Compromised and lost data

Health & Medicine

Data compromise and loss affiliation Data compromise and loss Nemours is a company, which manages the children’s health systems information data. In 2011, the firm claims to have lost some computer encoded backup tapes, which were been stored in the company’s facility based in Wilmington. The ultimate consequence was the loss of huge information totalling to around 1. 6 million of its patients, vendors, guarantors and employees who have ever worked at the company from the year 1994 to 2004 at its various facilities in Pennsylvania, Delaware, New Jersey and Florida. Those missing encrypted backup tapes comprised of social security numbers, names, bank account information on direct deposit, information on insurance, addresses, medical treatment data and the date of births.

Due to alterations in computer systems in the year 2004 the computer encoded tapes were kept in locked cabinets. Nemours says it lost the computer tapes during the period of remodelling its facility, which took place in August 10, 2004. It could have prevented loss of data by tagging the cabinets and put them in a register containing the name of the person who did the tagging, where they kept the cabinets and at what time, thus this could bring to accountability of the workers who did the tagging process and easy traceability of the cabinets. The cabins could also be moved to one single location in order to avoid tampering by the workers during the renovation process.

In order to prevent data from being compromised and lost, the right security measures should be put in place. In specific, there should be data recovery policy to respond effectively and swiftly to security breach. Moreover, there is need to appoint personnel who will be responsible in ensuring data quality data maintenance. In addition, strong procedures, rules and well-trained staff

who are reliable should also be put in place in order to minimize data loss. Lastly, security measures should be organized and designed according to the data’s composition (Liu & Kuhn, 2010).

Due to numerous information loss, there also exists numerous ways of taking precautions to prevent data loss, for example, numerous power circuits with a generator and battery backup can only prevent loss of information emanating from power failures. Likewise, redundant array of independent disks storage and the journal filing system only prevent data loss arising from specific hardware and software failures. Consistent backup of information are a significant asset when trying to recover from loss of data. Nevertheless, they do not curb system failures and user mistakes.

Good approaches to protection of information ensure incidents of data loss are avoided completely. Such approaches includes procedures like sustaining network firewalls and antiviral protection, equally applying all printed system patches and security repairs. However, the most hard and important aspect of avoiding information loss is by educating the users on how to avoid making errors that endanger the security of information making it prone vulnerability. However, when an organizations data is lost or compromised, there exists steps that need to be taken to increase its chances of recovering the lost information. Firstly, whenever a storage media is affected, all operations that tend to alter or create data should be avoided completely. This comprises of activities like booting the system that is linked to the device that is affected. This is because in numerous operating systems booting may generate temporary files which occupy the region of information loss and this can make the retrieval of lost data completely impossible. Equally, also avoid operations like copying, altering and deletion

of files whenever there are occurrences of data loss. The best thing to do in such situations is switching off the computer and taking away the drive containing data from the computer and re-attaching it to a lesser computer machine which has a write blocker device and try to recover the lost data to your level best (Hawkins, Yen, & Chou, 2000).

Often data recovery is carried out by experts who have already established effective recovery methods to retrieve data from impaired media. This experts provide specialized services and their charges usually depend on the type of security procedures required to be carried out on the damaged media and also the size of the media also counts a lot.

For successful retrieval of information lost, an operational backup strategy is required. In the absence of this effective strategy the process of recovering data entails reinstalling programs and redeveloping data. The cost of retaining the capability of recovering data lost for long durations should also be considered when formulating an operational backup strategy.

Even with good backup strategies, reinstating a system to its previous state can be an uphill task thus data recovery procedures also consider the time when the loss of information occurred and logically, data loss that occurred long ago tend to be difficult to recover compared to recent information loss.

Lastly an operational backup strategy has proportionalities between the amount of effort required and the degree of information loss, for instance it is easier to recover single files that have been lost compared to recovering an entire system (Strunk, Goodson, Scheinholtz, Soules, & Ganger, 2003).

References

Hawkins, S. M., Yen, D. C., & Chou, D. C. (2000). Disaster recovery planning: a strategy for data security. Information Management & Computer Security.

doi: 10. 1108/09685220010353150

Liu, S., & Kuhn, R. (2010). Data Loss Prevention. IT Professional, 12. doi: 10. 1109/MITP. 2010. 52

Strunk, J. D., Goodson, G. R., Scheinholtz, M. L., Soules, C. A. N., & Ganger, G. R. (2003). Self-securing storage: protecting data in compromised systems. Foundations of Intrusion Tolerant Systems, 2003 [Organically Assured and Survivable Information Systems]. doi: 10. 1109/FITS. 2003. 1264933