



---

Annie Searle & Associates LLC

## Research Note

# Data Loss and Business Responsibility

By Emily Oxenford

Copyright © 2011, ASA Institute for Risk & Innovation

*Keywords: Data Loss, Risk Management, Business Continuity, Risk Planning*

**Abstract:** The vast amounts of data being created, edited, stored, transported, and analyzed on a daily basis is astronomical. For businesses, more and more critical services and products are driven by and complete dependent on data. With a growing quantity of data and expanding risks to data, a business must be increasingly protective of data, ensuring that neither business operations nor customer data are compromised.



---

Annie Searle & Associates LLC

## Introduction

The vast amounts of data being created, edited, stored, transported, and analyzed on a daily basis is astronomical. For businesses, more and more critical services and products are driven by and complete dependent on data. With a growing quantity of data and expanding risks to data, a business must be increasingly protective of data, ensuring that neither business operations nor customer data are compromised.

But many businesses are not addressing the issue of data loss, a risk that could not only severely damage a business but could even close it down for good. A study done a few years ago found that nearly half of IT and compliance professionals said that “their organizations are doing an inadequate job of lowering the rate of data loss” and that they would be unable to notify users and customers of a data breach.<sup>1</sup> From the same research study, it was found that most of the 1,000+ people surveyed felt that their organizations did not possess “the necessary security tools or internal controls to prevent, detect, and correct data security breaches.” This is a serious problem that highlights the need for businesses to consider the serious problem that data loss represents.

## Responsibility

In order to account for responsibility, it is important for a business to determine to whom they are responsible. For the purposes of this discussion, this research will assume an obligation of responsibilities to employees, customers, community, and shareholders. These four groups are all part of making or breaking the success of a business, and therefore there is an obligation towards them from an organization’s perspective.

A business has an obligation to protect its customer data (from things such as loss, fraud, and theft). An organization may also be said to owe its customers and stakeholders clear communication about the status and use of data. In certain sectors, such as finance, there are legal obligations that require communication to customers when data has been lost or compromised. But in sectors where there are little or no legal obligations for compliance, it is often left to the business to self-regulate. This self-regulation certainly benefits a business in general (poorly handled data will likely result in loss of reputation, finances, and business), but it is sometimes tricky to implement full preventative measures without the government or legal

---

<sup>1</sup> Gaudin, Sharon. "IT Managers Say Risk of Data Loss Is Bad and Getting Worse". InformationWeek.com 18 June 2007. Accessed <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199905013>.

incentives. There are many decisions to be balanced in a business - the protection of data should be incorporated into both policy and practice to ensure priority.

## Data Loss

There are three trends<sup>2</sup> that have been identified as reasons for why data loss is a rising issue among businesses, even though there is also an increasing awareness about the critical nature of protecting an organization's data.

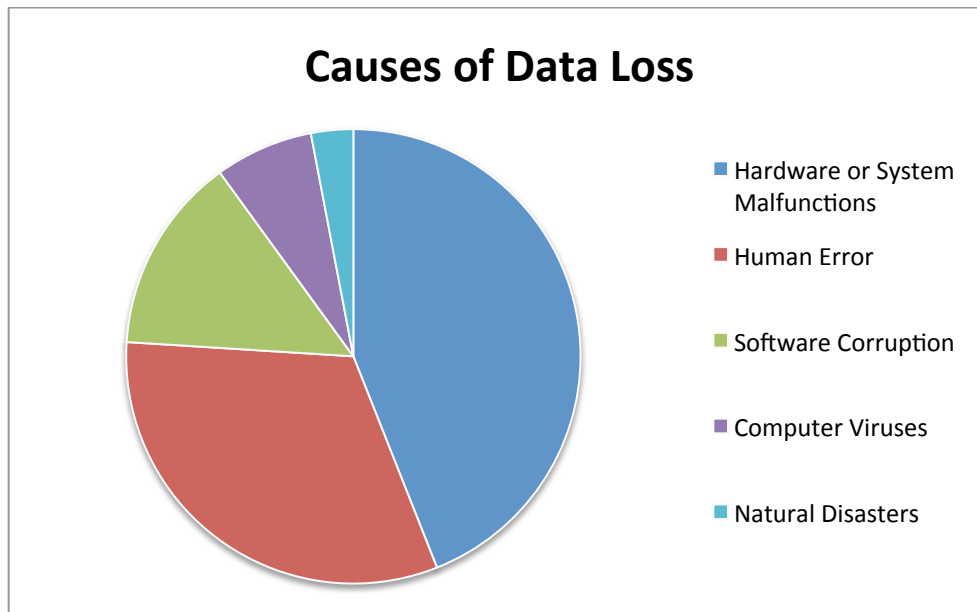
- There is an increased storage capacity for data in fewer devices and for less money. This means that while businesses can afford to store more and more, the repercussions of that storage being compromised are significantly higher.
- There are so many types of information that are being recorded and stored in digital formats. In the information age, we see that data has become key to business operations and services. The loss of this data can have devastating results on a business, and either cripple or kill the future of a company.
- The ability to backup and recover data is increasing, but the tools and methods are not always perfect. People sometimes rely too heavily on the software or hardware to ensure the complete, frequent, and healthy (non-corrupted) backup of data.

It is important to understand how data loss can occur. According to research done by the Protect-Data.com, there are five main causes for both an organization and individual to experience data-loss.

<b>Hardware or System Malfunctions (44%)</b>	<b>Human Error (32%)</b>	<b>Software Corruption (14%)</b>
<ul style="list-style-type: none"><li>• Electrical failure</li><li>• Head/media</li><li>• Controller failure</li></ul>	<ul style="list-style-type: none"><li>• Accidental deletion</li><li>• Accidental drive format</li><li>• Damage by drop or fall</li></ul>	<ul style="list-style-type: none"><li>• Corruption caused by diagnostic or repair tools</li><li>• Failed backups</li><li>• Configuration complexity</li></ul>
<b>Computer Viruses (7%)</b>	<b>Natural Disasters (3%)</b>	
<ul style="list-style-type: none"><li>• Boot sector viruses</li><li>• File infecting viruses</li><li>• Polymorphic viruses</li></ul>	<ul style="list-style-type: none"><li>• Fires</li><li>• Floods</li><li>• Brownouts/Lightening Strikes</li><li>• High Winds</li></ul>	

<sup>2</sup> Adapted from "Statistics About Leading Causes of Data Loss". N.D. *Protect-Data.com*. Accessed from <http://www.protect-data.com/information/statistics.html>

These different causes are not comprehensive, but certainly represent many of the different threat sources a business must consider when preparing for the increasingly common risk of data loss.



## Prevention Measures

There are a number of steps to ensure that data is protected, both during day-to-day operations and during a disaster or crisis. Adapting these measures to fit the business context and needs should be considered an important part of any risk planning.

### Technical Safeguards

A number of important recommendations for the protection of data come from the PCI DSS (Payment Card Industry Data Security Standard), which deal with the protection of data in the credit-card industry. These are not limited to this particular industry, and in fact can be adapted into any business where data is created, edited, and moved. A challenge for many businesses is limited financial and personnel resources to dedicate to the implementation of preventive safeguards, but the investment can result in a significant payoff if disaster does strike.

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored data
- Encrypt transmission of data and sensitive information across public networks

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to data
- Track and monitor all access to network resources and data
- Regularly test security systems and processes
- Maintain a policy that addresses information security policy

## **Business-Practice Safeguards**

It is not sufficient to implement technical safeguards and assume that the system will be enough to protect data. Planning for risk as a whole needs to be part of business culture and practice. As part of risk management, the following safeguards<sup>3</sup> can help address not only data loss, but help in other risk areas within a business.

- Internal company review of policies, procedures and controls. Knowing the existing state of these is one of the first steps of identifying and closing gaps in a business.
- Third-party review of policies, procedures and controls. An outside perspective is often necessary for painting a complete picture, but ownership and responsibility is not transferred.
- Identify standards that third-party vendors must meet. The risk of data-loss is not limited to internal practices, and communicating with partners and vendors can be key to mitigating risk.
- Company-wide awareness and training program. This is important for making risk planning and prevention part of business culture and practice.

## **Conclusion**

Keeping in mind the increasingly critical nature of data to businesses and their customers, it is equally as important to prioritize the protection of said data. Businesses need to not only protect data but in the event of its loss, take up the responsibility to recover, restore, and replace it as they are able as part of their responsibility to stakeholders. Strong prevention is key, though, in reducing the threat of data loss in the first place.

---

<sup>3</sup> Adapted from "Enhanced Security Policies and Procedures". *BNY Mellon*. N.D. Retrieved from: <http://www.bnymellon.com/tapequery/security.html>



---

Annie Searle & Associates LLC

### **Works Cited**

"Enhanced Security Policies and Procedures". *BNY Mellon*. N.D. Retrieved from:

<http://www.bnymellon.com/tapequery/security.html>

Gaudin, Sharon. "IT Managers Say Risk of Data Loss Is Bad and Getting Worse". *InformationWeek.com* 18 June 2007. Retrieved from:

<http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199905013>.

Leppik, Peter. "To Whom Does an Ethical Business Owe a Responsibility". Blog Dispatches from the Frozen North. 24 Feb 2004. Retrieved from:

<http://www.frozensouth.org/C1848698620/E2013508927/index.html>

"Statistics About Leading Causes of Data Loss". *Protect-Data.com*. N.D. Retrieved from:

<http://www.protect-data.com/information/statistics.html>

Zoladz, Chris. "Why PCI Compliance Is So Confusing: You Too Can Take Charge!". By NYMITY, February, 2011. Retrieved from:

[http://www.nymity.com/Free\\_Resources/Privacy\\_Interviews/2011/2011\\_Chris\\_Zoladz.aspx?](http://www.nymity.com/Free_Resources/Privacy_Interviews/2011/2011_Chris_Zoladz.aspx?)