



Seven Rules for Effective Information Technology (I.T.) Management

© René Mente - October 1, 2005

Corporate Data

Is there anything more important to a business than its corporate data? In most cases, a company's corporate data **is** the company. Sure, corporate data is input [and sometimes managed] by company employees, and is stored on corporate servers accessible by workstations that reside on the company's enterprise network.

Corporate data is often stored in databases (on corporate database servers) and can consist of a company's customer list, inventory, finances, vendors, employees, legal contracts, memos, business plans, etc. In effect, a company's corporate data is a direct reflection of the company itself. It is therefore imperative that we safeguard corporate data, because if irreplaceably lost, it could mean the end of the company.

We have seen this happen in the wake of catastrophic events such as September 11, 2001, and Hurricane Katrina. Entire businesses have vanished from the commercial playing field simply because they neglected to adequately protect their corporate data. This should be the central theme of effective Information Technology (I.T.) management.

Protecting Corporate Data

Protecting your company's corporate data doesn't need to be as sophisticated as rocket science or brain surgery, although many business owner's equate the complexity of these tasks, and therefore the task of protecting corporate data often falls by the wayside.

Also, it's no secret that company's are in business to make a profit. The bigger the profit, the more successful a company is deemed to be. One of the biggest expenses in any business is the company payroll; most companies try to get by with as few employees as possible. This usually translates to a skeleton crew of workers managing their company's corporate data.

We're not advocating that businesses start hiring armies of I.T. geeks to help with the sometimes-daunting task of managing corporate data. In fact, in many cases, it makes perfectly good sense to outsource this function to I.T. specialists [like Neptune Consulting Group, Inc., for example]. If you elect to use the outsourcing option, just make sure that the I.T. outsourcing company is a reputable company (ask for and check references, for example), because you are in effect entrusting them with the crown jewels.

Protecting corporate data can be achieved by observing the following seven rules:

- 1. Data Backups** If you do nothing else, please make sure that your corporate data is getting backed up on a regular basis. Additionally, verify that your backup process, backup software, and backup media are working properly by performing random restores periodically. For lack of any better verification schedule, perform these random restores twice per year, like when standard daylight savings time begins and ends, for example.
- 2. Off-Site Storage** In order to ensure your company's survivability should a cataclysmic event occur, make sure that you regularly send your backup media to an off-site location. If you are the owner of a

small business, you should take copies of the backup media home with you. That way, if your office building is destroyed and/or inaccessible, you will still be able to restore your corporate data at a Data Center or Disaster Recovery Facility.

- 3. Server Management** Corporate data is only as reliable as the servers that store your business's information. Ensure that your corporate database servers are patched with the latest operating system updates, and that they are running the most recent version of database management software from your software vendor. Also make sure that your server has enough disk capacity, memory, and CPU horsepower to effectively run your company's daily operations.
 - 4. Network Security** Taking care of your corporate data also means securing your corporate data. Make sure that the necessary security policies and practices are in place, or you could be sharing your company secrets with your closest competitors. Ensure that user passwords are secure; be sure to keep servers and network equipment patched with the vendor's latest security updates, etc. Periodically review who has access to your corporate database servers, and make sure that only those users with a "need to know" have access to sensitive information.
 - 5. Workstation Management** Every workstation on the corporate network should be well-known to systems and network administrators. Keep an inventory or workstations if necessary. Any unknown device should be treated as a *rogue workstation*. Policies should be in place for allowing rogues, such as laptops and PDAs. Make sure that all workstations have current operating system patches and vendor application patches. Patching workstations should be performed at least once per week. Devices like laptops and PDAs should be patched more frequently, because you probably don't know where they've been.
 - 6. User Policies** Review your Acceptable Use policies at least once per year. If revised, make sure that your employees have reviewed the updates and have them sign the newly revised policies. Technology is constantly changing, and therefore, Acceptable Use policies should keep up with the rapidly changing pace of technological improvements. For example, consumer electronics such as digital cameras and MP3 players can store large quantities of data (up to 100 Megabytes). What is to prevent them from connecting their Apple iPod to a workstations USB port and walk out the door with 100 megabytes of corporate data? This is but one example of how Acceptable Use policies need to keep up with emerging technologies.
 - 7. Disaster Recovery Plan** If your company does not have a Disaster Recovery Plan in place, then please make this a high priority. Taking care of your corporate data is meaningless if there isn't a plan in place to recover should a disaster occur. Disaster Recovery Plans should also be reviewed on an annual basis. Make sure that you have identified potential Disaster Recovery facilities or Data Centers that can handle your data capacity if needed.
-

In Conclusion

Observing these seven basic tenets of I.T. Management could save you enormous headaches down the road; in fact, it could even save your business should a catastrophic event take place. The bottom line is that “being prepared” is everything. Neglecting to take care of your corporate data is the same thing as neglecting your business.

Let's hope for the best, but plan for the worst. Don't be caught off guard. If you do not have the staff to effectively manage your corporate data, then please either hire the expertise, or outsource this vital function to a reputable I.T. service organization like [Neptune Consulting Group, Inc.](#)



René Mente
President / CEO
Neptune Consulting Group, Inc.
