



## **Measuring Vector Defense, Part I**

**infectionvectors.com**

**July 2004**

### **Overview**

The use of metrics to benchmark and evaluate the success of a project is nothing new. Over the last few years, however, the push behind Return on Security Investment (ROSI) has brought the use of metrics to the forefront of Information Assurance (IA). This article will attempt to identify the special issues relating to virus defense and ROSI.

### **Metric Selection**

Any measure of security efforts may be appropriate, depending on the environment. It is possible to chart only the actual security incidents that occur (things such as successful penetration attempts, virus infections, etc.) and use this simple tally as a means of determining how much progress is being made by the IA team. If the number of events continues to decline, all is well. This type of calculus is unlikely to fit with the actual security goals of many organizations. The shortcomings of such a model are probably clear: such a simple calculation does not take into account the seriousness of each event and it cannot help fix problems. The model does not offer any insight as to whether too many or too few resources are applied to IA.

The ROSI literature is full of ideas for metrics and how to improve them. Searching this existing base of information is all that is needed to obtain procedures for measuring an organization's security planning and solutions. Most of these begin with extensive reviews of organizational assets, quantifying their importance, and assigning a value to their compromise.

### **Technical Defense**

In terms of technical defenses, such things as the number of patched/unpatched machines that exist on a network are important. These are easily tangible figures, whether a certain fix or mitigation has been applied. The importance of each fix is quantified by the threat that exists; if there is no known exploit code or worm that takes advantage of the vulnerability then the patch level is less important. On the other side, if a number of machines have been cracked by manual or automatic methods, the patch compliance number is a critical measure of the overall security posture. How an administrator measures such a figure, however, is still up for individual interpretation. Is it better to have a single machine missing 10 patches or 10 machines missing a single patch? The paradigm selected here also impacts how the measurement is taken, whether the number of patches missed or the number of machines that are missing one or more patches populates the numerator.

Technical defense is best measured with technical tools such as vulnerability scanners, penetration testing, and audits. Such tools will generate a rather definite score, the number of vulnerabilities that are not patched on the network. This score will be reliable as long as the scan is completed from the same location (inside/outside firewall, ACLs remain consistent, etc.). These types of tests offer a look at the security posture and provide a road map for mitigation, namely a list of vulnerable hosts.

Of course, vulnerability scanners can't tell an administrator how susceptible hosts are to viruses. That measurement would be a combination of firewall rules, which patches were missing from a box (clearly the RPC DCOM patches should be weighted more heavily in terms of virus security than a local privilege escalation based on the number of active worms that exploit the former), and the antivirus software running. In addition, the user of a machine is often the most important factor in judging whether a virus compromise is likely, an issue that is discussed below. Vulnerability scanners can, however, provide a very clear report on patchable infection vectors.

Vulnerability scanners don't have to take the form of large packages from security-focused companies, although there are some very good ones available. Additional tools fill the needs of security administrators very nicely:

#### Open Share Tools

There are free applications and easy to modify scripts that can scan a network for all available shares and the rights associated with them. With the extensive use of network share vectors (worms like Lovgate and Netsky include this as a propagation mechanism), this information is critical to know. Charting the number of open/unprotected shares on the network each month gives a good indication of how machines are being configured for network use.

#### Password Crackers

Every security administrator probably has to run some type of password audit. Ensuring that local administrator/root passwords are not easily guessed (and especially that they're not in the list included with worms like Agobot) is an important step to locking down devices. These types of cracks give a good idea of how well shares/devices are guarded and how well users are doing with selecting good passwords.

#### Social Defense

As important as technical measures are, it is also critical to ensure that users have a solid "virus IQ." This means that the user population is aware of best practices when it comes to opening email messages, downloading files, and identifying strange PC behavior.

User training and testing, indicating how much a user retains can measure social defense. Anonymous polling is also helpful, where it may be possible to gauge what a user actually does when encountering an unknown email attachment, for instance. Along the

same lines, it can be very insightful for a security administrator if he or she simply sits and talks to users about the habits they practice and what they observe in the office.

The idea of such a “score” for antivirus knowledge is certainly nebulous, however, there are some very real measurements that can be taken. The following is a short list of examples:

## **Virus Culture Metrics**

### Self/Company Assessments

In addition to asking users what they know about safe computing practices, it is important to gauge how secure they feel on the organization’s LAN. Questions such as “How safe and reliable is data stored on company servers?” may be very helpful in uncovering the perceptions the users have about the network.

### Response Audits

“What would you do if you received the following email, pop-up, warning, etc.?” type questions are distinct from the previous assessment in that they determine how a typical user would respond to specific incidents. These measures can be used to diagnose the awareness of the user base. Further, with respect to such issues as phishing and mass mailer tactics, the questions alone may spur dialog that helps train the user how sophisticated an attack may look.

### Simulations

Basic scripting or coding knowledge would allow a security administrator to create a simulated “mass mail message” or pop-up warning for a random sample of users (broad scale simulations will likely result in a lot of help desk calls), just in an effort to judge what the response would be. Simulations can also take the form of focus group style meetings, to ask questions similar to those above.

### External Groups

Reputable outside organizations can offer a number of tests, from the simple surveying above to real “pop quiz” style assessments and penetration attempts.

With any type of assessment, the goal is simply to create a reliable test that produces a measured score and can be reproduced regularly. It isn’t important that the score is imprecise, as long as it does give an accurate reflection of the overall security posture. The numbers can be charted, progress monitored, and presented to higher level decision makers for action. A steady decline in virus knowledge may be the impetus for additional security training (as opposed to the traditional catalyst for additional education: a major outbreak within the organization).

The next part of this article will discuss what to do with this information and how it plays into the ROSI concept.

Copyright © 2004 infectionvectors.com. All rights reserved.