

Information Security In Times Of Recession

In the farming community, they say that the cow will only milk as much as it is fed. The theory applies bizarrely well to information security budgets in organizations today. While it is definitely unfair to say that higher security budgets always mean better security, the reverse has often proven to be true.

In times of recession, the budget belt needs to be tightened, and sometimes information security spending is seen as the area with excess fat. What happens then is a classic vicious cycle. In slow times, little attention and low budgets can lead to vulnerable infrastructures. During difficult economic times, budget tightening and infrastructure vulnerability go hand in hand.

Virtually Criminal

Cyber-crime is a highly lucrative proposition today. In 2004, cyber-crime surpassed even the drug trade to become a US \$105 billion business¹. The lure of big bucks is a 24/7 pursuit for the underground, and does not slow down when times are rough for the economy. In fact, from a hacker's perspective, it is best to attack targets when they are down and depressed.

During a recession, the impact of a cyber-attack on an organization can often be fatal. The organization is usually busy trying to find its footing in troubled times and a hacker eyeing its information assets can deliver a telling blow to its credibility. In the days when all our assets were on paper, theft was easier to detect. Someone would step into your office and try to make off with a confidential document lying on your desk. Chances are high that you, someone outside your office, or one of the security guards might spot this person. If all fails, it is highly possible that the person's face would be caught on a security camera. Things aren't quite the same in the virtual world. What is worse, it could be too late by the time you find out that someone has stolen your document.

Organizations that have been hit by cyber-attacks report that the cost of proactively implementing information security is nothing compared to that of fixing and plugging leaks after things go horribly wrong. Many organizations don't survive to tell the story.

Getting it right

So if we can agree that information security warrants investment, how do organizations juggle that need when a recession is looming and budgets are constrained?

While it is imperative to have a reasonable and realistic amount of the budget allocated to information security, the key is the correct allocation of funds towards implementation.

Efficient allocation of funds and evaluation of your assets and security controls leads to better results:

- **Inventory of Information Assets**

Take stock of exactly what is included in your infrastructure. It's important to know exactly what you're dealing with before you determine how to protect it. An inventory of information assets must be detailed and include the entire range of infrastructure elements including applications, electronic documents, physical documents, and any other item that holds data critical to your business.

This step is akin to an information gathering phase where you would need to enumerate all the departments that lead to the functioning of the organization and then move on to create a comprehensive inventory. It is important that the information gathered include granular details of each information asset such as the name, type, location, and department responsible for the asset.

- **Classification of Information Assets**

The next step is to classify the assets based on the organization's information classification scheme. This classification is essential to fully understand the value of each information asset and the category it fits in. Often each category of information assets needs a specific type of handling.

The information asset classification process should involve evaluating and ranking information assets based on their sensitivity, with regard to confidentiality, integrity and availability.

- **Threat Analysis**

If you were going to be away on a vacation, you'd think of securing your possessions. Most likely, you'd sit down to evaluate what things are most valuable to you and probably secure them in a bank safe deposit box. You'd then think about the things that are next in line, the ones that are valuable but not quite as valuable. These things would probably be placed in a locked drawer or safe at your home. The basic idea of this entire approach is to prioritize based on risk level. That's exactly what you need to do for information assets as well.

The first step is to identify existing threats that affect the organization's information assets. Examples of threats include viruses, spyware, disgruntled employees, electrical disturbances, vandalism, etc. Next, evaluate each information asset in relation to each threat defined. Then, for each threat, assign a value to the probability that the threat will materialize and another value to the level of impact that would be incurred if the threat were to materialize. Finally,

assign a risk factor to each information asset and then prioritize the assets based on the risk levels involved.

- **Security Control Analysis**

At the end of the threat analysis phase, you'll have a clear picture of the prioritization of information assets. The security controls then need to be applied in that order of priority and in a measure commensurate with the associated risk level identified.

When addressing each information asset, the existing security controls for it must be identified and evaluated. Additional controls should be then identified, evaluated and applied as necessary. This analysis needs to include detailed testing of all administrative, physical and technical security measures and delineating controls that would minimize each threat. For example, the threat posed by an incident could be minimized if an incident response plan was in place that contains critical business function recovery plans, including resource requirement definition, team member contact lists, detailed recovery activity lists and procedures, and off-site requirements. The main focus at this phase is to ensure that high risk rating information assets have adequate security controls in place.

With these steps performed, independent third-party assessments of the infrastructure, such as penetration tests, comprehensive audits and vulnerability assessments, can effectively evaluate if the job was well done and where there is need for improvement.

Managing Enterprise Risk

The right approach to utilizing your information security budget can often make the difference between an organization surviving or going out of business at the slightest hiccup. No business is recession-proof. In depressed times, it becomes all the more important to ensure efficient allocation of funds.

The task of managing enterprise risk remains a daunting one and may well increase in complexity in the months to come. A methodical, process-oriented approach to allocating information security funds is essential to addressing this growing challenge.

References

1. <http://www.foxnews.com/story/0,2933,177016,00.html>