

eSubnet Fragment Article

Risk Management

I'm going to discuss a fictional company named SMB Inc. SMB distributes business products., and over the last 4 years has grown by focusing on their clients' needs, keeping costs low, reliably meeting payroll, and opening new distribution channels for their clients' products. The management and staff of SMB have worked hard to grow and are successful with a roster of satisfied well-known clients.

SMB Inc. management understand that with their new found success comes responsibility. One of their new big clients has developed their own products, along with the intellectual property and well-known and valued brand. They aren't willing to risk this success in any way. And so SMB Inc. has been asked to provide assurances of security.

How should SMB's management approach this problem? Certainly they could throw money at the security problems they know about. But they'll be left with questions. Have they spent the right amount, too little or too much? Did they spend in the right areas? Did they focus on the right concerns? Let's look at how to answer these questions.

Determining Risk

Security architects understand that in order to put the proper defenses in place, the risks involved to the organization need to be known and understood. There is a simple formula for quantifying risk:

$$\text{Impact of the Event (\$)} \text{ multiplied by the Rate of Occurrence (\#)} = \text{Risk (\$)}$$

We all do this calculation regularly. We are constantly judging and managing risk in order to act wisely.

What makes risk management work?

For risk management to be effective it should:

- provide value
- be a regular part of everyday processes and decisions
- acknowledge user needs while remaining transparent to the users
- be flexible, adaptive, and responsive to change

With these criteria in mind, anyone can build the basis of a good risk management system.

Here are two examples:

1. We are all exposed to the risk of getting shot on the street. There were 34 incidents of people dying from gunshot wounds in Toronto in 2008. Now, any one of these people could have avoided death with the purchase of a bulletproof vest, roughly \$250.00. However, most people don't wear vests despite the high impact of the event (death) because the rate of occurrence (34 out of roughly 4 million people per year) is so very low and vests are bulky and uncomfortable.
2. Almost everyone puts on their seatbelt when they get into their car. Why? There are two risks here to be considered. The first is the risk of death or injury in the event of an auto accident. The rate of occurrence here is relatively high considering the number of cars on the road. The second consideration, and the one I think has stronger bearing, is the chance of being fined when caught by the police. The penalty for seat belt infractions is between \$60 and \$500. This is a high impact event for many of us, and with a high rate of occurrence.

Managing Risks

With a risk framework in place, the management of SMB Inc. can begin to look at where the value lies in their company. Management has to consider digital and physical assets, the value of their people and processes, and the costs of a lost day of work. They might consider their ability for revenue generation, their intellectual property and that of their clients, their ability to retain staff, etc. I've stated these areas of consideration broadly so that they cover the entire organization. Now, we can calculate losses and the occurrence rates, allowing SMB to set a budget for their security needs.

With a budget in place based on the risks, SMB will be able to decide where to focus effort and money. Two that come to mind are the high danger areas or hot-spots, and the simple to fix areas or low hanging fruit. And there are side-benefits to watch for; often protecting one area reduces risk in other areas of the organization.

There are four ways (in order of preference) to handle a risk: Avoidance (eliminate), Reduction (mitigate), Transfer (outsource or insure), and Retention (accept and budget). Every solution will use one or more of these elements to manage risk. The final choice, retention, is the least desirable. The level of risk for any valued asset can never be brought to zero. There are always factors outside the control of staff and management, so there is always some risk left. Through avoidance, reduction and transfer, the risk might be reduced almost to zero but not eliminated.

After going through each of their assets, valuing them, assigning one method of managing the risk involved, and implementing that method, SMB can carry on working with their new big client with more confidence. The new big client will receive its assurance that SMB is a reliable and secure partner. The unknown has become known, the unmeasured quantified and now everyone can sleep a little easier at night.

Conclusion

Here you have been given a brief view in to risk management. Your organization's risks are unique. In IT, risk management is usually broken into the following areas: anti-virus to protect workstation and server computers, firewalls to protect and control access to networked servers, back-up systems to protect the data, and encryption to protect systems outside of the office. This is list is neither definitive nor complete. You have unique requirements as well, which will require going beyond this usual list of security protections. To be comprehensive, make sure to add these areas to your risk management solution, just like SMB Inc.

Originally published May, 2009

About the Author

Richard Danielli is the founder and President of eSubnet Enterprises. He has broad expertise in the fields of networking and data security. Based in Toronto, eSubnet provides superior customized solutions for networking and data security. Additional articles are available at <http://www.esubnet.com/fragment.html>.

Reprints

1. Commercial use: Commercial newspapers, magazines and websites that wish to reprint an article should contact eSubnet for permission.
2. Non-Commercial use: Any reproduction of content (excerpt or full text) by nonprofit organizations or companies wishing to share information with their members or clients requires that you notify us, whether for print or online usage.

Regarding reprints, contact Mr. Danielli at [rdanielli\(at\)esubnet.com](mailto:rdanielli@esubnet.com) or at (416) 203-1223.