

INFORMATION SECURITY MATTERS

January 2005
Volume 2, Issue 1

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



Information Security Can Be a Very Tough Sell

It can sometimes feel like pulling teeth to get most of our colleagues to understand and act in ways that will protect the institution's critical information resources. More to the point, it is often extremely difficult to obtain funding for the things that minimally need to be done to provide a reasonable level of protection to the institution.

It can be frustrating, for those responsible for information security, to find that the decision-makers seem not to understand how critical the information security issues are. But that should not be so surprising.

Institutional resources are always scarce and there are usually many very important priorities competing for those limited funds. Moreover, while providing good information security for the institution may be mission-

"...while providing good information security for the institution may be mission-critical, it is not the critical mission of the institution."

The Growing Spyware Threat

Over the past few years a new kind of internet-based threat has been steadily and stealthily growing to the point where it is now becoming a serious epidemic. That threat is coming from a class of software known as spyware.

If you've noticed your computer seems to be run-

Inside This Issue

Information Security Can Be a Very Tough Sell	1
The Growing Spyware Threat	1

critical, it is not the critical mission of the institution. It is up to information security leaders to make the case strongly and in terms to which others in the institution can relate.

Effective information security leaders understand that the fundamental method for determining where to apply scarce security resources is through risk assessment. Unfortunately, the results of the best risk assessment can only point to the areas of greatest need for increased threat mitigation. That documentation cannot do much to help others understand that mitigation's relative importance compared to other competing campus priorities.

Since information security is most often about preventing or fixing security problems, funding requests will not usually be about providing some new academic or administrative service that can show a return on investment, cost savings, or even an improved level of service. The fact is that information security delivers a "negative benefit" — that is, if it is working well, then certain undesirable events happen less often.

Please see *Tough Sell* on page 2

ning slower or crashing more often, it may be infected with spyware. If your browser's home page has been hijacked (it is no longer set to the page you chose), the computer is most certainly spyware infected.

There is not complete agreement on the definition
Please see *Spyware* on page 2

Tough Sell from page 1

There is a way, however, to compute a Return on Security Investment (ROSI) for a risk mitigation approach by looking not at the dollars it will save but at the dollars it can avoid losing. The evaluation of this potential loss, called the Annual Loss Expectancy (ALE) is the financial damage that would be created by a particular security failure times the annual frequency of that failure occurring. So, for example, if a particular failure will cost \$100,000 and it is likely to occur every two years, then the ALE is \$50,000. Then computing the ROSI is a matter of subtracting the cost of the mitigation from the ALE. A positive result, indicating a security investment that has a positive cost-benefit, can then be compared to other priorities competing for the same funds.

This approach has real value and does work but has some obvious weaknesses that must be addressed by anyone using it. Those weaknesses are data credibility and impact.

The ALE calculation is very sensitive to its two data points — cost of damage and annual frequency. Anyone using this formula must take some pains to be able to support the numbers used. Cost of damage can consist of such items as the cost of system recovery, costs of data recovery and validation, costs of any fines, the costs of litigation, and the costs of any resulting lost revenues (e.g., loss of a contract, research grant, or donation). There are secondary costs that are even harder to quantify like reduced enrollment because of a loss in reputation — these are so ethereal that they are best left out of any calculation. Determining an annual frequency is also difficult. Sources for that information can be past institutional experience or the experiences of others found in public studies or by networking with peers at other institutions.

Even when the data used is well supported and documented, the overall impact of the calculated ROSI can be the most difficult challenge to manage. That is because this issue is about believability and not about the calculation itself. If no one believes what is, after

all, a *potential* loss then the argument essentially falls on deaf ears. Impact is addressed best by reference to actual events. Keeping track of what is happening at peer institutions is one way to bolster the impact of the calculated ROSI. Having good data with regard to cost of failures on one's own campus will usually provide the strongest support of all. ♥

Spyware from page 1

of spyware – it comes in several forms. At its most basic, however, it is software that gathers and transmits personally identifiable information from your computer to some other place on the internet without your knowledge. Another, slightly less obnoxious form of spyware (called *adware*) transmits aggregated information that is supposedly less personally identifiable.

Spyware usually comes along as a hidden portion of some other software you've chosen to install. In many cases, though not all, the End-User License Agreement (EULA) that you "sign" by clicking some sort of acceptance will include some lines indicating the possibility of information gathering — but most of us never read the EULA.

What can you do about spyware? There are several commercial products now on the market, as well as some excellent freeware, that will help you control spyware on your computer. Microsoft has recently released an anti-spyware beta (currently free).

None of these products will find all the spyware that might exist on your computer — most experts recommend that you run a couple of different anti-spyware products to increase the chances that you will find everything.

One important note of caution, however, is that some of the software you installed that also slipped spyware onto your computer may fail to run without that spyware's presence. You should use care the first time you use spyware removal tools. ♥