Amenaza
TECHNOLOGIES LIMITED

Approaching Risk in Your Business

A World of Risk

We are surrounded by risk! If it were not for the belief that "bad luck" usually happens to "the other guy" most of us would be paralyzed with fear, huddled in a corner imagining all of the bad things that might happen.

Not all risks are equal. In many common situations our intuition will tell us which dangers can safely be ignored and how to deal with those that matter. In other, less familiar circumstances, the correct choices may not be as obvious. For example, our lives are increasingly dependent on information technology (IT). Developments such as the Internet and wireless networks are double-edged swords. On one hand, they enable the business opportunities and provide the economies of scale that are required for success in many business sectors. On the other, they can be weapons in the hands of adversaries. Hackers, disgruntled employees, competitors, radical social groups, terrorists and enemies of the state all have the means, and the motivation, to actively disrupt IT services and data. Unfortunately, while these sorts of generalizations are true, they have little impact with senior management. Business leaders have become desensitized to these issues because they do not comprehend the relevance to their organizations.

Several years ago the business community was warned that the use of two digit dates in computer systems would result in chaos when the world moved from 1999 to 2000. As a result of these concerns a huge effort was spent correcting Y2K bugs. Given that there was not a single reported major Y2K related disruption anywhere in the world, one of two conclusions can be reached:

- IT departments worldwide, did an outstanding job and got it right the first time
- IT consulting houses did an outstanding job of marketing Y2K related products and services to solve a problem that was not as severe as expected

To this day people debate whether or not the Y2K risks were real. Computer people believe they saved the world. Management suspects they were hoodwinked.

Experiences like Y2K have made management justifiably incredulous when presented with speculative doom and gloom scenarios. Organizations find it difficult to justify spending their limited resources on something that cannot be directly tied to business success. This paper outlines a three step approach to risk management that can be easily defended to all levels of management.

Why Risk Matters

While there are many definitions of "risk," for the purposes of this paper, risk (of a particular event) is defined as

$$Risk \equiv Probability\ of\ an\ Adverse\ Event \times Impact\ of\ the\ Adverse\ Event$$

Knowing that there is the potential for an "adverse event" is of limited use unless the context in

Amenaza Technologies Limited
550, 1000 8th Ave SW
Calgary, AB, Canada
T2P 3M7

Tel: (403)263-7737
Fax: (403)278-8437
Toll Free: 1-888-949-9797
http://www.amenaza.com

Amenaza
TECHNOLOGIES LIMITED

which the event may occur is also known. The potential impact of the event on day to day business activities must be understood in order to evaluate risk.

Business people do not generally use the term *Impact of the Adverse Event.* They are more likely to speak of *Business Impact (BI).*

The determination of Business Impact is often made far more complicated than it needs to be. At its root, the Business Impact can be determined by asking the question:

How will the disruption of information services impact business activities?

This question can be answered by classifying the impact of the incident in one of three ways

- **Tangible direct losses** – "Tangible" literally means "perceptible by touch." In other words, something you can feel or measure. "Direct losses" means that "the revenue stops." An example is an automated manufacturing line. No matter how automated the production line, if parts do not arrive in time because of corrupt inventory data, the production line stops. Non-existent goods cannot be sold. This has an immediate and obvious effect on revenue.
- **Tangible indirect losses** – Indirect losses are harder to quantify than tangible, direct losses but ultimately have just as serious an impact on revenue. For example, company *A* is very interested in building a pipeline in South America. Competition for the pipeline bid is strong as this is a billion dollar deal. Despite the competition, company *A*'s bid is thought to have an edge in several key areas. The entire bid proposal, with all costs, is on the laptop of Company *A*'s Vice President. During the very close negotiations, the bid needs amendment and is insecurely transmitted several times back to head office for clarification using the hotel's Internet facilities. When the contract is awarded, company *A* has lost out to a company which has managed to very slightly undercut company *A*'s key bid areas.
- **Intangible losses** – Intangible losses are difficult to prove or, in some cases, even difficult to detect. The resulting losses are all too real, however. Examples are:
  - Loss of public confidence. If no one buys your stock or bonds the company will have difficulty raising capital for expansion.
  - Loss of customer satisfaction. Repeat business is a key to growth.
  - Damaged reputation. The inability to deliver on promises leads to a loss of customer confidence. It becomes more difficult (and requires more advertising) to attract new customers.
  - Lost opportunities. Suppose that a breach of data security allows a competitor unauthorized access to an important bid or proposal. If the intrusion is not detected the organization may never realize why they lost the bid to the competitor.

Amenaza Technologies Limited
550, 1000 8th Ave SW
Calgary, AB, Canada
T2P 3M7

Tel: (403)263-7737
Fax: (403)278-8437
Toll Free: 1-888-949-9797
http://www.amenaza.com

Amenaza
TECHNOLOGIES LIMITED

A Simple, Three Step Approach to Managing Business Risk

1. **Determine the Probability of Adverse Events**

   Secur*IT*ree, an attack tree based threat modeling tool from Amenaza Technologies, allows you to predict your adversaries' behavior. Based on concepts popularized by Bruce Schneier[1], Secur*IT*ree allows for quick and easy creation of a graphical model showing the most likely points of attack for individual systems or the entire IT infrastructure. With Secur*IT*ree, it can now be predicted

   - who will attack a system.
   - where they will attack.
   - how the attack will be carried out.
   - what resources the attacker will expend to compromise the system.

2. **Determine the Impact of Adverse Events**

   With the sound understanding gained in step 1 of how attacks are likely to occur, it is now possible to assess the impact of the attacks against your IT systems on day-to-day business activities. This can be accomplished by using the three criteria of

   - tangible direct losses
   - tangible indirect losses
   - intangible losses

3. **Create a Prioritized Risk Management Strategy**

   Risk can be managed in only three ways. It can be accepted, avoided or assigned. Refusing to deal with the issue implies risk acceptance. While this is occasionally a good strategy, it is generally better to reduce undue risks to more tolerable levels.

   Analysis of the model created in step 1 will identify ways to modify a system to prevent the attacks that were identified. The cost of the risk mitigation efforts can be estimated and compared to the impact costs found in step 2. **This leads to a simple *cost/benefit* prioritization of the various mitigation activities.** In some cases, it may even indicate that it is more cost effective to accept the risk than to reduce it. In other cases the results may show the best strategy is to assign the risk to another party through an insurance policy.

---

[1] B. Schneier, Secrets and Lies: Digital Security in a Networked World, pp 318-333, 14 August 2000, John Wiley & Sons; ISBN 0471253111
B. Schneier, Attack Trees, Dr. Dobb's Journal, v. 24, n. 12, December 1999, pp. 21-29.
B. Schneier, Attack Trees: Modeling Actual Threats, SANS Network Security 99 – The Fifth Annual Conference on UNIX and NT Network Security, New Orleans, Louisiana.
B. Schneier, Seminar session at the November 1997 Computer Security Institute conference held in Washington DC.

These references do not imply endorsement of Amenaza's tools or processes by Mr. Schneier.

Amenaza Technologies Limited
550, 1000 8th Ave SW
Calgary, AB, Canada
T2P 3M7

Tel: (403)263-7737
Fax: (403)278-8437
Toll Free: 1-888-949-9797
http://www.amenaza.com

Amenaza
TECHNOLOGIES LIMITED

With this prioritized list of mitigation steps you are in a position to invest your finite security resources on measures that yield the greatest *Return on Investment*.

Conclusion

The identification of the risk to your data and information services no longer has to be an abstract concept that is difficult to justify to senior management. Using this three step approach, risk can be modeled for your entire system in terms of the tangible and intangible impacts on business. Senior management can be presented with simple, graphical representations of the significant risks and their potential impact on day-to-day business activities. The graphical approach easily allows "what if" scenarios to be tested to see which countermeasures are most cost effective. Decisions need no longer be made based on the scare tactics of the past.

SecurITree – Dare you risk IT?

Amenaza Technologies Limited has developed the world's most advanced Attack Tree based vulnerability assessment tool, SecurITree. *When used with the accompanying methodology and attack tree libraries,* SecurITree *allows enterprises to discover which weaknesses are most likely to be used against them by attackers .* SecurITree *turns the tables on the attackers by enabling enterprises to quickly and efficiently invest in those security measures that result in the greatest reduction of risk.*

Learn more about Amenaza Technologies and SecurITree *at www.amenaza.com*

Amenaza Technologies Limited
550, 1000 8th Ave SW
Calgary, AB, Canada
T2P 3M7

Tel: (403)263-7737
Fax: (403)278-8437
Toll Free: 1-888-949-9797
http://www.amenaza.com