COST OF A DATA BREACH

EXECUTIVE SUMMARY

Whether in business, education, finance, healthcare or any other type of industry, data is being abused in every organization around the world. According to a study carried out by Ponemom Institute in 2010[1], the total costs resulting from data breaches reached $6,751,451 in the US in 2009. And with every year, the number steadily grows.

The harm caused by data breach incidents, however, goes far beyond monetary expenses. It leads to indirect losses, such as losing the customers' trust, losing a good reputation, and the worst scenario: losing the whole company and undergoing bankruptcy. The costs resulting from a single data breach continue to increase as years pass by, and companies have to face the consequences, both direct and indirect.

[1]"2010 Global Cost of a Data Breach". Revised: April 19, 2010. Ponemon Institute LLC

CONTENTS

1 Introduction 4

2 Cost of Data Breach 5

2.1 Cost of Data Breach According to Country 5

2.2 Cost of Data Breach According to Industry 6

3 Direct Costs: Tip of the Iceberg 7

4 DLP Solutions: Are they worth it? 7

5 Conclusion 8

6 References 9

1 INTRODUCTION

Though data breach is for companies a very costly issue, it can be very hard to determine the exact scope of the damage. In some parts of the world, companies are not by law obliged to report data breach incidents, while in others they should always report them – they must announce data breaches whenever customers' records are involved. And yet they might prefer to stay silent, especially when company's confidential information or intellectual property are involved, because such data breaches could often lead to weakening the company's position on the market, if accessed by a competitor.

Data breach incidents constitute very costly problems for organizations, and have a tremendous impact on the business as such. Figure 1 below is based on findings in a study carried out by Ponemon Institute in 2009[2]. It shows how the average per-record cost of a data breach continues to increase over the years from 2005 to 2009.

Average per-record cost of a data breach

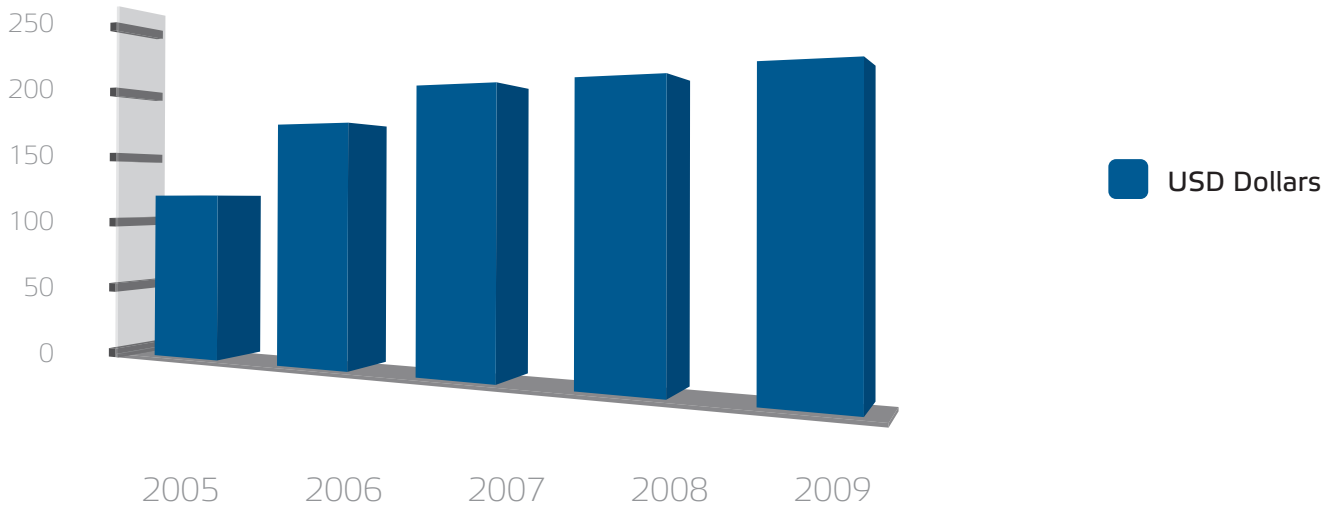

Figure 1 Average per-record cost of a data breach, 2005-2009

The cost has increased by $44 in only four years' time and it is very likely that it will continue to rise. You should also keep in mind that the numbers provided here are only given per-record. Data breach incidents, however, happen on a much larger scale and the total costs are in reality much greater. Costs huge as that put companies in a multi-layer jeopardy: The risk here does not include data security breaches only; the prosperity of a company is threatened as well.

The impact of a data breach does not only involve the direct loss of money that the company experiences after a data breach incident occurs, but also and perhaps even more importantly, it generates indirect losses that affect the prosperity of the business. Customers can simply lose the trust they had in the company after a data breach incident takes place, which logically leads to revenue losses. In the worst scenarios companies lose their place on the market and the business has to be wound-up. That's why it is most important to eliminate the opportunities for data breaches before they occur. When it comes to security, prevention is better than cure – it can save the corporation a lot of money and effort that is needed for the recovery process.

[2]"2009 Annual Study: Cost of a Data Breach". January 2010. Ponemon Institute, LLC

2 COST OF DATA BREACH

Data breach incidents happen on a large scale in every part of the world. Whatever the country or the type of industry is, companies report data breaches every single day. The average cost of a data breach varies according to the following criteria:

2.1 Cost of Data Breach According to Country

The total cost of a data breach was studied in five countries: The United States, The United Kingdom, Germany, France and Australia[3].

Total cost of a single data breach by country

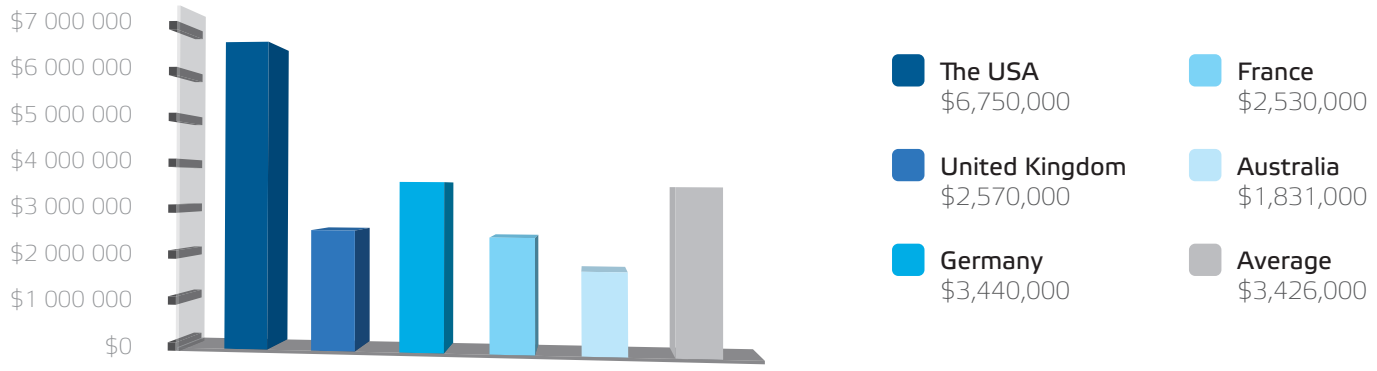

Figure 2 Total cost of a data breach

The average cost in these countries reaches $3,440,000 million. This huge amount of money shows what a single data breach incident would cost. Several breaches can be fatal.

It is also clear that most data breach incidents occur in the US, followed by Germany, UK, France and Australia. However, this ranking is directly linked to the population size; the largest number of people lives in the US. The following figure shows the population size in these countries in 2011, along with the total cost of a data breach.

Population and total cost of a data breach

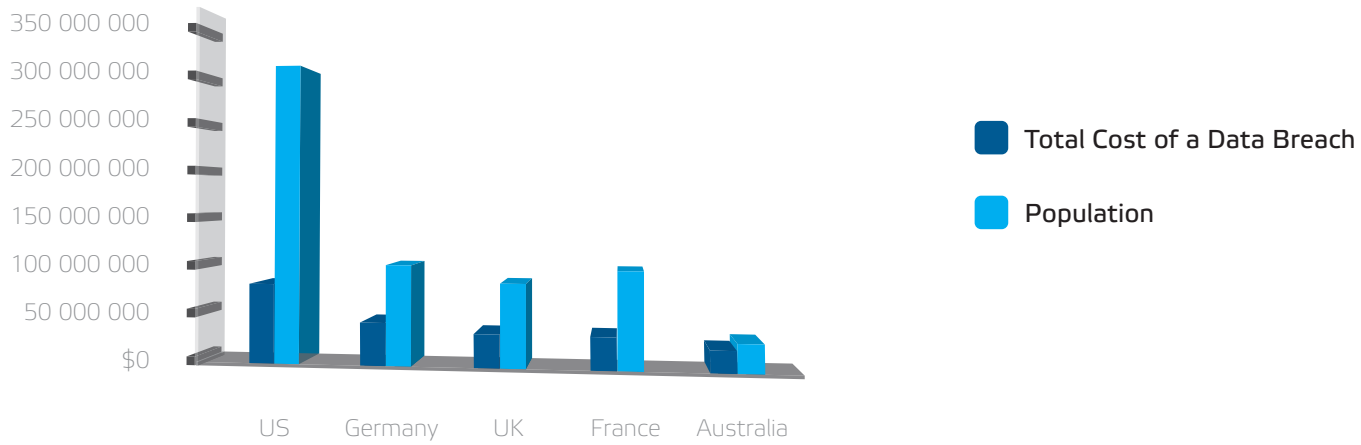

Figure 3 Population and total cost of a data breach

[3]"Five Countries: Cost of Data Breach". Revised: April 19, 2010. Ponemon Institute LLC

2.2 Cost of Data Breach According to Industry

The cost of data breach is also connected to the type of industry. Still, companies in nearly any industry are highly vulnerable to data breach incidents. A study conducted in September 2009[4] confirms this. The following figure shows findings of the study.

The percentages of data breach incidents in various industries in 2009 (January-June)

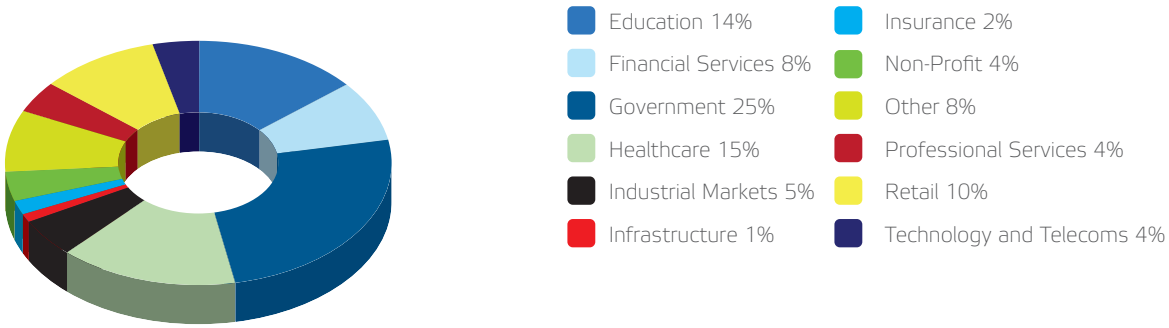

Figure 4 the percentages of data breach incidents in various industries in 2009 (January-June).

Also, the cost of a data breach differs in relation to the type of industry. According to a study carried out by the Ponemon Institute in 2009[5], the infamous prime hold the health related sectors, including pharmaceutical industry with $310 and healthcare with $294. The following table shows the costs resulting from compromised records in different types of industries.

Type of Industry	Cost of Compromised record
Pharmaceutical	$310
Healthcare	$294
Research	$266
Services	$256
Financial	$249
Energy	$237

Table 5 Cost per incident including compromised records in various industries

[4]"Data Loss Barometer, Insights into lost and stolen information in 2009". Issue 2.2009 KPMG International.
[5]"2009 Annual Study: Cost of a Data Breach". U.S. January 2010. Ponemon Institute, LLC.

3 DIRECT COSTS: MERE TIP OF THE ICEBERG

Data loss incidents cause many problems that go far beyond monetary losses. Once a company loses its sensitive data, it has to prepare for the harsh blow that such loss brings. Below are listed some of the consequences that companies can expect after a data loss incident occurs:

- Direct and Indirect monetary losses.
- Loss of customers' loyalty and the trust they had in the company.
- Loss of a good reputation on the market.
- Lawsuits filed against the company.
- Bankruptcy.
- Winding-up the business.

A recent incident of data breach took place in August 2010. The UK branch of Zurich Insurance plc was fined £2,275,000 by the Financial Services Authority (FSA). The FSA blamed the branch of not having sufficient security systems in place that would be capable of preventing the incident. It was the largest fine that the FSA has ever imposed on a single company for data security failure so far. The branch lost 46,000 customers' personal details, and what made the problem even worse was that the company was unaware of the incident until a year later.

Because of this incident, Zurich Insurance plc had to pay a tremendous amount of money, the company lost its good reputation, and as a result the customers' were no longer loyal to this company. They doubted that their data will be safely stored. After the incident, the UK branch of Zurich Insurance plc is adopting the necessary measures that are going to prevent such incidents in the future. Stephen Lewis, the Zurich Insurance UK chief executive, said 'It served to remind us of the need to strive continually to improve the ways in which we seek to protect customers' data[6].

UK Zurich Insurance branch realized – perhaps too late – the necessity for a robust data loss prevention solution that would protect their sensitive data. These incidents often serve as a wakeup call for the victimized companies, and also for other: People finally realize that there are a few critical steps companies must take in order to ensure complete security of their systems and safe data storage.

4 DLP SOLUTIONS: ARE THEY WORTH IT?

Data loss prevention (DLP) solutions are much more than traditional anti-virus software or other security tools that keep data safe from outside attacks. DLP solutions can help you keep your sensitive data safe from any internal abuse or unauthorized access. It also reveals any undesirable employee behavior inside the company. All in all, a DLP solution prevents data breach incidents before they actually happen, which eliminates information leaks and the subsequent losses.

Endpoints should be the priority number one, when it comes to data loss prevention. Your network may be protected against attacks from outside, but what about internal threats? Many employees working for various corporations operate on desktops or laptops, which they quite frequently take to distant places that are beyond the network's range. Data on these portable devices get lost very easily. Any reckless or even malicious behavior concerning this data will pass undetected, because there is no security tool watching over these endpoints. Data can leak through USB devices, CD/DVD drives, the internet, and via Bluetooth or wireless LANs to other networks.

Data's real worth is underestimated and sometimes even overlooked by today's companies. Only after a major data breach incident occurs do they realize the enormous value that data have. Companies' confidential data lose their value once they are publicly available. This is often followed by catastrophic consequences and sometimes can even lead to the liquidation of the business. The fact is that the value of a company is measured by the value of its data. This statement applies to businesses across a number of industries. Data Loss Prevention solutions are necessary; they can save companies huge amounts of costs, direct and indirect, that would have to be covered if a data breach incident took place. With the continually increasing number of data breaches reported,

[6]"Zurich Insurance hit with record fine over data loss". David Meyer. August 2010.

DLP solutions are becoming an essential part of every security system within every single organization. Some of the benefits that a DLP solution provides are listed below:

Benefits of a DLP Solution

Gain

- Full visibility of the stored, in use and transferred data
- Clever detection and classification of sensitive data
- Early detection of any data loss incident

Prevent

- Data breach through any type of media
- Loss of reputation and loss of customers' trust

Reduce

- Data breach costs to a minimum
- The insider threat caused by employees to a minimum

Keep

- Compliance with data protection regulations
- A solid place in the business market
- The management aware of any incidents immediately as they happen
- Complete supervision of employee's behaviour
- Awareness amongst employees that the data they are dealing with is under maximum security

Organization should take strategic security measures that will reduce the cost of data breach and prevent data vulnerability by installing and using data loss prevention solutions. These solutions watch out for internal threats, which are the major cause of data breach incidents.

5 CONCLUSION

Companies need to realize that without a DLP solution, they are not protected from data breach. The question is not whether a data breach incident will take place, but rather: When is it going to strike? Whenever a data breach incident occurs, companies have to cover huge expenses.

What most companies usually underestimate are indirect losses, such as the loss of customers' trust, loss of a good reputation on the market, the money spent on combating lawsuits. And yet, this often results in bankruptcy and business liquidation. Companies with no security measures preventing data breach are playing with fire.

Data Loss Prevention solutions complemented with other security software like monitoring systems etc. contribute to preventing data breach, they eliminate all connected direct and indirect losses and avoid all the consequences that would otherwise follow.

6 REFERENCES

- http://web.interhack.com/news/n2009/taxonomy
- http://www.information-age.com/channels/security-and-continuity
- https://www.infosecisland.com/blogview/3983-Education-Sector-is-Failing-Security.html
- http://www.telegraph.co.uk/news/newstopics/politics/1574687/Governments-record-year-of-data-loss.html
- http://findarticles.com/p/articles/mi_m0FOX/is_9_4/ai_54530433/
- http://www.solutionmatrix.com/return-on-investment.html
- http://www.solutionmatrix.com/tco-roi-cba-difference.html
- http://www.deepspar.com/wp-data-loss.html
- http://www.rbs2000.com/index.php?cat_id=103&nav_tree=179,103

Prague | Czech Republic | Europe | 15th of April 2011