much-needed efficiency to the healthcare enterprise, as well as significant risk if not managed properly."*

You Have to Take the Good...

In many ways, the Web has simplified the delivery of even complex applications to users. But the increase in mobility offered by portable computing will go even further to bring more applications to more people more of the time.

Within the context of the healthcare enterprise, portable computing goes beyond support for traveling users. It enables state-of-the art applications to be delivered anywhere a user needs them to help improve delivery of care, reduce the potential for medical errors and control administrative cost. In the academic medical center, mobile computing increases flexibility and enables staff to bridge clinical and research roles more readily by spending less time readjusting to different locations that often come with different roles.

Mobile computing is more flexible computing, less constrained by the idiosyncrasies of floor plans and wiring schemes. It yields a more flexible staff. A more computer-literate workforce improves the prospects of both the individuals and the enterprise for personal and institutional development.

...With the Bad

These added benefits are not without additional cost and risk. Portable platforms can be more fragile than desktop systems subject to more physical abuse and failure. Portable platforms are subject to loss or inappropriate access in ways that many desktop systems are not, although computers located in high traffic areas in clinical facilities also are subject to potentially inappropriate access and need to be secured accordingly. Wireless networks, if not properly configured, can expose the user to inappropriate access to information as well as expose the organization to theft of service.

On the social engineering side, does greater mobility, better network access and more connectivity bring with it an expectation that workers stay more connected, more of the time? Already many Internet users feel there is an expectation of immediate response to e-mail, no matter what time of day or night. The healthcare enterprise is a round-the-clock operation, but are the lines between work life and home life finally blurred beyond recognition?

Looking Ahead

So what can we do to make use of this emerging opportunity without sacrificing our peace of mind? Here are some tips:

- As usual, it starts with good policy. Be sure users know that they are responsible for protecting portable devices, especially from loss or inappropriate access. Insist that passwords be used for all laptops and PDAs. Provide methods for users to easily backup portable devices and educate them on the risks of not doing so. Without taking these steps, data can be quite vulnerable. Remember the State Department laptops that were stolen with sensitive information on board? Think of how easy it is to leave a laptop or PDA at an airport security checkpoint while dashing for a late flight (you would be shocked to learn how many people do just that!).
- Understand your infrastructure and take nothing for granted. Ensure that encryption is in place when needed. Offer virtual private network support for remote users and locations. Final migration to more mature versions of Windows (such as Win2000 and XP) makes the client side of virtual private network configuration much easier than before. Plenty of server solutions are available that interoperate well with desktop software. SSL is the *de facto* standard for encrypted communications and is becoming more widely relied upon in SOAP and Web services-enabled applications. Some compromises will be necessary, but that does not mean that it's impossible to ensure some degree of confidence that information assets will be protected. Recognize that you cannot have the same level of control over portable devices as you might over fixed-location devices.
- Know your users. Policies are created to be circumvented; infrastructure can also be befuddled. Study how your users work in their various settings and make policy, infrastructure and work process support each other rather than conflict with one another. Some of your users may be comfortable as "road warriors," but many others simply want to be able to get their work done with as few superfluous moving parts as possible. The appropriate strategy may not be a one-size-fits-all solution. Profile different user types, determine commonalities and differences and craft as many distinct solutions as you can afford and support.

Next issue: AAA (authentication, authorization and accounting).

About the Author

Noam H. Arzt, PhD, is the president and founder of HLN Consulting, LLC, San Diego, CA. He can be reached at arzt@hln.com.