TECHNOLOGY

Information Security Strategies for Healthcare: Part I

Noam H. Arzt, PhD

It's been an interesting week. First, wildfires raged through San Diego County, obliterating houses and foliage. More than 350 homes were destroyed in a neighborhood not 15 miles from where I live. Needless to say, my car was packed and pointed out of my garage as I wondered what critical items I needed to pack to ensure that both my business and family life could continue. This wake-up call made clear to me the tenuousness of my personal and professional infrastructures.

Two days later, the building that houses my company's East Coast offices was hit by a late-day power outage—a pervasive one that cut off all of our servers from the Internet and stranded a number of our remote developers without access to e-mail and shared resources. As a small company, we have not yet implemented redundant services, although these plans are on the drawing board, and we have taken initial steps toward preparing ourselves for this eventuality.

Defining the Agenda

In my last column (Summer 2003), 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.
- In the end, it's all about AAA (authentication, authorization and accounting).

In each of the next three columns, I'm going to select one of these important issues and provide some insight into managing it. Today's issue, as exemplified by my introductory anecdotes, is basic infrastructure.

> *"If an environment is too homogeneous, it puts the institution at risk of becoming too dependent on one (or a small number) of vendors."*

Can Environments Be Too Homogeneous?

Almost none of our institutions are homogeneous when it comes to their computing environments. A number of factors account for this:

- Our IT infrastructures have grown up over time, with replacement cycles often extending for years, even for key components.
- Some of us choose best-of-breed strategies that recognize the importance of unique or specialized functional requirements over the compromises often required by more comprehensive solutions.
- Changes in our leadership—perhaps occurring more often than we'd like—provide frequent opportunities for course changes and realignments.

While these may seem like liabilities, perhaps these factors are really blessings in disguise. If an environment is too homogeneous, it puts the institution at risk of becoming too dependent on one (or a small number) of vendors. Could anyone have predicted the ups and downs of IBM during the past 10 years? The demise of Digital Equipment Corporation? The eclipse of Novell and Apple? A more heterogeneous computing environment enables us to distribute that risk over a number of products and players as long as we have the capability to make compatible choices.

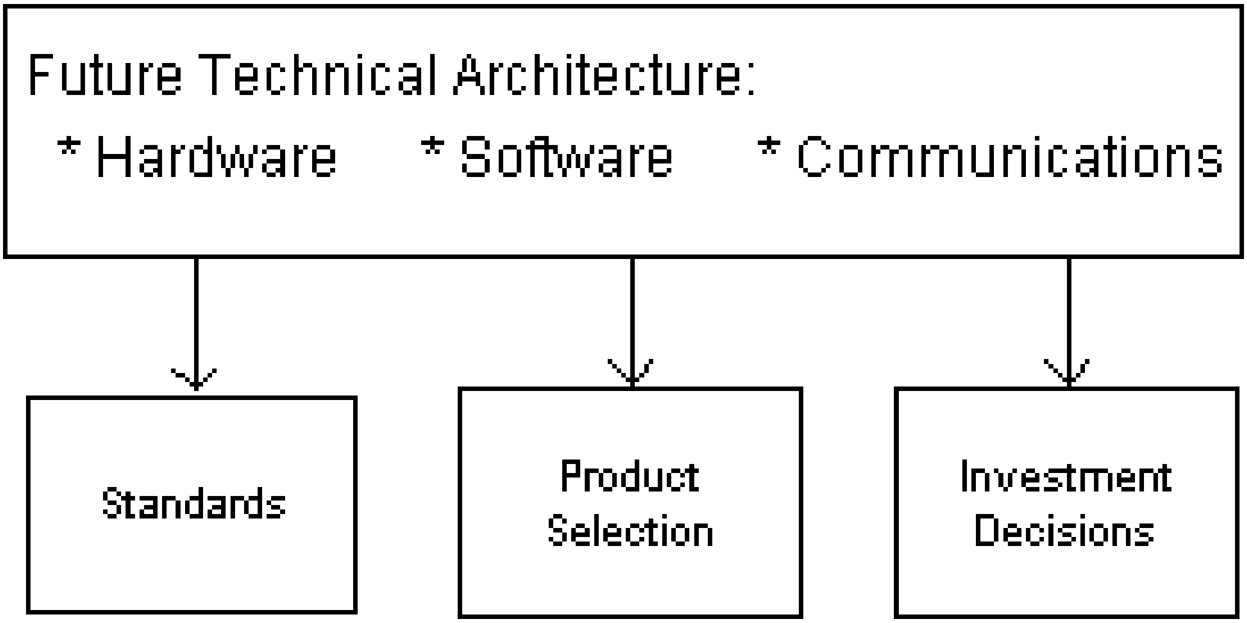
It Comes Down to Architecture

Defining a stable technical architecture is the key to effectively managing a more heterogeneous environment. Architecture is more than simply adherence to standards. A technical architecture has a number of key components:

- ***Requirements.*** A clear set of business requirements must be identified and ratified.
- ***Principles.*** These organizational core values about IT should be articulated in business terms and vetted with the organization's senior management.
- ***Documentation.*** The organization must understand and document its current architecture if it is to be able to plot a new course to something different or better.
- ***Trends.*** Some investment must be made in identifying and researching emerging technology trends and opportunities and then determining their relevance to new architectural alternatives.

A technical architecture is the process for developing a blueprint for making choices about hardware, software and communications procure-

Figure 1. Technical Architecture



ments for an organization. From it flows standards, specific purchase recommendations and other investment decisions regarding technology and its use in the organization. The crucial objective is to improve the performance of the organization. (See Figure 1.)

A technical architecture is not a platform from which to preach a certain methodology or justify a predetermined technical direction. It is also not technical mumbo-jumbo: it must speak to business people as well as to technical people.

Strike a Balance

Before you wonder whether I am off my rocker for lauding heterogeneity as a strategic imperative, understand that I do recognize that when it comes to system integration, there is no question it will be more expensive—and more risky—to integrate a set of "best-of-breed" technologies than a set of products that were designed to work together. This is as true of basic infrastructure components as it is of applications. A strong, well thought out technical architecture will provide the framework for making these choices properly.

Back To Fires and Power Outages

Security solutions are as susceptible to poor planning as anything else. It is even more important that the definition of a security architecture be done properly within a framework such as the one described above. The tension between homogeneous components and the threat of vendor lock-in suggests the use of a standards-based approach that will recognize and help manage the tradeoff between seamless integration and "the security tail wagging the functional dog." HIPAA and a growing set of additional state privacy laws will require that even more rigor be added to these strategies.

A properly executed security architecture—one that is revisited periodically to account for changes in the technical, organizational and regulatory environment—will help ensure that your wild fires and power outages don't catch you by surprise.

Next Issue: Portable Computing

About the Author

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