ROI OF SAFETICA

safetica®

EXECUTIVE SUMMARY

The current business environment requires cost optimization. As high effectiveness as possible is a must for every company that wants to keep its competitive edge and operate successfully on a long-term basis.

Personnel costs generally account for a major part of a company's operating expenses. Tools bolstering up employee efficiency are being broadly implemented in places where we need to improve profitability and support business growth.

Huge amounts of data which companies handle and process every day need to be protected, as their loss can lead to severe business and financial damage.

Safetica addresses both these issues with its unique combination of employee monitoring and DLP features.

CONTENTS

INTRODUCTION

Nowadays, employees and data belong to the key aspects driving successful operation of a company in the long run. And therefore, both must be closely watched and carefully handled.

Data leaks of various kinds may cause fatal consequences for a business. What most employers fail to realize is that their own employees represent the most dangerous factor affecting data security.

However, data breach is not the only way employees are likely to harm their companies. Wasting time at work is another serious threat companies must combat. Employees often waste several hours a week on personal matters, while they should be focusing on their work-related tasks.

When calculating the Return on Investment into Safetica, solution delivered by Safetica Technologies, one must explain the benefits it provides to its users.

Safetica covers all of the above mentioned issues and offers more than just a solution.

1 PRODUCTIVITY MONITORING – THE IMPACT OF DEPLOYING SAFETICA

Productivity Monitoring and Blocking features of Safetica bring about several benefits which lead to a direct decrease of operational costs and hence to improved profitability; and – if followed up by HR measures – it also encourages better trained, more competitive and efficient workforce.

1.1 Higher Employee Effectiveness

One of the key issues the Safetica solution targets is inefficient employees, i.e. employees who tend to waste time on their PCs during working hours. Nowadays "office" employees often let themselves be distracted from their work-related tasks and they go on to surf the Internet, play PC games, shop on-line etc., and often this is just because they get the opportunity to do so.

A simple announcement informing employees that their activity at work is being monitored might prevent plenty of them from spending so much time on activities unrelated to their job. If announcing the fact that they are being watched fails to deliver the desired effects, HR management can take the next step: identify the workers who are wasting company resources and apply the following measures. First, block particular web-pages, social networks, games etc. Further, problem employees should be talked to individually, and if necessary, dismissed.

There is no doubt that these measures lead to a higher work efficiency as you can do the same amount of work with a smaller team or take up a heavier workload with the same number of employees.

The impact on a company's profit margin is evident. Cutting personnel costs but at the same time maintaining the same business size boosts profitability.

1.2 Identifying Malicious Employees

Furthermore, Safetica enables you to identify malicious or perhaps only negligent employees, and helps you prevent any harm they could cause. Usually, you can identify employees whose activity puts a company at risk because their behavior:

Threats the good reputation of a company and/or causes financial losses

The biggest threats include spams or worms sent as if by the victimized company, illegal downloading of software, sharing movies or music, or even propagating child pornography.

Indicates an employee is disloyal to a company

Which is when an employee is about to quit a company while the company has not yet been notified of this. What is even worse, employees sometimes work as spies for the competition. In that case, they are likely to steal sensitive data and/or know-how; misuse company assets and working time for private purposes.

According to the Gallup Management Journal survey, there are, typically, three kinds of employees:

- **Engaged** – employees who work with passion and enthusiasm; they are basically driving innovation and moving an organization forward; according to the survey, there are 27% of such employees.
- **Not engaged** – average employees who work rather without passion and energy, and fail to use their full potential; the biggest group, amounts to 59% of all employees.
- **Actively disengaged** – they are more than unhappy at work, they undermine what their Engaged co-workers accomplish; As much as 14% of all employees were found to belong into this category.

Safetica is able to identify employees who are likely to harm a company before any actual damage is sustained. It gives you time to create and apply necessary measures. Employees who once posed a threat can be better motivated, rotated or dismissed if necessary.

1.3 Restricting Wasteful Printing

Safetica provides information on the employees/departments printing activity. Further, those employees who do not require any printing privileges for their work may be prevented from printing altogether and/or company management can tag certain documents as blocked for printing. Again, implementation of Safetica leads to significant savings in this area.

2 THE ROI OF THE SAFETICA MONITORING FEATURES

Dollar quantification of the benefits which Safetica brings to a random company would certainly vary from organization to organization. The amount of both direct and indirect savings depends on the type and size of a business, relevant processes already implemented etc.

There have been several employee studies and surveys carried out on real data, the findings are alarming:

- 30 to 40% of total internet access is wasted on non-work related browsing, and a staggering 60% of all online purchases are made during working hours, according to a survey by International Data Corp (IDC)
- 25.5% of all workers said that working hours are the best time to conduct their personal activities online; surveyed by Burstmedia.com
- Employees who use Twitter and other social networks in the office are costing U.K. businesses more than $2.25 billion a year, according to London-based Morse PLC, an IT services and technology company (Morse).
- The popularity of social networking sites has grown substantially in the last few years. The side effect, however, is that the temptation to visit such sites during office hours has become a productivity black hole.
- 57% of surveyed employees admit to browsing social networking sites for their personal use while in the office; source: the Morse survey
- Those workers use social networks an average of 40 minutes a day at work, which adds up to a lost week each year, the Morse survey found.
- 77% of employees who have a personal Facebook account use it during their working hours. These are the results of a study by Nucleus Research, an IT research company in Boston.

Such behavior obviously leads to huge productivity losses. Businesses world-wide look to formulate and enforce policies that would encourage sensible usage of Internet access.

While we understand that short breaks within working hours are acceptable and may even improve one's efficiency, we are still aware of the threats hovering over company executives' heads. If an employee stretches

their once short break every day by few minutes, it will become a time consuming bubble causing productivity losses.

When calculating the ROI of Safetica productivity monitoring features, we estimate that employees waste on average 30 minutes a day on undesirable non-work activities. This estimate is based on results of the studies mentioned above. Our aim is to demonstrate how huge the impact of such negligibly looking amounts of wasted time can be when it comes to the whole company level.

Safetica enables you to identify and eliminate opportunities that allow your employees to waste time.

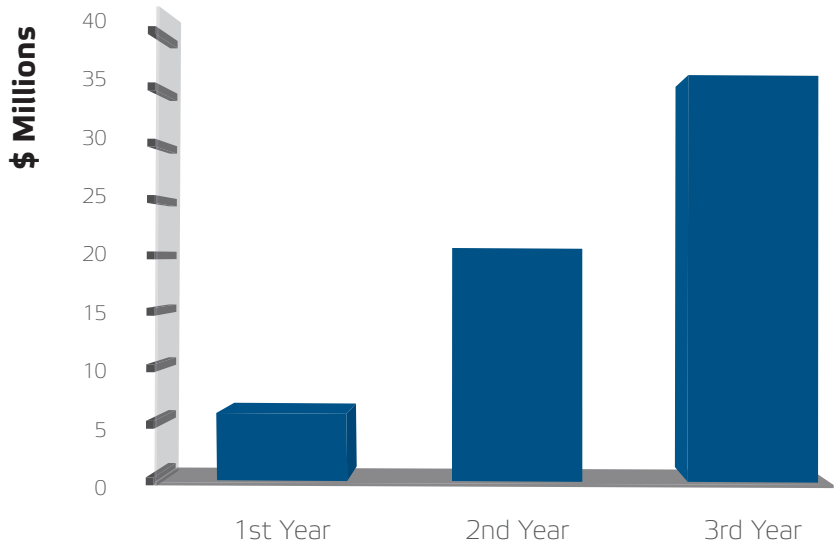
A company with 5 000 office employees may reach an increase in profitability of $36 million over a three year period, under these, rather conservative, assumptions:

- the company purchases a 3-year license of Safetica
- average personnel costs are $ 24 per hour per employee
- in the first year of implementation, we assume that only a half of the average yearly savings will be reached (Company management needs some time to apply the appropriate measures based on insights provided by Safetica. On the other hand, Safetica makes it possible for certain steps to be taken immediately.)

Savings per employee

Improvement in the work efficiency per day in hours	0,5	Headcount	5 000
		Average Personal costs per working hour in USD	$24
Working days per year	250	Hours wasted per year	125
Hours wasted per year	**125**	**Total savings to be reached every year**	**$15 000 000**

Cumulative Increase in Operating Margin



The impact on the company's operating margin over the three year period was calculated as follows: Personnel Costs Savings less Total costs incurred by implementing and maintaining the Safetica software.

In $ thousands	**0 Year**	**1st Year**	**2nd Year**	**3rd Year**
Savings in Personal Costs	0	7 500	15 000	15 000
Total Cost related to Safetica	1 194	57	57	57
Increase in Operating Margin	-1 194	7 443	14 943	14 943

The return on Investment was calculated as the Internal Rate of Return of the investment over a three year period. When calculating NPV, the costs of capital are assumed to be12%.

Discounted Cash-Flow	-1 194	6 645	11 912	10 636
NPV	**27 999**			
Internal Rate of Return	**699 %**			

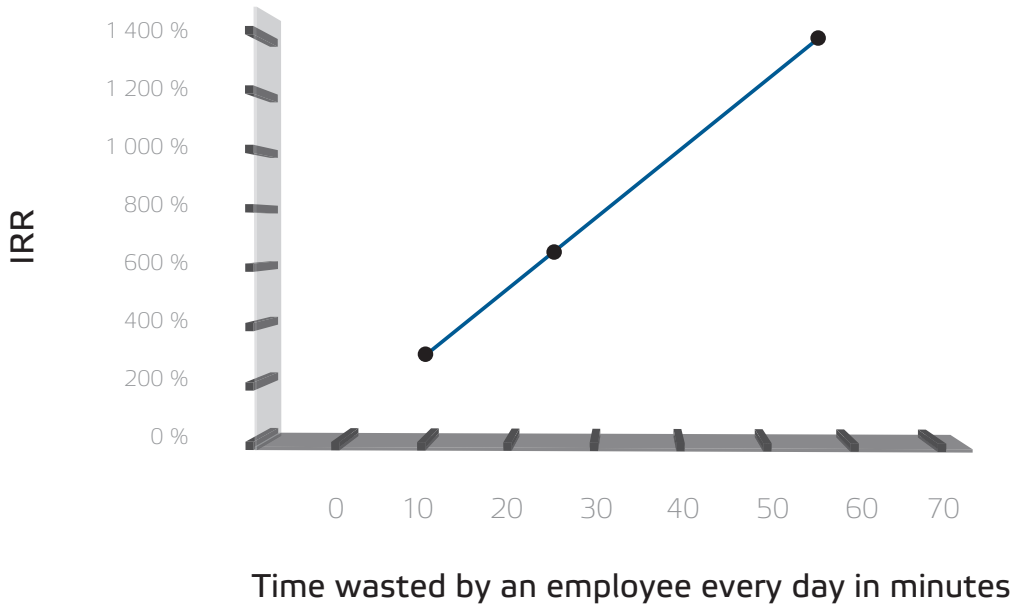
Do you know any other investment that generates an IRR of 700% p.a.? And don't forget, this is the direct impact of just the Safetica productivity monitoring and undesirable behavior blocking features. Extensive savings from the DLP features are not included in the calculation.

The impact on company profitability would be even greater if one was considering more than just 30 minutes per day as wasted by an average employee, or if a higher average wage was applied.

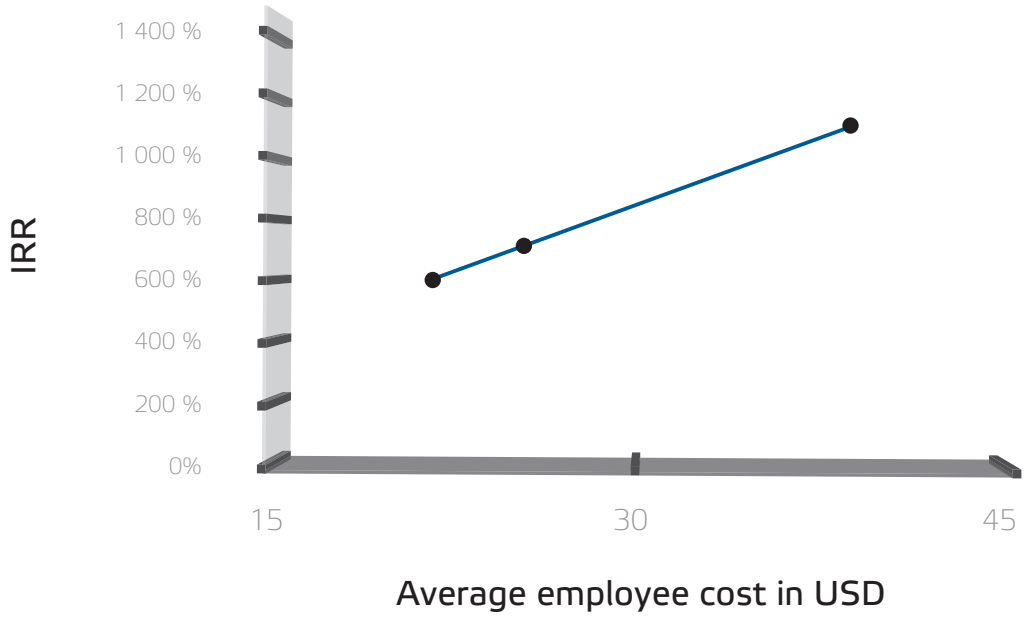
The following graphs illustrate the dependency of the IRR (i) on the amount of wasted time per day by an average employee; (ii) on an hourly wage (expressed as the total savings of personnel costs)

If we assume that an average employee wastes 60 minutes per day instead of 30 minutes, ceteris paribus, the IRR of Safetica exceeds 1300%. Vice versa, if we consider just 10 minutes as wasted, the IRR still goes beyond a fantastic 250%.

How does the Time Wasted by an Employee affect IRR



How does the Average Employee Cost affect IRR



If we assume that an average employee wastes 60 minutes per day instead of 30 minutes, ceteris paribus, the IRR of Safetica exceeds 1300%. Vice versa, if we consider just 10 minutes as wasted, the IRR still goes beyond a fantastic 250%.

3 SAFETICA DATA LOSS PREVENTION SOLUTION

Safetica does not only deliver a high-quality protection solution, it also embodies reliable prevention software. In fact, it can be perceived as a kind of insurance with the perfect Return on Investment –with only a small upfront investment, you will avoid huge potential losses.

Sensitive data are one of a company's greatest assets. If lost, they often cause serious financial harm, which in turn severely affects the very existence of a company. The origin and extent of the costs and/or damage is related to the kind of data lost. Data can be divided into three categories: Personal data, Know-how and Proprietary data.

3.1 Personal Data Losses

This group covers leaks of the sensitive personal data (incl. e.g. Social Security numbers, addresses, and card numbers) of customers, employees and third parties, whose sensitive data your company handles and is compelled to protect.
Whether it is a deliberate malicious action or mere negligence that causes a leakage, both ultimately incur severe direct costs, long-term indirect costs and future losses which can have infinite extent.

- Direct costs following a sensitive personal data leakage typically comprise:
- Detection, notification and ex-post response
- Legal representation
- Public relations and extra marketing expenses
- Indemnity – compensating the affected subjects

Indirect costs originate from various sanctions and requirements ex-post imposed by the state authorities:

- Regulatory fines/sanctions
- Further regulatory security and audit requirements

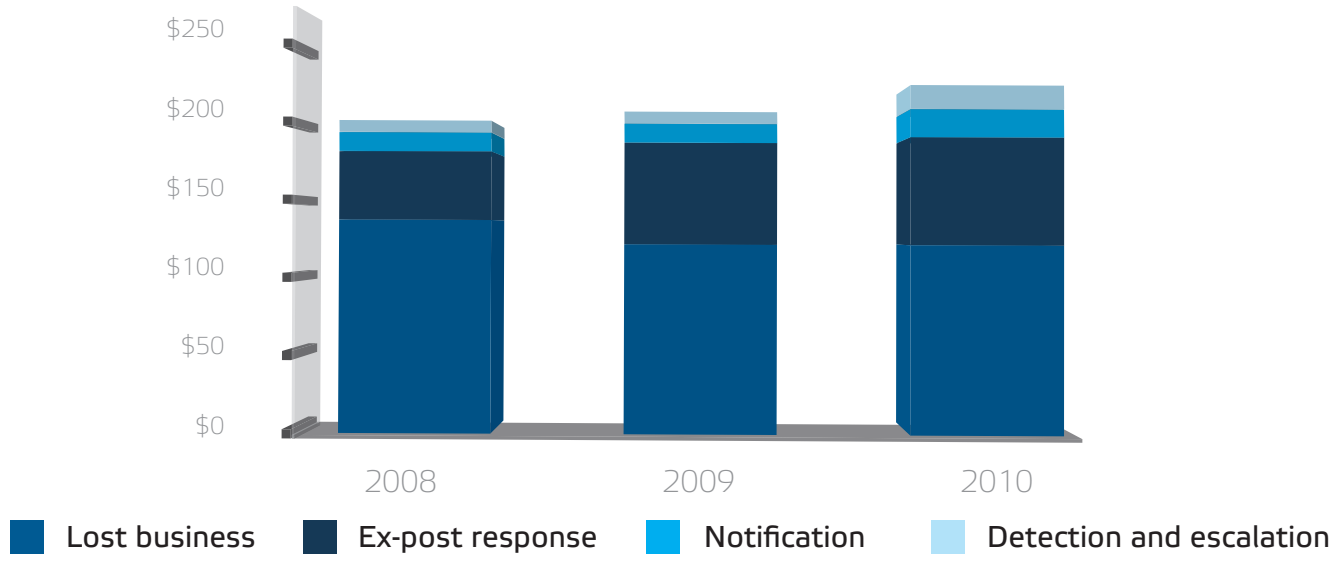
Potential future losses result from decreased demand (both current and future) mainly due to:

- the loss of the customer trust
- general damage of a company reputation

Ponemon Institute and Forrester Research have both carried out separate researches and analyses to calculate the Average Cost of a Data Loss Record. Both institutions arrived at a quite similar number. In 2010, the Average Cost of a single lost record reached $214 according to Ponemon Institute and $218 according to Forrester Research.

Ponemon calculated the direct costs as a sum of the expenditures associated with the detection of a leak and the response to it, plus diminished profit due to lost business (current and future customers).

The Components of Costs incurred by one Leaked Personal Record



Source: 2010 Annual Study UK Cost of a Data Breach by Ponemon Institute

Real case study I. - Data broker Choice Point

In 2004, the following data breach affected more than 160 000 U.S. residents.

- This data breach incident resulted in at least 800 cases of identity theft.
- A settlement and 2006 court order required the company:
- to pay $10 million in civil penalties and $5 in consumer redress,
- to maintain a comprehensive data security program,
- to obtain an independent assessments of its data security program every other year until 2026.

In 2008, another breach compromised personal data of 13 750 people.

- The Federal Trade Commission accused the company of failing to implement a comprehensive information security program which would have protected consumers' personal information.
- Choice Point agreed to pay $275 000 to resolve the FTC complaint.
- The court order requires Choice Point:
- to provide detailed reports to the FTC on how it is protecting the breached database and certain other databases and records containing personal information,
- to present a report every two months for two years.

Real case study II. - Countrywide Financial

- In 2008, a Countrywide Financial employee, senior financial analyst at Full Spectrum Lending, was arrested for stealing and selling customer data:
- For two years, he downloaded personal information of 20,000 customers each week and sold them to other mortgage brokers as sales lead.
- In total, 2 million people's identities, incl. Social Security numbers have been compromised.
- An agreement settling the matters was approved by a federal judge in Kentucky. Bank of America, which acquired Countrywide in 2008, decided to enter into this agreement in order to avoid additional expenses and uncertainties of further litigation.
- Based on the agreement, Bank of America Corp. is obliged to provide free credit monitoring, identity theft insurance and reimbursement for losses to as many as 17 million customers who dealt with its Countrywide Financial mortgage unit.
- The agreement has settled more than 30 lawsuits, including nationwide class actions.

3.2 Know-How Disclosures

The proprietary know-how of a company constitutes long-term competitive advantage and represents an essential base for a bright company future.

Revealing your know-how to a competitor or any third party means robbing yourself of this vital asset. Consequences which follow have inconceivable and inestimable extent.

What is more, know-how is much more vulnerable to leaks because it has an unquestionably high monetary value, which makes it a frequent target of malicious attacks or even ingenious espionages.

3.3 Disclosure of Proprietary Information

Proprietary data typically comprise strategic issues, such as financial forecasts, commercial data, price policy, product plans etc. Such data are of an outstandingly high value to your competitors. A deliberate or negligent leak of this data strengthens the position of your competitors and makes your share value fall. But that's still quite an innocent scenario because when it comes to proprietary data, it is often intentionally stolen and then sold to competition right under your nose. Your business falls apart, and without the proper tools, you will never find out who is to blame.

3.4 Trends in Data Breach Incidents

Following statistics were taken from the Ponemon study.

Data breach costs have continued to rise (five years in a row).

Data breach costs vary according to individual industry sectors. The highest costs are incurred in Communication and Financial sector ($380 and $353 respectively). The lowest costs were found in Public and Education sector ($81 and $112 respectively), which results from the limited impact on potential future losses.

Malicious or criminal attacks are causing more breaches. In 2010, malicious attacks were the root cause of 31 percent of all data breaches, which is a significant increase from 24% in 2009 and 12% in 2008. Malicious attacks come from both outside and inside of the organization.

Data breaches resulting from malicious or criminal attacks are the most expensive as

- a criminal is out to monetize his work; they are trying to profit from the breach,
- these breaches are harder to detect, the investigation is more involved and they are more difficult to contain and remediate.

Negligence is still the leading cause of data breaches at 41 percent.

4 IMPLEMENTATION COSTS AND OPERATION EXPENSES OF SAFETICA

There are three areas of costs Safetica – its implementation and operation – incurs:

4.1 Software License

The license represents the fee for the right to install and use the software. It also gives you the right to seek support from Safetica Technologies representatives and/or our partner companies. The fee can be paid annually or as a one-off payment for up to 3 years in advance, which brings about interesting discounts. The individual User price differs according to the number of licenses purchased (quantity discounts).

4.2 Implementation costs (first year)

The implementation of Safetica covers mainly installation and configuration tasks, both of which require cooperation and assistance of in-house IT employees. Typically, Chief Information Officer and other skilled IT security worker(s) are involved.

The implementation costs depend on how long the in-house IT specialist(s) are involved.

For 10 000 user licenses, Safetica Technologies estimates that the required time for implementation could reach around 1200 hours. We are talking about one-off expense.

	CIO	**IT Security Engineer**
Hours	90	1 120
Costs per hour	$70	$45
Total costs each per month	$6 300	$50 400
Total costs per year		**$56 700**

4.3 Administration and maintenance (every year)

This area comprises estimated costs of in-house IT employees who spend a particular amount of time administrating the system each month. It is to be spent every month. The following Safetica Technologies estimate applies for enterprise network with thousands of PCs.

	CIO	**IT Security Engineer**
Hours	4	100
Costs per hour	$70	$45
Total costs each	$280	$4 500
Total costs each		**$57 360**

5 COMPREHENSIVE CASE STUDY

Based on previous findings and real cases, we have simulated a comprehensive Case Study:

A global Insurance company, employing 60,000 people worldwide, decides to implement Safetica in its US offices, which include about 9,500 employees, after it experienced a leak of personal data which affected 40,000 of its customers.

- The FTC imposed a fine of $200,000 and requires regular security audits for 10 years.
- An annual security audit will cost the company $400,000 per year.
- The average cost of one breached record amounted to $353[1]; 40,000 breached records cost the company $14,120,000over three years.

By implementing Safetica, the company expects to reach over a 3 years period savings in areas of

- personnel costs – by decreasing the average time its employees waste surfing the internet by 30 min a day[2]
- printing costs (cartridge and paper)amounting to $100,000 a year[3]

The following scenarios serve to illustrate the various impacts Safetica could have on the company operating profit.

1st scenario: Safetica had not been implemented at all

- the company suffered a data leak incident and hence must bear costs and fines resulting from the leak
- the company has not reached any savings in the personnel and printing costs areas
- the company does not bear implementation and maintenance costs of Safetica

2nd scenario: Safetica was implemented after a data leak incident took place

- the company suffered a data leak and hence must bear costs and fines resulting from the leak
- the company has reached savings in the personnel and printing costs areas
- the company bears implementation and maintenance costs of Safetica

3rd scenario: Safetica was implemented before any data leak incident took place

- the company avoided data leaks, and so no costs and no fines resulting from a leak occurred
- the company has reached savings in the personnel and printing costs areas
- the company bears implementation and maintenance costs of Safetica

[1]In Financial Sector, each data breach costs $353 per record, according to Ponemon Institute
[2]The same assumptions as in the ROI calculation (the hourly wage) were used for this quantification
[3]Assuming approximation: an employee will on average print 2 pages a week for private purposes, the cost of one printed page is 0.1$;