Rising to the Challenge: Strategies for the New Healthcare Enterprise

Noam H. Arzt, PhD

Ah, security — it has become the new mantra of the IT world. In the past, information security was mostly a game of risk and insurance: you determined what your level of risk was based on a threat analysis and judged how likely and how damaging the threats might be if they occurred. You then developed mitigating strategies and decided if the cost of mitigation was warranted based on the perceived risk of taking no action. Networks were by and large private, technologies less varied. Public awareness of the risks was much lower. "Security by obscurity" often ruled the day.

Today, the stakes are considerably higher, and the environment is considerably more complex. I had the privilege of working at a major research university when the Internet was born. Back then we had a pervasive campus-wide network; albeit the interface for most users was terminal-based and not Ethernet, yet the hospital remained apart and disconnected. We worried about security then, too, but our focus was almost exclusively on protecting our host-based systems. Research universities operate on open networks and free exchange, so the advent of the Internet brought all kinds of new challenges to this environment.

A survey completed last year by the Medical Records Institute identified access to patient records by unauthorized users as topping the list of major privacy and security concerns (respondents worked in a wide variety of clinical settings from solo practices to hospitals). In 2001, 59 percent of respondents identified unauthorized access as a major concern; by the following year's survey, it had crept up above 62 percent. When asked about concerns regarding inappropriate access from within the institution, that percentage jumped from 55 percent in 2001 to over 65 percent in 2002. Nearly half were concerned about violations of data security practices in 2001, with that rising to nearly 58 percent of respondents expressing this concern a year later.[1]

Can information technology organizations rise to these challenges?

"'Security by obscurity' often ruled by the day."

Managing Tradeoffs

Maintaining security has always been about managing ongoing tensions, not just solving immediate problems. Information security requirements force important tradeoffs to be considered:

- ***Ease of use:*** Users often feel security implementations interfere with their ability to do their jobs effectively. Password challenges can be annoying (especially when they constantly change or require multiple steps); role-based security that enforces "need to know" does not always meet users' perceptions of what they need to get the job done.
- ***Location:*** Many hospitals strive to create a clinical workstation that can serve as a platform for any authorized user to log into clinical systems. Still, specific applications often cannot be accessed from certain locations. Remote access to information from satellite clinics or facilities, or from home, is sometimes impossible or prohibited.
- ***Cost:*** Security can be expensive, and often the components are buried so low in the infrastructure that it is hard for management to see (let alone understand) what it is paying for. But all it takes is one disaster for many institutions to open the checkbook.

Hospitals, too, face new challenges as the healthcare environment changes:

- ***Organizational flux:*** I lived in Philadelphia for almost 25 years. I don't think anyone could have anticipated the constant churn of organizational purchase, divestiture, merger, and acquisition that has taken place over the past few years. Yet as organizational affiliation changes, so do the requirements for technical infrastructure and the security implications that follow from that.
- ***Consumerism:*** The Internet has made many of us information junkies, and good-quality healthcare information is widely sought. Americans continue to be fed up with the healthcare system writ large, and many now use the Internet aggressively to "shop" for information and services. Institutions have to consciously decide to enter the fray or stay on the sidelines.
- ***New services:*** Our infrastructure has gone from no networks, to private networks, and now to the Internet. Some hospitals offer patients and their families the ability to surf the web as a convenience. Shortly, this kind of service may be a strategic necessity in an ever-competitive market. Wireless services are no doubt close behind.
- ***Funding:*** Technology competes for funding with many other capital and operational priorities. As the technology sector of the economy weakens, corporate sponsors will

likely become less reliable for significant donations or partnerships. As expansion continues nonetheless for some organizations, appropriate funding for technology is often squeezed out of the plan in an attempt to streamline or reduce the budget.

- ***Technology transfer and intellectual property:*** Advances in biomedical research have pushed issues of intellectual property ownership and appropriately controlled technology transfer to the foreground at many institutions. Yet their handling of this volatile topic varies greatly, with significant repercussions to both individual clinician-researchers and their institutions. Increasing digitization of research material, coupled with changes in international copyright law, place added pressure on institutions to focus their limited resources in this area.
- ***HIPAA (could an article on security not mention it?):*** HIPAA has crystallized the focus of information security efforts by requiring a new level of compliance and documentation than had previously been required. The essential elements of the regulations, though, are already embedded in industry best practice (and in some cases in pre-existing state or local legislation, which is often more stringent). But an increase in this general awareness by senior management can only be a good thing as protection of information assets will perhaps now rival protection of other more physical assets.

An additional set of technical challenges face us as well:

- ***Getting tangled in the web:*** Healthcare organizations continue to struggle with appropriate use of the web both inside and outside their institutions. Web technology is very suited to the distributed nature of hospitals, yet corporate interests often fight to rein in this electronic entrepreneurship in the name of web site coherence and control of content. The challenges are to keep website content fresh, unified, and appropriate as the marketplace's standard for visual presentation continues to get more and more sophisticated.

While hospitals are not compelled to comply with the Americans with Disabilities Act presentation standards, this will become increasingly important as their web sites attempt to appeal to wider audiences for marketing and educational purposes. Developing an effective e-business strategy also continues to be an active (and controversial) topic.

"As devices get smaller, more powerful, and more pervasive, will IT be able to protect the sensitive data stored on them?"

- ***Increased mobility with decreased attention span:*** Our users expect an ever increasing amount of mobility provided not only through wireless support (within the institution's borders and in the outside world as well), but through access to systems and information from fixed locations anywhere. The web has certainly helped to provide this ubiquity. Portable computing and wireless networks have fueled this mobility as well. But this new mobility has come with a price: the pressure of "constant connectedness" has reduced our attention span as we juggle pagers, PDAs, cell phones, laptops, and our commitments. As devices get smaller, more powerful, and more pervasive, will IT be able to protect the sensitive data stored on them?
- ***Hazy outlook on clinical systems:*** Most medical centers in the United States have made little progress toward the vision of an integrated electronic patient system or electronic medical record (EMR). Often, the needs of inpatient and ambulatory care units do not coincide closely enough to make an integrated system easy to deploy. Yet system planning and deployment continue, with HIPAA implications looming as a more substantial (and costly) compliance activity than even Y2K.
- ***E-whatever:*** The move towards implementing application integration using web technologies and protocols is unstoppable. Out-of-the-box encryption services are compelling. Easy passes through firewalls ("yours" and "theirs") even more so. Yet just as HL7 messages require trading partner agreement as to the rules of engagement, e-exchange has not yet adequately solved all the problems of authentication and authorization, syntax, and vocabulary. There are still many choices available (EJBs, .net, web services), so options need to be carefully considered.

Defining an Agenda

OK, now what? How do IT managers maintain their sanity (and their organization's integrity) in an environment of increasing change and uncertainty, this "permanent whitewater"? My advice — stick to the basics:

- ***Security starts with principles and policies.*** They form the foundation of your organization's philosophy and beliefs in this area. They should be guided by top management and intelligible to top management. If your CEO cannot explain the basic philosophy concisely, and understand the more detailed written policies, you're not ready to move on.
- ***Continue your move to the Web.*** Sure, application functionality may not be quite as rich as it is on desktop applications, but the ability to provide a secure computing environment accessible from anywhere inside and outside of your organization is compelling. Your ability to support applications with

an increasingly distributed user base and a shrinking budget will be enabled by this strategy.

- ***Keep your basic infrastructure healthy.*** Your servers, desktops, and network infrastructure must be kept up-to-date and secure. This is relentless, thankless work. It requires constant vigilance and attentiveness. This is increasingly becoming a product and services market of niche players on the one hand, and a continuing consolidation of the bigger players on the other.
- ***If you're not already doing so, start worrying about portable devices.*** It's amazing what someone can fit on a laptop (or PDA) these days. And it's amazing what the average home PC can do with a broadband connection as well. Be open-minded about how to leverage the convenience of these devices, but establish clear guidelines for their appropriate use.
- ***In the end, it's all about AAA.*** That's authentication, authorization, and accounting. Whether you have an online application, an automated transaction, or an identity card reader, the continuing proliferation of systems and devices will demand some coherence in user authentication and authorization standards and implementation. IPv6 will only make this worse once it is deployed as more and more devices appear on the Internet and offer services or access to information. For some time to come, these tools will continue to work against each other rather than together, but you must continue to track their development and the compatibility of your existing products to any apparent winners.

"Your servers, desktops, and network infrastructure must be kept up-to-date and secure. This is relentless, thankless work."

So keep plugging away… You need to have someone in your organization continue to monitor new threats, products, and solutions. Be sure your HIPAA compliance officer is in the loop. And keep stressing to senior management that information security issues are as important a part of institutional asset protection as any physical asset.

About the Author

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

References

[1]Annual Medical Records Institute Survey of Electronic Health Record Trends and Usage, 2001 and 2002. See http://www.medrecinst.com.