Profitable Investments Mitigating Privacy Risks

John Borking

PROFITABLE INVESTMENTS MITIGATING PRIVACY RISKS

John Borking (Director Borking Consultancy – Wassenaar – Netherlands)

Risk control plays an important role at privacy protection. Article 17 (1) of the Directive 95/46/EC (DPD) requires that the controller must implement appropriate technical and organizational measures to protect personal data. ICT offers solutions in the shape of privacy protection for users, consumers and citizens. The application of ICT to protect privacy has become widely known under the name Privacy-Enhancing Technologies (PET or PETs). This chapter points out that a positive business case for the economic justification of investments in PETs is needed before a positive decision on the investment will be taken. The ROI and EPV calculation methods are useful tools for management assessing PET investments.

According to Article 23 of the DPD [1] a person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to DPD is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event causing the damage.

The term risk is not defined in the DPD. The term risk is frequently used as if it is for everyone a univocal term. At closer consideration that is still but the question. Gratt, President of the American society or Risk Analysis (SRA) concluded after a two-years research that " a consensus was not being reached for the key definitions or risk and risk analysis". [2]

In this chapter as a definition of risk will be used: Risk = consequence *probability or (consequences_of_threat) * (likelihood_of _occurrence).[3]

A privacy threat analysis or a privacy impact analysis must be carried out examining the risks and documenting the results, before designing an information system that will be capable to protect personal data adequately against loss or against any form of unlawful processing. [4] A privacy risk analysis is mandatory according to the DPD as article 17 states that " (…) such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."[1]

Schneier writes that " Threat Modeling is the first step in any security solution. It's a way to start making sense of the vulnerability landscape. What are the real threats against the system? If you don't know that, how do you know what kind of countermeasures to employ?" [5]

THE PRIVACY RISK ANALYSIS

There are many ways determining privacy risks. The general approach for privacy risk analysis and subsequent requirements determination etc. is derived from a comparable domain: the risk assessment for information security in British Standards 7799, the Code of Practice for the Risk Analysis and Management Method, Information Security Handbook of the Central Computers and Telecommunications Agency (CCTA). [6] The pentagonal privacy threat analysis approaches threat identification and assessment of severity of consequences of such threats from five different perspectives:

- Privacy legislations, as defined in a certain country or country union: these regulations inherently list a number of privacy threats, if these regulations are not adhered to;
- Purpose of the system, which creates its own threats: because the user (private person) wants to achieve something, that person creates privacy threats;
- Solution adopted, which may or may not create threats of its own;
- Technology used: because of the way a certain system is implemented, certain threats may emanate which are not necessarily consequences of the intended purpose. Meanwhile, the technology will harbour some of the privacy enhancement measures;
- Situation in which the ultimate system will be used: which, although not necessarily creating threats of its own, may or may not aggravate (or alleviate) previously identified threats and hence may incur more demanding technological measures. This part is especially needed when a commercial off the shelf (COTS) product is going to be used in an unforeseen situation; the previous four types can be followed whether or not the system is a COTS or dedicated to a certain problem and environment. See figure 1.

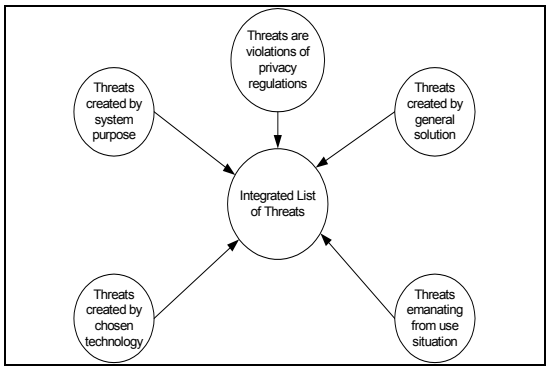

***Figure* 1. Five-pronged approach to Privacy Threat Analysis [3]**

Derived from the Directive 95/46/EC (DPD) the following risks or threats can be discerned:

- Secret possession of (control over) personal data files: the data subject and the authorities are unaware of the existence of the personal data and the control the controller of these data has;
- Secret processing of personal data: processing out of sight or knowledge of the data subject;
- Out of bounds processing by controller: processing of personal data that is not within the bounds stipulated in the personal data constraints or can be expected to be outside the scope and intention of the collection;
- Out of law processing: processing of personal data that is illegal, forbidden by national law (or is not explicitly allowed if it can be expected to be of dubious nature);
- Personal data deterioration: the personal data is in contradiction with the current situation, either caused by external changes or by incorrect or incomplete insertion, collection or insertion;
- Irresponsiveness to discontent: the controller does not respond, or incorrectly, incompletely or unduly late, to requests for correction or other implications to the personal data or the personal data constraints of a data subject; the controller thwarts communication; also: there is no authority with reprehension, correction, sanction or other influence on the controller to sustain the data subject's legal rights;
- Out of bounds processing by processor: the processor does not follow the personal data constraints as provided by the controller or violates the rules;
- Out of jurisdiction processing: the personal data are transferred to a controller which has no legal obligation to obey the personal data constraints or where legal obligations about privacy are less stringent than in the data subject's privacy regime;
- Personal data and personal data constraints violation: the controller and processor disobey the obligation to follow the personal data constraints concerning disclosure, retention, termination and safeguarding of correctness, including the obligation to take precautions against loss or mutilation of the personal data or the personal data constraints. [3]

TRADITIONAL SECURITY MEASURES NOT SUFFICIENT

The requirements referred to in the DPD must be implemented efficiently in the organization in order to give proper support to the citizen's right to privacy with respect to personal data. It is therefore important to devise a proper system of general processing measures and procedures that should be present in order to protect company processes and in connection with specific protective measures for the processing of personal data. The restrictions that the organization of information systems can impose on the possibility that their users can comply with privacy

legislation are evident. One simple example is where a system contains an inescapable 'date of birth' field, while analysis of the company's processes shows that recording the birth date of all persons included in the system is excessive. System design can just as easily ensure that users correctly observe the law. As a rule, privacy protection will constitute a supplementary system of measures and procedures in addition to the usual processing and security measures, but it should be assigned a significant place in management processes in order to implement and maintain a balanced processing policy for personal data.

When an organization is asked what it has done to protect privacy, it is apt to emphasize the personal data security measures it has in place. Although the use of safeguards to prevent unauthorized access to personal data is an important aspect of privacy protection, it is not sufficient in its own right. This is because such safeguards rarely involve the encryption of stored data; consequently, effective protection depends entirely on the security measures being correctly implemented and functioning properly.

It is therefore preferable to take technical measures that protect the individual's privacy at the point of data collection. Such measures may do away with the need to generate or record any personal data at all. Alternatively, they may minimize or even obviate the need to use or store identification data.

Given the basic legal requirements for privacy protection and the risks of privacy incidents, it will be apparent that, if technical provisions are to be deemed adequate, they must go beyond the implementation of traditional security measures.

PRIVACY ENHANCING TECHNOLOGIES (PET)

ICT offers solutions in the shape of privacy protection for users, consumers and citizens. The application of ICT to protect privacy has become widely known under the name Privacy-Enhancing Technologies (PET or PETs). [6] PETs have been defined by the EU Commission as a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system. [7][8]

PETs can guarantee data protection without making excessive demands on the processing of the data. By applying PETs and streamlining personal data processing, the organizations can continue to meet the high public expectations with respect to services and dealing with personal data.[9]

The basic driver to invest in PETs is their potential to avoid privacy incidents and so to reduce the risks and subsequently the damage caused by privacy breaches. In general terms a privacy incident can be defined as an event in which personal data are misused, because of the fact that personal data accompanied by a list with personal data constraints haven't been respected.

Privacy breaches may impact an organization in different ways. Tsiakis and Stephanides distinguish direct, short-term, and long-term economic consequences. [10] Direct consequences are the costs for repairing or changing systems, costs of

stopping or slowing down production or processes, costs of legal action. Short term consequences comprise the loss of existing customers, contractual relations, and the loss of reputation. Companies may loose business because of privacy breaches, which harm their trust relationships with customers and other business relations. Safeguarding privacy has been identified as a major component of building trust.[11] Long term consequences include the loss of stock value and market value. An example of the latter is DoubleClick in 2000. After a serious violation of their existing privacy statement on their website and the lawsuit that was the result of this violation, their stock declined with 20%. [11] This also occurred with Choicepoint after their public announcement that they were hacked, and approximately 10 million data records were stolen. Their stock declined with 17% since the data breach. [6] The study on the economic benefits of privacy-enhancing technologies (PETs) from the EU Commission states that an obligation to notify privacy incidents would make risk assessment more accurate. [12]

BUSINESS CASE FOR PET INVESTMENTS

Investments in (risk reducing) PET require insight into the costs and the quantitative and qualitative benefits. It is essential for the decision-making process concerning the investment for PET.[6]

The decision to spend money on privacy in any direction has to be financially justified. There is no point in implementing an expensive solution if a less expensive solution would offer the same risk reduction and because of that a better privacy protection. Beyond the legal compliance, it makes no sense to invest in a solution if its true costs are greater than the value it offers.

From the perspective of a business, privacy implies an investment to be measured in Euros saved as a result of reduced cost, or in additional revenues and profits from new activities that would not have occurred without an investment in privacy.

From the risk management literature a number of metrics have evolved to measure security risks, some of which apply to privacy risks as well. [13]

ANNUAL LOSS EXPECTANCY

One of the most common measures for the assessing the risk of a harmful event is Annual Loss Expectancy, or ALE. ALE is the product of the expected yearly rate of occurrence of the event times the expected loss resulting from the occurrence. Other yardsticks here are SLE and ARO. SLE stands for the Single Loss Exposure; this is the true cost of a security incident. ARO means annual rate of occurrence; this is the frequency in which a risk happens on a yearly basis. The annual loss expectancy foreseen from all of an organization's operations would be the sum of the expected yearly losses that could result from multiple (privacy) threats. Determining adequate inputs to this ALE equation is however very difficult, due to lack of statistical data.

For example if a bank estimates the probability of a serious security incident at one of its subsidiaries during 2008 as one in a million and the direct and indirect cost of such incident as 150 million Euros, the ALE created by the risk of this security incident for 2008 will be € 15 million times 1/1,000,000 = € 150. Of course the actual costs of this risk will never be that of the ALE, but it will be either € 0 or €150 million. In most cases the situation will be less certain and the probability or cost may range between one in five hundred thousand and one in a million and the cost may vary between € 100 million and € 200 million. The ALE would then be between: (€100M or €200M) x (1/500,000,1/1,000,000) = €100 or €400. [14]

RETURN ON INVESTMENT (ROI)

A metric that is quickly gaining in popularity is Return On Investments and specifically Return On Security Investments (ROSI). [15] Cardholm writes that: "Return on Investment (ROI) is a straightforward financial tool that measures the economic return of a project or investment. It is also known as return on capital employed. It measures the effectiveness of the investment by calculating the number of times the net benefits (benefits minus costs) recover the original investment. ROI has become one of the most popular metrics used to understand, evaluate, and compare the value of different investment options" [16]

The equation is: ROI = [(Savings from safeguards) + (profits from new ventures)] / costs of safeguards = [ALE (baseline) – ALE (with safeguards) + (profits from new ventures)] / (divided by) costs of safeguards. [13]

Hereunder follows an example. Suppose an organization decides to implement a Privacy Management System (PMS). The business case could be substantiated as follows:

If PMS were not implemented, the minimum annual costs for a company employing 1,000 staff to comply with privacy policies are estimated as follows:

1. Annual costs

Salary costs for Privacy Protection Officer (100% time allocation) Euro 100,000;

Management and secretarial salary costs Euro 40,000;

Costs for privacy audit Euro 30,000;

Security costs with respect to privacy compliance (excluding essential information security) Euro 20,000;

Report maintenance, regulations, settling registered people's rights, information, image and other damage, etc. Euro 20,000.

This leads to the total annual costs of Euro 210,000.

When comparing the situation where a PMS is used, the picture is as follows:

2. Development and implementation of PMS

For the acquisition of PMS has to be paid: Euro 150,000;

Consultancy for PMS implementation (60 days) costs Euro 80,000;

Start-up costs after implementation Euro 20,000.

The total one-off costs are Euro 250,000.

To these costs have to be added:
a. Annual costs PMS
b. PMS operational costs are Euro 30,000;
c. Maintenance costs are ± 15% of acquisition cost per annum: Euro 22,500;
d. Costs for privacy audit: Euro 10,000;
e. Salary costs for Privacy Protection Officer (50% time allocation) Euro 50,000;
In this situation the total costs are Euro 112,500.

The saving per annum compared with the situation when there wasn't an investment in PMS is Euro 210,000 - Euro 112,500 = Euro 97,500. Thus the extra investment costs for PMS would be already fully recovered after approx. two years and 2 months. [8]

RETURN ON SECURITY INVESTMENT (ROSI)

ROSI is a special application of ROI. The Return On Security Investments (ROSI) formula is the most well known ROSI calculation in the security industry. [6]

ROSI is an approach to look at the investment costs of security protection and the risk the investment removes. Assuming that the annual benefit of a security investment will be received throughout the lifetime of the investment, ROSI calculates the sum of the annual benefits over its cost. Benefits are calculated by adding expected cost savings to the new profit expected from new activities and sales.

Cardholm states that "it is basically a "savings" in Value-at-Risk; it comes by reducing the risk associated with losing some financial value". [16] Three core elements are determinative for the output calculation of the investment, namely: costs, turnovers and non-financial measurable elements. ROSI can be calculated using the equation below.

$$Rosi = \frac{(RiskExposure \bullet \%RiskMitigated) - SolutionCosts}{SolutionCost}$$

Figure 2. ROSI Equation

The earlier discussed ALE can also be written as: Risk Exposure * %RiskMitigated or Risk mitigated because of the investment in security. [13]

The difficult parts in ROI method is determining ALE and SLE the risk-mitigating benefits of the security investment, since it is very difficult to know the true cost of a security incident. According to Sonnenreich, Albanese & Stout [15] there is very little known about those costs, because very few companies track those incidents.

Cardholm has a better approach with less uncertainty. His calculation is as follows:

ROSI = R – (R – E) + T,
or
ROSI = R – ALE, where ALE= (R - E) + T

The terms in Cardholm's equation can be described as:
- ALE: What we expect to lose in a year (Annual Loss Expectancy)
- R: The cost per year to recover from any number of incidents.
- E: These are the financial annual savings gained by mitigating any number of incidents through the introduction of the security solution.
- T: The annual cost of the security investment. [16]

ROI FOR PRIVACY PROTECTION (ROIPI)

The ROI calculation methods can be applied also analyzing the return on investments that mitigates privacy risks, PET.

PET investments differ from "normal" ICT investments, since the investment may not directly improve the workflow, or does not make a process more efficient. The costs from PET are tangible and because of that are relatively easy to know. The benefits however are mostly intangible, because for example reputation improvement and a decreased risk for privacy incidents are not easy to quantify. However, these intangible benefits have the biggest value in a PET investment.

Luckily, the value of risk mitigated can be calculated using the method of Darwin (2007). The Darwin Calculator can be found at www.tech- 404.com/calculator.html.

The focus in this method will then be on the tangible benefits, the value of risk mitigated and the total costs, related to the PET investments. This method will be named: Return on Privacy Investments (ROIPI). How these figures will be calculated will be explained hereunder in more detail in the example of the Ixquick Europrise seal business case.

The formula is: ROIPI = {(TangibleBenefits +ValueOfRiskMitigated) – TotalCosts} divided (/) by the total costs

When the ROIPI gives a positive result, it means that the investment is beneficial for the company since the benefits outweigh the costs. Note that if the value of risk mitigated is positive this also has a positive influence on the ROIPI. The strong point of this formula is that it is not necessary to derive at an accurate estimate. The ROIPI only has to be precise enough to support the decision-making.

ROIPI assumes that the organization will fully comply with the law. This isn't often the fact. Violation of privacy, i.e. the illegal use of personal data, generates a lot of revenue and the chance that violation will lead to a prosecution is nil, due to the lack of resources of the National Data Protection Authorities.

CASE STUDY: IXQUICK

Ixquick is a meta searchmachine. The website of Ixquick be found at www.ixquick.com. Ixquick revenue model is the number of hits times the advertising benefits. The revenue is highly correlated to the search queries done through the site.

In 2003 and 2004, Internet traffic went down. In 2005, Internet traffic only went down with 5% and stabilized. In 2006 and 2007 the traffic increased again, due to the fact that Ixquick anonymized the IP addresses and search results in June 2006. Because of the anonymization, the traffic in 2006 and 2007 increased considerably. Due to the optimalization of the privacy protection of the users of the Ixquick meta search engine, triggered by the requirements for obtaining the EuroPrise privacy certificate (see www.european-privacy-seal.eu/about-europrise/fact-sheet) the number of visitors of the website increased again substantialy in 2008, thanks to the investment in the PET tool anonymization. With the increased traffic the revenue od Ixquick went up as well.

The reason of Ixquick for using PET was that it is a unique selling point; Ixquick became and is still the first fully anonymized meta search engine. Besides this reason the other driver was privacy risk minimalisation.

The investment costs for the PET tool were Euro 129.800, inclusive the extra investments needed for meeting the requirements of the EuroPrise certificate. The expenditure for the optimalized privacy protection amounted to € 37.000 for the technical and legal expertise. For press releases and communication costs announcing the Europrise privacy certificate award in July 2008 € 8.000 was spent. The mentioned costs were non-recurrent one-off expenses.

Moreover there are also recurring costs for the maintenance and the further development of the system amounting to € 16.500 per year. The total costs for the whole PET investment was: € 183.300.

The ROIPI equation can now be used for calculating whether Ixquick's privacy protection investment was the right decision of Ixquick's management.

ROIPI={(TangibleBenefits +ValueOfRiskMitigated) –TotalCosts} / (divided) by the total costs.

The total PET costs are Euro 183.300. The tangible benefits of using PET tools are the extra revenues in because of the increased data traffic. The directly tangible advantage for Ixquick due to the use of PET for the period of PET investments (2005-2008) is Euro 345.800. [6] To estimate the factor 'risk mitigated' the calculation tool of Darwin (2008) has been used. It will be assumed that in a privacy incident 10.000 records were stolen. Based on the daily users of the Ixquick search machine, the actual risk was much higher. The risk class of this data is of risk class II according to the guideline of the Dutch Data Protection Authority (CBP) [17] since the data consist of searches, these can consist of IP address, social security numbers and credit card numbers.

Based on the Darwin calculator (2008) the value of risk mitigated is Euro 1.050.300 on the 80% level (loss of 10.000 records) and the Dollar/Euro exchange rate in November 2008.

Using the values, the ROIPI equation produces as result:

TotalCosts= Euro183.300
TangibleBenefits= Euro 345,800
ValueofRiskMitigated= Euro 1.050.300
The intangible costs and benefits are appreciated as Euro 0 .
Thus ROIPI = {(345.800 + 1.050.300 + 0) – 183.300} / 183.300 =ROIPI = 6,6165 = approx. 662 % of the PET investment.

As this ROIPI value is very high, the conclusion is that the investment is very worthwhile. This number is also very high because of the value of risk mitigated. The ROIPI equation is especially preferable for SMEs because of its simplicity. This formula is a quick and reliable indicator whether the investment is worthwhile.

The intangible costs and benefits have been appreciated as zero euro, but if these intangible elements would be calculable, then the result would be even more favorable. However the ROIPI value is here significantly large enough to carry out the PET investment and to justify the investment from a business economy point of view.

Others advocate rightfully that organizations should discard the above equations and instead use discounted cash flow methods for investments that have different costs and benefits in different years. The theoretical flaw in ROI (and so in ROSI, ROIPI and related approaches) is that it processes financial figures irrespective of the dates that will be received or paid. The value of 1 euro today is not the same as of 1 euro in two years time. [13] The Discounted Cashflow methods (DCF) encompass two separate methods, the internal rate of return (IRR) and the Net Present Value (NPV). The allotted space for this chapter doesn't allow elaborating on the IRR method.

NET PRESENT VALUE (NPV)

The Net Present Value (NPV) of a project or investment is defined as the sum of the present values of the annual cash flows minus the initial investment. The annual cash flows are the Net Benefits (revenues minus costs) generated from the investment during its lifetime. These cash flows are discounted or adjusted by incorporating the uncertainty and time value of money. NPV is one of the most robust financial evaluation tools to estimate the value of an investment. [16]

The calculation of NPV involves three simple yet nontrivial steps. The first step is to identify the size and timing of the expected future cash flows generated by the project or investment. The second step is to determine the discount rate or the estimated rate of return for the project. The third step is to calculate the NPV using the equations shown below:

NPV = initial investment + (Cash flow year 1 divided by (1+r)1) … (Cash flow year 1 divided by (1+r)n)

Or:

$$\text{NPV} = \text{Initial investment (i)} + \sum_{t=1}^{t=\text{end of project}} \frac{\text{(Cash Flows at Year t)}}{(1+r)^{t}}$$

The meaning of the terms is as follows:

·Initial investment (*i*): This is the investment made at the beginning of the project. The value is usually negative, since most projects involve an initial cash outflow. The initial investment can include hardware, software licensing fees, and start-up costs.

·Cash flow (cf_n): The net cash flow for each year of the project: Benefits minus Costs.

·Rate of Return (*r*): The rate of return is calculated by looking at comparable investment alternatives having similar risks. The rate of return is often referred to as the discount, interest, hurdle rate, or company cost of capital. Companies frequently use a standard rate for the project, as they approximate the risk of the project to be on average the risk of the company as a whole.

·Time (*t*): This is the number of years representing the lifetime of the project.

Experts are convinced that a company should invest in a project only if the NPV is greater than or equal to zero. If the NPV is less than zero, the project will not provide enough financial benefits to justify the investment, since there are alternative investments that will earn at least the rate of return of the investment. [16]

ECONOMIC JUSTIFICATION OF INVESTMENTS IN PRIVACY RISK REDUCING PET

Within the context of the NPV method, the following data have to be collected:

1.The initial investment in privacy protection [I(p)], which encompasses cash outlays for Privacy Risk Analysis, process modeling, PET, implementation of PET, productivity loss, change management.

2.The yearly recurring cash flow, which contains all yearly financial effects of the proposal. This calculation bears on an analysis of expected cash flow patterns that would occur with and without the investment; it reflects a difference between two defined situations. The so-called ‘without’ situation will usually be the continuation of the current situation. This can for example be a situation with existing privacy protection in place, where the added value of PET is considered. The ‘without’ situation might also be a situation without any privacy protection. The definition of the ‘without’ situation depends on the starting position of the decision-maker.

Ribbers proposes to take into account the following cash flow components: Annual Loss Exposure (ALE), Reputation Recoverage Costs (RRC), Expected Revenue Accrual (ERA), Recurring Privacy Costs (RPC). [13]

ALE is the multiplied projected costs of a privacy incident and its annual rate of occurrence. Basically this encompasses revenue losses, legal claims, and productivity losses because of privacy breaches, repair costs and lost business.

RCC contain those expenses needed to restore the reputation of the company damaged by privacy breaches; examples are additional costs for PR and Marketing. Moreover if a privacy breaches affects the share price of the company (see ChoicePoint, Double Click), possibly breaches affects the share price of the company (see ChoicePoint, Double Click), banks and other financial institutions may require possibly additional financial guarantees.

ERA represents, on the positive side, possible marketing impacts on market share and revenue of publicized implementation of PET.

RPC contains the yearly (additional) privacy costs caused by the proposal; this will encompass needed privacy threat or impact analyses, audits, privacy officers etc.

As said, the analysis compares the project situation with the situation without the project. Basically this comes down to analyze the cash flow differences between the two situations. This can be done either by applying a factor RM (Risk Mitigated) to the situation without the investment or by subtracting the full-expected cash flow of the two situations from one another.

The RM factor for the applied privacy risk reducing/protection solution indicates what part of ALE and RRC has been compensated by the solution. Mitigated Risk is expressed as a reduction of the expected number of privacy breaches per year.

The resulting NPV of a privacy protection solution is consequently as follows:

$$NPV = - I(p) + \sum_{J=1}^{n} \{(ALE + RRC)\, RM + ERA - RPC\} / (1+i)^{j}$$

Figure 3 privacy NPV equation [13]

THE CASE OF THE NATIONAL VICTIM TRACKING AND TRACING SYSTEM (VITTS)

The nation-wide implementation in the Netherlands of the Victim Tracking and Tracing System (ViTTS) is an important contribution to effective disaster management. The system provides regional medical officials with a concrete support to execute their tasks, through access to the required relevant contextual information,; it supports the allocation of injured persons to local and regional hospitals, and it provides the relevant competent authorities with necessary information. Moreover, municipalities will be better placed to execute mandatory registration procedures under the municipal disaster plan, and hospitals will be provided with timely information about the numbers of victims and the nature of their injuries. Due to the fact that sensitive personal medical information is processed about victims, the DPD

requires optimal protection of such sensitive personal data. Privacy issues with respect to the health sector are particularly sensitive.

The EU PRIME ((Privacy and Identity Management for Europe) research team [6] has applied the NPV calculation approach in several case studies. One of the case studies is ViTTS. The following data have been collected from ViTTS.

The initial investment in privacy protection I(p) comprises the following components:

- System analysis and design, prototyping, test runs:	Euro 15,000
- Privacy audit and Privacy risk assessment:	Euro 50,000
- Smart Cards for on line authentication and encryption:	Euro 25,000
- Implementation costs of PET measures:	Euro 80,000
Total initial investment in reducing the risks of privacy incidents:	Euro 170,000

Privacy breaches affecting the process of handling victims would have serious consequences and should be at all cost avoided. The privacy threat analysis showed that without privacy protection the VITTS system would undergo privacy breaches on a regular basis. The damage that would result from that can be estimated as follows.

The direct consequence of a breach (SLE – Single Loss Exposure) would be loss of reputation of the national government, possible wrong allocation of victims to hospitals with ineffective treatment and possibly deceases as a consequence. This may lead to significant legal claims. Claims of Euro 100,000 per case are not exceptional.

Such a breach would necessitate a nation-wide roll out of system adaptations: for which is needed two man-months per designated preventive health care safety region at Euro 100 per hour:

Total costs	Euro 347,000
Test and Trials to prove effectiveness of the system: Euro 80,000 per region:	
Total cost	Euro 800,000
Training and education roll out:	Euro 50,000
The total recovering costs (RCC) would amount to:	Euro 1,197,000

The expected revenue accrual (ERA) can be estimated as follows. The most important reason for designated preventive health care safety regions to adopt the system is the built-in optimal privacy protection. So without privacy protection or with a much less rigid privacy protection there wouldn't have been developed such a system.

The estimated salary costs to replace the system by manual procedures would amount to 3 FTEs per region, which amounts to Euro 180,000 per region.

Nationwide this would result in a cost of: Euro 1,800,000

The total benefits of protecting privacy and reducing the risks of privacy incidents can be estimated at: Euro 2,277,000

(in this number legal claims are not included).

For the NPV calculation the following scenario is assumed: a time horizon of 6 years, a serious privacy breach every 2 years and a cost of capital of 5 %.

Applying the equation results into the following:
I(p): Euro 170,000;
Recurring cash flows:
- Costs avoided every two years: Euro 2,277,000
- Yearly recurring privacy costs: Euro 400,000
- Privacy costs in year 3 (no costs in year 6 given the assumption): Euro25,000.

Under this assumption Ribbers' equation would lead to the following calculation:

NPV = - 170,000 + 2,277,000 (0.907029 +0.822702 +0.710681) – 25,000 (0.863838) – 400,000 (5.242137) = Euro + 3,268,368. [13]

This (positive) business case does not include possible legal claims.

The business case for the investment mitigating the risk of privacy incidents is positive. Other scenarios lead to a positive business case as well. The privacy protection will even be profitable under the unrealistic assumption of a privacy breach only occurring once (and taking legal claims into account).

CONCLUSIONS

The ROI and NPV calculation methods are useful tools for management for assessing the (planned) investments in PET, reducing the risks of privacy incidents considerably.

ROI, ROSI and ROIPI provide useful insights. For a "quick and dirty" assessment of a PET investment ROIPI is useful especially for SMEs, like in the Ixquick business case. However ROIPI and other ROI methods are based on evaluating reductions in risks and do not take a time factor into account. The best approach would be to consider investments in PET as regular investments, characterized by cash flow patterns.

The Net Present Value approach is applied on the ViTTS case. This approach is effective in the context of assessing investments in PET, reducing privacy risks and enhancing privacy protection.

As many data are uncertain due to the lack of recording privacy incidents, scenarios have to be designed and assessed to give decision makers an understanding of the behavior of cost and benefit factors and their eventual effect on the business case outcome. Much more research on the economics of privacy has to be done. [12]

REFERENCES

[1] Directive 95/46/EC, Official Journal L 281, 23/11/1995 P. 0031 – 0050
[2] Muller E.R. (red.), Veiligheid, Studies over inhoud, organisatie en maatregelen, Alphen aan den Rijn 2004

[3] Blarkom G.W. van, Borking J. J., & Olk J. G. E., Handbook of Privacy and Privacy-Enhancing Technologies, The Case of Intelligent Software Agents, Den Haag, 2003. http://www.cbpweb.nl/downloads technologie/pisa handboek.pdf
cfr. Fritsch L. & Abie H., A Road Map to the Management of Privacy Risks in Information Systems, Oslo, 2008
[4] Flaherty D.H, Privacy Impact Assessments: An Essential Tool for Data Protection in Privacy Law & Policy Reporter Vol 7, No 5, October 2000
[5] Schneier B., Threat Modeling and Risk Assessment, in H.Baumler, E-privacy, Datenschutz im Internet, Wiesbaden 2000
[6] Borking J.J.F.M., Privacyrecht is Code, Over het gebruik van privacy Enhancing Technologies, Deventer 2010
[7] Borking J., 'Der Identity Protector', Datenschutz und Datensicherheit, 11, 1996; Hes R. & Borking J., Privacy-Enhancing Technologies: The Path to Anonymity, The Hague, 1998
[8] EU Commission, COM(2007) final
[9] Koorn R., Van Gils H., ter Hart J., Overbeek P., Tellegen R. & Borking J., Privacy Enhancing Technologies, Witboek voor Beslissers, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Den Haag 2004
[10] Tsiakis, T. & Stephanides, G., The economic approach of information security. Computers & Security, 24, 2005.
[11] Chapman S., & Dhillon, G.S., Privacy and the internet: the case of DoubleClick, Inc. – Social Responsibility in the Information Age: Issues and Responsibilities. Fort Lauderdale-Davie, 2002.
[12] Final report to the European Commission DG Justice, Freedom and Security, Study on the economic benefits of privacy-enhancing technologies (PETs), Brussels 2010
[13] Fairchild A. & Ribbers P. Privacy-Enhancing Identity Management in Business, in Privacy and Identity Management for Europe, J.Camenish, R.Leenes & D.Sommer (eds.) Brussels, 2008
[14] Blakley, B., McDermott E. & Geer D., Information management is Information Risk Management in Proceeding NSPW'01, Cloudcroft, New Mexico, 2002
[15] Sonnenreich, W., Albanese J. & Stout B., Return on Security Investment (ROSI) – A Practical Approach. Journal of Research and Practice in Information Technology, Vol. 38, No. 1, Feb. 2006
[16] Cardholm L., Adding Value to business performance through cost benefit analyses of information security management, Gävle 2006
[17] Blarkom G.W.van & J.J.Borking, Beveiliging van Persoonsgegevens, Achtergrond enVerkenningen 23, Den Haag 2001
Privacy Rights Clearinghouse: A Chronology of Data Breaches. 2007. Available at: http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP