3 METRICS TO GAUGE SECURITY SPENDING

IS YOUR SECURITY STRATEGY ON THE MARK? HERE ARE THREE RATIOS TO HELP YOU ASSESS ITS EFFECTIVENESS.

BY PAUL A. STRASSMANN

THE IDEA THAT THE INTERNET COULD FAIL never crossed my mind until Oct. 21, 2002. As acting CIO of NASA, I was informed that a computer at the Ames Research Center in California, operating as one of 13 global Internet domain name root-name servers—the master address controls for the entire Internet—was rejecting incoming traffic from California to as far west as India.

A globally coordinated distributed denial of service (DDoS) attack was aiming to overwhelm the processing capacity of each root-name server. We had to start throttling down incoming traffic before we ceased to function.

The attack volume did not exceed 50 to 100 megabits per second per root server, yet the impact was devastating. Failing servers handed over traffic to their peers. The workload on the survivors rose sharply and led to "cascading" failures. Nine of the 13 root servers were out of commission in a few minutes. The hidden attacker, after two hours, retreated after gathering sufficient intelligence about the weaknesses of our defenses.

This "information warfare" probe was the first known simultaneous attack on every root server.

The incoming flood of messages was traced as coming primarily from South Korea, but there was no way to track the perpetrators. On the Internet, assaults can be executed by proxy machines, triggered from anywhere. At that point, I stopped trusting the Internet as a safe information highway.

In January 2003, my apprehensions were confirmed again when the rapidly spreading Slammer worm started clogging the Internet. It was propagating worldwide by capturing the operating systems on infected computers—running the widely used Microsoft SQL Server 2000 as well as the Microsoft Desktop Engine 2000—and turning them into "zombie" generators of messages that replicated the worm. This worm was small, only 376 bytes, but clever in its self-propagating habits. As traffic surged, worms took over much of the Internet's traffic and jammed network switches, which then re-routed transmissions to less congested paths. In this way, the traffic queues could be built up and spread worldwide in a few minutes so that many messages could not be delivered.

And the Slammer isn't the only attempt to damage Internet communications; as of this writing, my library of known intruders contains 72,838 viruses, worms and other malware.

As designed, the Internet does not ensure the integrity of the data (e.g., e-mail messages) that traverses it. There's no way to be sure, for example, that a service provider between point A and point B has not tampered with data. It's also easy to disguise the source of an attack because of the Internet's decentralized architecture.

Many CIOs argue that it is difficult to measure the value of investments in computer security, but I believe you can determine whether your organization's approach is on target.

The prospect of imposing an all-encompassing security discipline on the global Internet is zero. The best an organization can do is carve out a securely managed intranet, sufficiently isolated from the public Internet with every affordable protective measure. Even then, attackers will find ways to circumvent the defenses.

So how, then, do you figure out a return on your security investments? While many CIOs say it is difficult to measure the value of investments in computer security, I believe it is possible to gauge whether your organization's approach is on target. I recommend looking at three ratios. (See "Is Your Security Strategy Sound?" on p. 108 for details.) The ratios are:

- Compare information security spending vs. total I.T. spending. If security spending exceeds 10%, your business architecture is probably poorly designed to cope with attackers.
- Examine the value of lost employee time vs. your investment in information security. If the cost of your security investment is 200% or more of the value of employee downtime, you may be spending too much on security.
- Measure what impact cyberattacks are having on employee productivity. If you are experiencing a loss of 1% or more in productivity, review how you are protecting your information. For instance, examine the location of your firewalls to determine whether centralization of defensive barriers would give you greater protection.

The goal of total security is not achievable in complex systems that have millions of hardware and software vulnerability points. The defenders will have to monitor the frequency and losses from intrusions to balance the costs of protection against potential damages.

PAUL A. STRASSMANN IS A FORMER TECHNOLOGY EXECUTIVE AT XEROX, NASA AND KRAFT. HE CAN BE REACHED AT PAUL@STRASSMANN.COM.

PHOTOGRAPH BY STEVE FREEMAN