



**Reverse Data Valuation**  
**infectionvectors.com**  
**June 2005**

**Overview**

Many articles on infectionvectors.com (and in the general information assurance arena) ask managers to assign a value to the data they protect. Identifying and evaluating the data stores inside any large organization is quite an undertaking, granted, but one that is vital to effective security strategy planning. By examining how important a particular asset is to the organization's mission, it should be easy to decide which areas need attention and where security spending should go. This paper takes a look at data valuation from the opposite view: by looking at the safeguards in place, one should be able to point to the most valuable and least valuable assets inside a company. Although meant as a complement to the other preparedness documents, whether one sees this report as handy checklist or as the cynical poke from an outsider is all a matter of perspective.

**Door Guards**

Although there are probably a few things any security professional can guess about the security needs of a company (i.e.: that the customer contact database needs to be locked up, that there are proprietary documents that scientific shops have to keep confidential, that the voice network is critical to a call center, etc.), there are many issues that simply cannot be addressed without direct input from the organization. Every sized company must determine what assets are important (in terms of mission criticality) and how important those things are (in terms of dollars/revenue). Hopefully, once security spending is allocated, an auditor could look at the defense infrastructure and determine what items are important to the business. If not, there is likely something wrong with one or more of these following:

- The amount spent on security (the investment)
- The allocation of the security budget (the strategy)
- The implementation of the strategy (the realization)

The word "investment" is used above to imply that there is a little more than money involved, there is the backing of senior leadership, their dedication to information assurance. The "strategy" is a well thought out set of tactics and a vision, again developed by senior leaders. The "realization" is how well the vision is passed down, how it is enforced, and how the vision is turned into a tangible defensive posture.

## Checklist

Given those ideas, there are ways one can take a quick survey of the environment that exists in their data centers. Previous infectionvectors.com reports focused on the possible metrics in place for evaluating the success of a strategy by measuring the security awareness. The items below will help evaluate the emphasis on security by looking at the data itself, not the culture surrounding it.

At a high level, the factors that define how well data is protected are:

- Physical Security
- Access Control
- Antivirus Support
- Backup
- Restore Speed
- Data Integrity Check
- Backup Proximity
- Backup Security

### Physical Security

This is emphasized by every general security text: if an attacker has physical access, they have your system/data. This goes for internal attackers as well; intentional and accidental data losses occur because proper physical safeguards are overlooked.

### Access Control

Hand in hand with physical security is the use of technical controls to ensure only those needing to access data (and make changes) can do so (least privilege and separation of duties for the security professional types).

### Antivirus

This is fairly well accepted across the board, with virtually no large organizations running their shops without virus protection. The precise level is certainly up for debate, however. Some security professionals insist that two different scanners are required, possibly one at a gateway level, one on the client. Is two better than one? Probably, but it's not required for every environment. Again, this is an area where the value of the data is going to drive the decision (expenditure).

### Backup

Does one exist?

### Data Integrity Check

This applies to the production (live) data but especially to the backup. How good is the data on the tape? There are only two answers: reliable and unreliable. That translates into worth restoring and not worth restoring. In terms of live data it also means how well protected are the platforms that house the data.

### Restore Speed

Having the tape is not enough, as the production database can't run off the tape. How fast can the backup be turned into something your company can use? The more data loss costs per hour, the better quick restoration technologies start to look. This also means ensuring that trained personnel exist to complete the restore if needed. At the (almost) obvious level it means that someone is always around that at least knows where the backup and restore devices are (and which tape is which).

### Backup Proximity

Continuity plans often make a mention of data being stored as far away from the main site as possible, but it rarely happens because of the costs involved. This works against the speed of the restoration in most cases, but has become a vital element.

### Backup Security

How well protected is the data at the "secure offsite facility?" That goes for the locks on your provider's doors, but also the state of the data on the tape (is it encrypted when it leaves your facility?).

### **Check Your Score**

There is no scoring system that will work for every type of asset, much less every type of organization. Each security manager can determine how many points they need based on their industry and asset criticality. That being said, there are few businesses that can afford missing everything in the list.

Other infectionvectors.com features have focused on the metrics behind security management. Please see <http://www.infectionvectors.com/emergencyprep.html> for more information.