OPINIONS

Security: Big Brother Really Could Be Watching

In September, PharmaVOICE's feature article, Biometrics — Beyond Passwords, examined the potential use of biological markers, such as fingerprints and iris scans, in the pharmaceutical industry to ensure security. The Computer Crime and Security Survey, conducted by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, paints a compelling portrait of just how often crime occurs on computer networks and just how expensive such crime can be. Even organizations that have deployed a wide range of security technologies can fall victim to significant losses. Furthermore, the percentage of these incidents that are reported to law enforcement agencies remains low. So attackers may reasonably infer that the odds against their being caught and prosecuted remain strongly in their favor. According to the CSI/FBI 2003 survey, respondents were asked what kind of security technologies they had employed to protect their organizations. Virtually all organizations use antivirus software (99%) and firewalls (98%). Most (91%) employ some kind of physical security to protect their computer and information assets and most employ some measure of access control (92%).

PharmaVOICE asked: Do the benefits of increased security outweigh the abdication of such personal information?

Treat passwords with respect

Adding biometrics to the current password system is mainly an attempt to cope with users' lack of care in securing their passwords. They either select an obvious password and never change it, or, when forced to use a computer generated one, write it on a slip of paper taped to the screen.

If users just treated their passwords with as much care as they do the keys to their car, the need for biometrics would be generally eliminated in all but the most secure systems.

Personally, I would be hesitant to allow my fingerprint to be the "password" to a system to which criminals really wanted access, since they would not need me to get in, just my finger. And, if the system is less valuable than that, why go to such lengths?

Stephen Ruger
Project Manager

Differentiating between security and privacy

When assessing the value of increased security relative to decreased privacy, one must consider their separate definitions. Privacy is generally defined as the use and abuse of authorized information access. Security is defined as controlling and preventing unauthorized access to authorized information.

The inability to see security and privacy as two separate issues will further delay the adoption and implementation of technologies that will ultimately contribute to a safer environment. For example, two recent Homeland Security initiatives have been stymied by public outcry and lobbying: The Computer Aided Passenger Profiling and Screening system and Total Information Awareness initiatives. These systems were to be used to collect and analyze U.S. citizens' personal information and when combined with planned biometric border security initiatives purportedly would help better maintain our borders against the increased threat of terrorism. Public outcry over the perceived loss of privacy forced our government to reconsider these activities.

Many consumers openly express their desire for enhanced privacy practices but continue to engage in activities that freely divulge their personal information. Whether making telephone calls on their cellular phone, traversing the Web from their local Starbucks or repeatedly using their favorite credit card, these activities are being monitored, documented, and mined for information. When you last visited your local grocery store did you refrain from using your preferred-shopper card because of the loss of privacy (some of the largest databases of consumer purchasing practices and patterns are maintained by grocery retailers) or did you swipe the card to take advantage of the discounted grocery items? Most consumers are aware of these practices but continue to divulge their personal information to obtain some tangible benefit.

The collection and use of personal information should be afforded to the appropriate organizations in order to provide for the safety and security of others. Similar to my grocery shopping experience I would gladly trade some personal privacy, provided that the information was appropriately secured, in return for the tangible benefit of increased physical safety and security. The public perception that the adoption of certain security and biometric technologies is inextricably tied to a loss of consumer privacy will further delay the adoption of stronger security practices and may lead to a situation where, similar to 9/11, we are unprepared to react appropriately to external threats.

Craig Cuyar, Ph.D.
Senior VP, Chief Information Officer
CommonHealth

For the sake of self-preservation

We must embrace biometrics and other heightened security measures for the sake of self-preservation. The endless plague of terrorism is the most compelling reason. The insurrection will seek to use our strengths against us through agriterror, bioterror, and cyberterror targeting the computer systems that control every aspect of our existence (for example, electricity and natural gas).

"We should regard cyberterrorism as a weapon of mass destruction," according to William Pelgrin, chairman of the Multistate Information Sharing and Analysis Center (MS-ISAC). "In this environment, hackable passwords are no longer an adequate defense."

In addition, biometrics offer freedom from memorizing myriad passwords, or defeating their purpose through cheat sheets.

But even biometrics are undoubtedly penetrable. Security is a never-ending arms race that may require combinatorial applications using multiple layers of conventional and innovative safeguards. But we must not let Orwellian paranoia leave us vulnerable to the real threats we face. President Clinton recently said had his administration had access to private sector data mining technology, 9/11 could have been prevented. When the Bush Administration attempted to implement that technology, civil libertarians sabotaged the effort in a misguided attempt to protect our privacy. Such folly will leave us with the ultimate privacy, that of the grave, at the hands of our real enemies. Let us not make Osama Bin Laden prophetic when he says, "Our enemies are our fools."

Terry Nugent
VP, Marketing
Medical Marketing Service Inc. (MMS)

Benefits beyond security

People are so leery of spam, credit card fraud, and identity theft that we're seeing the "security sword" cutting both ways: provide more personal data to identify yourself, but use all means possible to protect it from misuse. The benefits must go beyond security to offer more innovations in customer service and customized offerings. Yet even in developing personalized medicines, a recent survey said most people would be afraid to provide a DNA sample for fear it would be misused. The old fear of tradeoffs appear to working against innovation.

Mark Stinson
President
Brand Innovation Inc.

Personal choice

The question of whether the benefits of increased security outweigh the abdication of personal information can't be answered generally. Personal information requires personal choice: is the value of extra security worth surrendering my information? For corporate security initiatives, the value exchange issue remains the same: is the value of extra security for my employer (or perhaps my job itself) worth surrendering my information? Therefore, the impact on employees and their commitment to their employer are crucial issues to consider when requiring personal information for security purposes. From a purely economic perspective, employers who require personal information will need to provide greater pay or benefits to compensate employees for their information.

Paul Buta
Chief Operating Officer
Optas Inc.

A changing world

I used to be opposed to security measures that were invasive to people's privacy. But I am now in favor of such methods in the workplace and in sensitive government or security areas. The world has changed. With identity theft, hackers, viruses, and terrorists, there has to be some measure of control to thwart these behaviors. Unfortunately, sometimes a worker's letter to mom gets caught up in this, but I think the public good is better served by tougher security methods.

Norma-Jeanne Hennis, M.S.
President
MedPharm Communications LLC

Increased security isn't working

I believe we are no longer a democracy. Streets, buildings, supermarkets, and shopping centers are lined with cameras, and we are constantly being watched.

It is the innocent whose rights are being violated. The right to privacy as stated in our constitution is completely obliterated, yet the perpetrators appear to benefit. From what I've observed, increased security hasn't worked. Technology is much more astute but the laws have not kept up with what is being offered today.

We still get attacked by computer hackers who have no lives and who go unpunished for their crimes. No matter how advanced technology becomes, we are always going to have those who are going to break the code, more than likely disgruntled employees who design the security technology in the first place.

Chris Conley
VP, Medical Affairs Division
Steffin Kutzman & Associates

Protection not abdication

At the end of the day all this is being done to protect the confidential information, which only the employees of a company should have access to.

Since the Internet has become such an important communication channel, it needs to be protected and kept secure. I support Internet security measures over abdication of personal information.

Ajit Baid
Consulting Manager
Healthcare & Lifesciences
Frost & Sullivan

Definitely in favor

Give me the security deal anytime ... they can get to personal info at anytime.

David M. McCarty
Koehler & McCarty

No simple answer

There is no simple answer or solution to this ever growing issue. While we are a nation founded on the principles of law and respect for individual freedoms, the world's landscape has changed significantly since our founding fathers. Whether we are discussing patient or personal privacy issues, we must weigh the security factor as never before. Do you even remember walking onto airplanes without a security check? Is this an invasion of privacy, or do we accept that as the "norm?"

To what extent, then, are we willing to sacrifice some freedom of movement to ensure we are more secure on that airplane? This leads to a series of questions relative to security and the public's right to feel safe/secure against individual liberties ... often ending in a draw depending on: a person's predisposition on the actual issue (ACLU, for example would probably defend the individual's rights on most accounts) and the severity of the potential action; are we talking loss of life versus inconvenience?

Mitchell Goldberg
National Sales Manager, Retail
Mallinckrodt

Securing the public

I think it is critical that security issues are continuously addressed and improved throughout all segments of the healthcare industry and not just pharmaceuticals — as referenced in the feedback question. Delivery organizations, such as hospitals and provider offices, as well as managed-care organizations perhaps hold the most critical data that need to be secured. Perhaps what is most compelling is the emergence of integrated patient data between the financial institutions and healthcare data, as many financial institutions are now in the business of healthcare transactions. The types of patient information that are now made available for protective purposes are more complex and expanded than ever, so enhanced security is a must.

Patient information can be properly and securely abdicated in an environment that is configured properly, as firewalls and other security technologies only work as optimally as possible according to how they are configured and as long as proper security process protocols are put into place among those individuals and a variety of access levels are established. Security shouldn’t inhibit our ability to drive better patient care and make more informed healthcare decisions.

Andy Weissberg
Executive VP
CPRi Communications

Technology dependency

Yes, we have become so technology dependent it is necessary to increase security to ensure the protection of confidential information.

Julie Kelly
Senior Director, Marketing and Business Development
Ventiv Pharma Services

Drawing the line

As a small business owner, I’m in favor of protecting company assets to the greatest extent possible. But I draw the line when that protection comes at the expense of people.

Turning people into data that can be stored, sorted, and analyzed is the path to an invasion of personal privacy and security that will spin out of control. We’re all smart people. There must be a better way to safeguard company intellectual property compared with the current options.

Mark Anzalone
Principal
M2 WorldWide Inc.

More on Patient Registries ...

Advantages outweigh disadvantages

I agree with the concept of patient registries. Whatever disadvantages it might pose are likely to be outweighed by the advantages (avoiding unnecessary duplication, inadvertent skewing of negative data, etc.). There should be a fair way to set this up that does not compromise patient privacy or pharma company intellectual property.

Cricket Darby, Ph.D.
Senior Medical Writer, Scientific Affairs
Interlink Healthcare Communications

Nothing to hide

It has become increasingly important, as authoritarian figures repeatedly violate the public trust, for companies to demonstrate that they are hiding nothing and that summaries of clinical-trial data are reflective of actual outcomes.

Whether the publishing of clinical data becomes mandatory or not, it seems to me that proactive companies will publish voluntarily in an effort to show they have nothing to hide.

Avis L. Bridgers, M.S.
ADME Team Leader
Cardinal Health

Study goals could be improved

In principle, full disclosure is in the public’s best interest. With public disclosure, the design of postmarketing studies may improve with more careful thought about study goals. One negative is that competing companies may use the public data to discredit the competition in unfair ways.

Jules T. Mitchel, MBA, Ph.D.
President
Target Health Inc.