



Information Security Budgeting and ROSI

By Richard A. Diamond ■ *Stradivarius Associates*

The core function of IT security is to protect your company's digital assets. Being in the broadband industry heightens these issues. We all know that total protection is impossible so there are risks that need to be reviewed and analyzed on an annual basis. Now is a good time to do this audit since we are closing in on budget time and invariably, there will be changes to your security budget. It is not easy to keep pace with technology and most security tools and programs need refreshing and updating. To keep on top of it all costs money. As

"We all know that total protection is impossible so there are risks that need to be reviewed and analyzed on an annual basis."

a rule of thumb, security spending has run between five and ten percent of the overall IT budget. Experts recommend devising a simple security scorecard that depicts your core business areas, the security technologies, the awareness programs and the level of compliance within each of these areas. This scorecard creates a basis for your budgeting process.

With all of the new heightened regulatory and compliance responsibility, most companies find themselves under scrutiny by clients, board members, business partners or government agencies. As you renew contracts, including insurance policies, you will find more language about your security practices included, plus requests for statements of policy, practice and technology strategy.

Board members and senior management understand the concepts of miti-

gating controls and risk management. Make sure that all communications are spoken in those terms. Accountability is of the utmost importance and on the mind of C-level executives. A company without a documented, funded and sustained program around information protection is @Risk.

Overall Market Update

Companies expect to spend roughly 10% of their total IT budget on security in 2003, an 8% increase over 2002 levels, with employee education, business continuity and disaster recovery

taking priority. Current employees still pose the biggest threat to companies' technology infrastructures, and security executives are most concerned about electronic attacks like viruses and unauthorized access to systems. Recent high-profile events such as the "Blaster" worm and "SoBig" virus in August 2003 affected over one million computers.

The importance of protecting company assets will continue to be elevated to the corner office and will become a priority of the CEO over other IT issues. The customer plays an important role in companies' security plans, and organizations that instill confidence in customers that their personal and business information is safe will establish a competitive edge.

Exercising Due Care

Due care and due diligence are in

order regardless of the line of business you are in. As an apartment building owner, broadband service provider or supplier to the industry, it is incumbent upon you to protect your key business assets.

The downside costs of not having a stated, sustained IT security program are greater now than ever. Corporate officers are expected to exercise "due care" with respect to protecting assets of the company. Information is one of the largest assets that many broadband related companies have—i.e. residents-customer information. Before convincing management or the board of directors of the need for security funding, your corporate officers need to be aligned with your proposed strategy.

Use a Simple Three-Step Approach:

Step number one: Take inventory of your company's digital assets.

Step number two: Establish the value of keeping those digital assets protected.

Step number three: Use your security scorecard to lay out your new budget based upon steps one and two.

Once you have gone through the exercise of identifying your company's core systems and data, you'll need to place a dollar value on what the cost would be to have this information in the wrong hands such as a competitor, disgruntled employee or data broker. Focus on the desired end results and place a value on these items (reputation, revenue growth, retained earnings). This too will factor into understanding how much to spend on security and where to focus your spending. With all of that information, you can begin to structure a sus-

"Companies expect to spend roughly 10% of their total IT budget on security in 2003, an 8% increase over 2002 levels, with employee education, business continuity and disaster recovery taking priority."

tainable security budget. Create a three to five year plan that clearly depicts what you plan to do, why you propose doing it and what the risks are of not moving ahead with each of the budgeted items. It may be a good investment to bring in an outside (unbiased) security professional to consult with you on your budget and implementation plan.

ROSI and Your Company

First, ROSI defined: Return on Security Investment. The point of maximum return on security investments is where the total cost of security is lowest—including both the cost of security events and the cost of the security controls designed to prevent them.

Executives know the threat is real but many don't feel it. For that reason, IT relies on, more than anything, FUD (fear uncertainty and doubt) to sell security. The thinking is that if you scare them, they will spend. FUD has its limitations though, especially during a recession. If you can prove a real return on invested dollars, management will listen.

Determining cost-benefit is the simple task of subtracting the security investment from the damage prevented. If you end up with a positive number, there's a positive ROSI. For example, an intrusion detection system that costs \$40,000 and was 85 percent effective netted an ROI of \$45,000 on a network that expected to lose \$100,000 per year due to security breaches. When this model is applied to your real life situation, this could provide the

data needed in order to demonstrate not only that the investment pays off but by how much.

The insurance industry in all likelihood will be the engine that drives both the science of ROSI and the technology of security. All other factors being equal, the insurance discounts will eventually make one web server a better buy than another. Software vendors will be forced to fix the holes in their products in order to benefit from lower premiums.

In fact, that is precisely what happened in the case of fire sprinklers. British insurance carriers began offering discounts to business owners that invested in sprinklers and deeper discounts for those with more sophisticated systems. Naturally, insurance rates rose for businesses without sprinklers. Ultimately, more companies will realize how important it is to add more advanced information security practices. As our ability to prove out the ROSI increases, so will managements investment in IT security. And when this practice is optimized, your company will no longer be @Risk.

About the Author

Richard A. Diamond is the President & CEO of Stradivarius Associates which specializes in business strategy consulting for public and private companies around the world. He actively consults with ImagiNet (www.imagi.net) a leading secure managed network service provider, offering a comprehensive suite of network management, online data backup, WAN and security products and services. ImagiNet has operated its "state of the art" Secure Operations Center 24 x 7 x 365 for over 17 years. He can be reached via email at rdiamond@stradass.com.



"...ROSI defined: Return on Security Investment."