BUSINESS **SOLUTIONS**

Making the case for security spending

Last Updated: 01/26/08

Executive Summary

Management wants to know the return on investment. But when it comes to security, there are more practical and realistic ways to decide what to spend.

Forget calculating the ROI. Common-sense risk management is the answer.

Return on investment (ROI) is a conventional business calculation that almost all companies use to allocate resources for maximum profitability. The calculation is simple: subtract the investment from the payback (increased profits) and divide by the investment. The key is to completely account for all the costs and all the profits. In most business situations, such as adding new production capacity, that's not hard to do. For network security, however, the ROI concept doesn't work well.

Many attempts have been made to develop a useful approach and even a special term, return on security investment (ROSI) has been coined, but the attempts have been less than successful. With some methods, calculations and speculations are so complex that by the time they're completed, the security situation has changed. Why is it so hard to do?

One difficulty is that security doesn't contribute to profitability the way machines or personnel do. Therefore, it can't produce a "return," any more than security fences or security cameras can. The financial benefits it delivers are difficult to identify and measure, because they involve events that (you hope) don't happen and might not even be recognized if they did. It's very hard to project the return on investment when you can't even measure the return.

Another difficulty is that there are so many variables, unknowns and intangibles in the world of network security. There are thousands of threats, with new ones arising every day and thousands of hardware and application vulnerabilities. And, the potential economic impact of a security breach is hard to predict; it can range from very small to large enough to threaten your organization's existence.

So, network security ROI is both difficult to calculate and essentially of limited value. But that doesn't mean you can't make a hard-nosed economic case for IT security investments. You just have to take a risk management approach. Following is a simple method that can help you and your management make reasonable decisions about security spending.

Base your investment on the risk

Start with the fact that your network is critical to your organization's survival and success; without it, you're out of business. Unfortunately, Internet access is also vital, and there's no denying that Internet-borne security threats are real and relentless, and they are becoming much more sophisticated and more numerous. It's certain that your network is being attacked all the time, and sooner or later, an attack is going to be successful. When? What kind of attack? What kind of damage? How much damage?

Risk management is a common business practice, and all major corporations employ it, especially insurance companies, which have actuarial tables for evaluating and quantifying many kinds of risks. If your organization has the resources to conduct comprehensive risk assessment and management, take advantage of it. But, for most organizations, sophisticated risk management for IT security is beyond reach, because of the time and resources required. If that's your situation, here's what you can do.

First, work with your management to quantify the cost of a potential security incident, starting with a realistic worst-case scenario. What happens to your organization if your network or Web site is down for a few hours? A day? A week? It should be pretty easy to come up with useful ballpark numbers based on lost revenues, lost productivity and other identifiable costs. Or, what is the potential cost of a security breach, where sensitive personal data is compromised and you are faced with restitution, regulatory penalties and legal costs? This is a little harder to define, but intelligent guesses based on the published experiences of other companies will help.

Answers to these questions will probably be a real eye-opener for everyone and should be a great starting point for discussing the value of network security for your company. The initial response might be that you should spend whatever it takes to prevent that worst-case loss, but that isn't the solution. You know by now that you can't buy perfect security for any amount of money, let alone for what your organization can reasonably invest. So, it's going to be a matter of identifying and addressing priorities. That's where you, as IT manager, can help your management make good security choices.

When you have management's attention, recommend a security assessment if you haven't already performed one. The assessment will clearly identify your weaknesses so you can develop a budget and allocate it for maximum effectiveness.

Let CDW help you reduce your risk

CDW's security specialists can help you with every part of your security strategy, from security assessment to selecting, installing and configuring the right security software and hardware solutions for your organization. We work with midsize to large businesses and stay up-to-date with the latest security developments. Ask your CDW account manager for details. If you don't have an account manager, call us at (800) 985-4239.