mozyenterprise®

Data Loss: Understanding the Causes and Costs

The MozyEnterprise advantage

Simple

Seamlessly manage backup, sync and mobile access for multi-user and server environments from a single web-based console.

Secure

Your data is safe with enterprise-grade encryption, world-class data centers and Dell EMC.

Affordable

Keep costs low with no hardware to purchase and minimal overhead required

Contact Dell

Datasecurity@dell.com
www.dell.com/datasecurity

Data loss means more than lost productivity

The digital universe is growing at an exponential rate and the amount of data in storage grows at a corresponding rate. Companies and individuals rely on data more than to enable the success of their business. Data loss continues to be a primary concern for IT professionals due to lost productivity and the high cost of data retrieval. The cost of a data loss episode impacting hardware devices is estimated at approximately $2,450, assuming the data can be retrieved. Episodes of data loss that compromise data records can run into millions of dollars, depending on the data loss episode and the industry under consideration. Robust security and backup protocols, when employed, may go a long way in reducing the costs associated with data loss episodes.

Impact of data loss

As corporations rely more and more on bits and bytes, and less on bricks and mortar, data value continues to increase. Lost data can lead to costly downtime, lost productivity, and long-term reputational damage. The economic losses are significant. A 2013 survey (Ponemon Institute) of 277 data loss incidents reports that the average data loss incident for a U.S. corporation costs $5.4 million.

Small businesses may be especially vulnerable. Another study Eddy, 2013 reports that small business owners pay little attention to data backup, with most businesses reporting more time spent on changing passwords than backing up data. With less margin for error, even short periods of downtime can drive a small organization out of business.

Households also suffer when experiencing data loss episodes. Hardware failure rates appear to be on the rise, even with the increasing use of more reliable solid state drive (SSD) devices. Increasingly, households now comingle personal and business data, and a lost data episode at home can impact a business process at work. One survey reports that the average commuter takes 470 GB of company data home every day (Mozy, 2014).

The cost of lost data depends upon the nature of the data loss episode, as well as the value attributed to data. In addition, there is a cost associated with recovering the data and lost productivity. Additional costs may also be relevant, including increased liability, regulatory costs, and reputation loses. This study attempts to categorize and quantify the different costs associated with data loss episodes.

Growing reliance on stored data

The amount of data stored continues to grow. Researchers from the University of Southern California estimate that data storage rates grew at an annual rate of 23 percent from 1987 to 2007 (Hilbert and Lopez, 2011). The authors estimate that more than 300 billion gigabytes have been digitally stored since 1987. Researchers at IDC estimate that the "digital universe," which includes everything that is created, replicated and consumed in any given year, doubles every two years. They estimate that by 2020 the digital universe will include about 5,200 GB per person, worldwide (Gantz and Reinsel, 2012).

This data explosion can be explained by increased storage media capacity (Moore's law), with the corresponding decreasing storage media costs. In 1980, the average cost per gigabyte was $437,500, while in 2014 a gigabyte could be purchased for 3 pennies. During the past 30 years, gigabyte storage prices have halved every 14 months (Statistic Brain, 2014). This has led to an information-reliant global economy, where information technology plays a central role within businesses,
organizations, and households.

Trends in data storage

The primary focus of this study is data loss episodes that impact devices. Over the last several years there has been a dramatic shift in the devices we use for data storage. The primary trend has been a movement away from relying on PCs and laptops, towards tablets and smartphones. IDC (2014) forecasts that by 2017 nearly 90 percent of connected devices will be tablets and smartphones.

Data is stored in a myriad of places, from portable USB drives to data centers in the cloud. With the explosion of the digital universe, it is not surprising that the primary challenge reported by IT storage managers is overseeing storage growth (EMC, 2014). For IT professionals more generally, data loss is the greatest fear, with 68 percent indicating in a recent survey that it will be their primary challenge over the next 12 to 18 months (Iron Mountain, 2014). As the volume of data increases exponentially, organizations struggle to archive information and protect it from data loss, all while working within constrained budgets.

Changing business processes add complexity in some industries. In health and financial services, organizations are moving to paperless environments, removing data from the "back office" to the "front office," where value-added and ubiquitous computing requires even greater levels of data storage and protections. Today's employees use an average of 3.5 devices in the workplace (iPass, 2012), adding to data storage and security challenges for IT managers.

Causes of data loss

In the global study (Ponemon, 2013) on data loss examined 277 cases of large data loss episodes. This study found almost equal distribution among malicious or criminal attack (35 percent), hardware or software failure (29 percent), and human error (29 percent). The causes of data loss depend on the storage device. A review of the literature reveals the following reasons for data loss on devices, ranked from most to least prevalent:

- Hardware failure
- Human error
- Software corruption
- Computer viruses
- Natural disaster

Hardware failure accounts for approximately 57 percent of data loss episodes, while natural disaster is approximately 3 percent. This list does not include theft or simply losing a device, two significant categories of data loss discussed below.

Cost of a data loss incident

When an episode of data loss occurs, there are two outcomes: the data is recoverable or lost forever. With robust backup solutions available to consumers and businesses alike, permanent data loss is avoidable, except in cases of major natural disaster. Unfortunately, the data shows that backup and recovery solutions are often missing, which can lead to permanently lost data. Indeed, in a study by Mozy (2012) reveals that the average consumer loses 1.24 devices per year, but the majority of survey respondents are more upset about losing their data than their device.

The major costs of recovering data include lost productivity and the cost of retrieval. When there is no physical damage to the hardware, which encompasses about 40 percent of data loss episodes, data may be recoverable by using in-house IT support. When outside

expertise must be sought, about 60 percent of the cases, the cost of data recovery varies, depending on factors related to the cause of damage, the severity, time sensitivity, as well as the type of storage media.

The authors surveyed eight separate data recovery companies in November 2014 on the estimated cost of recovering a hard drive. Price estimates varied from $300–$4,000 depending on the vendor and the factors noted above, most notably the severity of the damage, and the required turnaround time. For standard recoveries, the majority of estimates ranged from $400–$2,250. By taking the midpoint of this range as a reasonable approximation, the average cost of recovering data on a hard drive is $1,325.

When data can be recovered with in-house IT support, one must estimate the internal resources deployed in the recovery effort. If a computer support specialist is employed within the company, the number of hours needed to recover the data and the cost of employing this individual must be taken into account. The Bureau of Labor Statistics reports that the average computer support specialist currently earns $44.90 an hour, including salary and benefits. Assuming that the average time needed to recover lost data is approximately eight hours, the cost of using an in-house employee to recover lost data is approximately $360.

When we incorporate the expected probability of whether the data can be recovered in-house or outsourced, the expected average cost to retrieve data is calculated at $950.

The $950 estimate only includes the cost of recovering a hard drive. An important consideration with any data loss episode is lost productivity. Every device user is familiar with the frustration and downtime often associated with a data loss incident. In addition, if others within the organization must rely on the data that is lost, there is a "contagion effect" from a data loss episode. The productivity of others, and indirectly company sales, are likely to be impacted. In order to estimate these costs the following must be considered: the individual's productivity, the length of the downtime, and the extent to which an individual's data loss episode affects others in the company.

During data retrieval an individual is unable to access his or her device and data, which results in lost productivity. This opportunity cost, lost productivity due to downtime, impacts a company's bottom line just like out-of-pocket costs for data retrieval. How do we measure this? Economic theory says that an employee's productivity can be approximated using an individual's compensation. According to the Bureau of Labor and Statistics, the average worker earns $43.66 per hour in total compensation.

Each data loss episode is unique and the time needed to recover data may vary from less than one hour to several days. Most workers do not have their productivity reduced to zero, as they could shift to different tasks. This study assumes a productivity reduction of 50 percent.

Costs can rapidly accumulate when we consider the contagion effect; that is, when one individual's downtime impacts others within the company. This likely occurs in any collaborative work environment or where individuals share access to data, certainly not uncommon scenarios. Precision in estimating the contagion effect will depend on various elements, but a conservative estimate suggests that data loss would impact three other co-workers, reducing their productivity by 25 percent each.

Another element to consider is the downtime interval, which will hinge on whether the device needs to be sent to an outside vendor or whether the data can be retrieved in-house. For outside recoveries, survey data suggests a five-day turnaround as typical, including time needed for transport. Earlier, we estimated the time needed for in-house recoveries to be eight hours. The result of combining these expected probabilities and scenarios is an average productivity loss estimate of $1,500.

Adding together the expected cost of data recovery ($950) to the expected loss of productivity ($1,500), we calculate an average cost of a data loss episode at $2,450. Once again, this assumes that the data are retrievable.

Permanent and large-scale data loss

The above analysis relegates data loss to a single device and ignores large scale data loss episodes on corporate servers, data breech events, and incidents when data are permanently lost.

Some industries may carry an especially high risk for data loss, due to heavy reliance on data, the intrinsic value of data, as well as regulatory costs. The Ponemon Institute (2014) estimates the annual costs to hospitals of compromised data to be $5.6 billion, with each healthcare organization it studied suffering about $1 million in data loss costs per year. Unsecured devices under BYOD and employee carelessness were identified as the chief causes of data loss. The average

number of lost or stolen records per event was 2,150. They report the average cost per stolen record at $188. Thus, a typical data loss event could have a financial impact of more than $400,000.

Financial organizations may also be especially vulnerable. Crosby (2014) reports in a survey of nearly 4,000 financial organizations, the cost of lost financial data ranged from $66,000 to $938,000 per organization, depending on the size of the company. Organizations may be fined for losing records, or having client records compromised, thus legal and regulatory costs should be included in the analysis. If a data breech has criminal activity associated with it, forensic analysis may be costly. The cost of lost reputation (for example, the discount retailer Target data breech) may have long-lasting repercussions.

We have not incorporated consideration of the cost of replacing hardware, which must occur when hardware damage occurs or a device is lost or stolen. As noted earlier, most individuals lose at least one device a year. The cost of hardware, even expensive hardware, may pale in comparison to the value of lost data.

Finally, it may be that valuable intellectual property may be lost forever, rendering the value of a data loss episode extraordinarily costly. This highlights the need for data storage and backup solutions, which are highly cost-effective and inexpensive insurance for organizations and individuals alike.

Conclusion

Data loss episodes are common, and they represent a problem for companies large and small. As the amount of stored data grows, data loss has become more prevalent over time. Companies must take the necessary steps to ensure that their data is securely backed up, accessible, and easily recoverable. Mozy cloud backup is a cost-effective way to protect your valuable data. Simply choose the service level that allows you to back up as many computers and servers as you like. For more information, visit Mozy at www.mozy.com.

References

Bureau of Labor Statistics, Occupational Employment and Wages, May 2013.

Columbus, Louis, "IDC: 87% Of Connected Devices Sales By 2017 Will Be Tablets And Smartphones," Forbes, September 12, 2013, http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones/.

Crosman, Penny, "How Much Do Data Breaches Cost? Two Studies Attempt a Tally," American Banker, September 12, 2014.

Eddy, Nathan, "Small Businesses Unprepared for Data Loss, Lack Backup Policies," eWeek, November 14, 2013.

EMC, "Managing Storage: Trends, Challenges, and Options, 2013-14," https://education.emc.com/content/_common/docs/articles/Managing_Storage_Trends_Challenges_and_Options_2013_2014.pdf.

Gantz, John and David Reinsel, "The Digital Universe in 2020," IDC, December 2012.

Hilbert, Martin and Priscila Lopez, "The World's Technological Capacity to Store, Communicate, and Compute Information," Science, April 2011.

IDC, IDC Worldwide Quarterly SCD Tracker, June 17, 2014, http://www.idc.com/getdoc.jsp?containerId=prUS24935114.

iPass, "The Global Mobile Workforce Report: Understanding Mobility Trends and Mobile Usage Among Business Users," 2012.

Iron Mountain, "The Cost of Inertia: Insight from the Iron Mountain Data Predictors Study," 2014.

Mozy, "Lost and Found," http://mozy.com/about/news/reports/lost-and-found/, 2012.

Mozy, "The Daily Commute," http://mozy.com/about/news/reports/the-daily-commute, 2014.

Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," May 2013, http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis.

Ponemon Institute, "Fourth Annual Benchmark Study on Patient Privacy and Data Security," March 2014, http://www2.idexpertscorp.com/ponemon-report-on-patient-privacy-data-security-incidents/.

Statistic Brain, "The Average Cost of Hard Drive Storage," November 11, 2014, http://www.statisticbrain.com/average-cost-of-hard-drive-storage/.