

INFORMATION SECURITY MATTERS

October 2004
Volume 1, Issue 2

Cedric Bennett & Associates ◦ ced@bennettsite.com ◦ 650 858-0883 ◦ <http://bennettsite.com/cba>



PCs Can't Protect Themselves — They Need Help

It doesn't seem to matter when you check the news – there will almost always be an article about a serious internet-based attack. And, unfortunately, things seem to be getting worse.

For instance, this September a virus knocked out computer systems at the Colorado Division of Motor Vehicles offices preventing documents, identification cards, and driver's licenses from being issued and requiring costly and time consuming repair.

In the same month, exploit code designed to take advantage of a recently announced vulnerability in Microsoft Windows appeared on the Internet just a few days after patches became available. This particular vulnerability allows malicious code to hide inside the commonly used JPEG image file format.

"...asking PC users to download patches when they become available...just doesn't work"

Inside This Issue

PCs Can't Protect Themselves – They Need Help	1
Is Information Security Really Everyone's Responsibility?	1
What's That Shield About?	2

That malware (**malicious software**) can become active on a computer as soon as a picture is opened in any one of many popular programs capable of displaying photographs and other image files. Infected files could be delivered by visiting a contaminated web site or from opening the wrong email attachment.

Computer security firm, Symantec Corp., recently announced that the number of new viruses and worms aimed at Microsoft's Windows operating system rose 400% (1,000 to 5,000) between January and June 2004 over the same period in 2003.

At many of our institutions, networks are open enough to allow attacks to reach hundreds or even thousands of widely distributed personal computers. Researchers at the SANS Institute's Internet Storm Center now estimate that an unprotected PC will be compromised within 20 minutes of being connected to the Internet (down from the 40 minute estimate of 2003); one university recently put

Please see *Protecting PCs* on page 2

Is Information Security Really Everyone's Responsibility?

If you pick up just about any "how to..." book on information security you'll find a place where it will say "...information security is everyone's responsibility." But such a statement can't seriously intend that everyone must become an information security expert. That would be similar to a book on home security suggesting that everyone must become an

experienced police officer. But if it doesn't mean that, what does it mean?

The answer to this question lies in the ideas behind **information security awareness**. Awareness with regard to information security is similar to awareness with regard to personal security (e.g., it

Please see *Awareness* on page 2

Protecting PCs from page 1

that estimate to the test and empirically verified the time frame. Even if a campus has a strong perimeter defense in place, enough PCs travel to unprotected areas where they can be successfully attacked (e.g., laptops that go back and forth between home and office or are taken on the road) and then return to the local network where they can become an internal source of infection to others on the network

In considering how to protect personal computers, it has become obvious that asking PC users to download patches when they become available or to keep their anti-virus software regularly updated just doesn't work. Security officers and others responsible for the safe and effective operation of the network need to take more proactive steps to ensure that infection is stopped before it begins.

Patch management systems that can automatically provide system patches and anti-virus systems that push updates as soon as they become available are very effective ways to prevent run away infections from getting started. Even if some computers become infected while they are off the protected net, they will not be able to spread the damage very far when they return if most other computers have already been inoculated against the latest virus or other internet-based attack. ♥

Awareness from page 1

is the same sort of thing that causes most of us to fasten our seatbelts when we get into a car or teach our children not to open the door to strangers). We learn some basic rules about personal safety and are also able to apply the concepts behind those rules to new situations as they arise. The difference is that personal security awareness is fairly high for most people while information security awareness is much less so.

What we'd like is for everyone associated with the use of information processing technologies (and

on our campuses, that's just about everyone) to develop similar habits with regard to information security. And we'd also like them to apply the concepts behind those habits to new situations.

A good way to accomplish that objective is to leverage concerns about personal security toward habits that will protect assets in information environments. For example, identity theft is a growing concern for most individuals; helping colleagues learn how to prevent identity theft will pay larger dividends as they begin to apply those lessons to institutional information. ♥

What's That Shield About?

It is probably obvious that the shield logo on the front of this newsletter is designed to symbolize the protection that a good information security strategy and the exercise of effective practices provide to institutions and individuals. The three words engraved into the shield represent the three principles upon which information security is built (some believe there are more).

Integrity can be defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. **Confidentiality** is seen as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. **Availability** means ensuring timely and reliable access to and use of information. [Each of these definitions was extracted from 44 U.S.C., Sec. 3542.]

Of the three, I put **Availability** first on my shield because I like the reminder that information security is about much more than just preventing bad activity. The word **security** implies so much about protecting assets that I think it is important to stress that it is also very much about ensuring accessibility to those information resources. ♥