An Overview of Economic Approaches to Information Security Management

Xiaomeng Su

University of Twente, Information Systems Group, Enschede, The Netherlands
x.su@ewi.utwente.nl

Abstract. The increasing concerns of clients, particularly in online commerce, plus the impact of legislations on information security have compelled companies to put more resources in information security. As a result, senior managers in many organizations are now expressing a much greater interest in information security. However, the largest body of research related to preventing breaches is technical, focusing on such issues as encryption and access control. In contrast, research related to the economic aspects of information security is small but rapidly growing. The goal of this technical note is twofold: i) to provide the reader with an structured overview of the economic approaches to information security and ii) to identify potential research directions.

1 Introduction

Information security - the safeguarding of computer systems and the integrity, confidentiality, and availability of the data they contain - has long been recognized as a critical issue. Two current trends indicate that its importance is growing. First, the integration of computers into more and more aspects of modern life continues. Second, cyber-attacks, or breaches of information security, appear to be increasing in frequency, and few observers are willing to ignore the possibility that future attacks could have much more severe consequences than what has been observed to date.

The core issue, in both public and private sectors, is whether we devote enough resources to information security or too much resources to information security[1]. Part of the answer must come from economic analysis. What are the costs, both historical and potential, of security breaches? How frequently can attacks be expected? Can these factors be quantified precisely, so that business firms and other organizations can determine the optimal amount to spend on information security and measure the effectiveness of that spending?

This technical notes surveys the state of art on economic approach to information security. First, we investigate whether organizations use economic analysis for information security. Is it required to economically justify security expenditure? Why justify security expenditures? What caused the move to justify security expenditure?

[1] As stated by a security officer in a Fortune 500 company, "you don't want to secure yourself out of business".

X. Su,"An Overview of Economic Approaches to Information Security Management", Technical Report TR-CTIT-06-30, University of Twente, June 2006

Second, we look at what techniques have been used to justify security expenditure. Much of the industry has begun to embrace the economic metrics to validate the security department expenditures by expressing them in terms of Return on Security Investment (ROSI), Net Present Value (NPV) and Internal Return on Investment (IRR).

Third, we examine what topics have been addressed in the literature and in practice. We categorize the studies in three topics: i) measuring the cost and effect of security breaches, ii) measuring the benefit and effect of security control and iii) determining the optimal level of security investment.

2 Why justify security expenditures?

2.1 The need for economic approaches

Information security expenditures are increasingly coming under greater and greater scrutiny. Security departments are both struggling trying to manage the risk associated with the e-commerce growth and fighting for their growing budget needs. Gordon and Loeb comment in saying, "To protect the confidentiality, integrity, and availability of information, while assuring authenticity and non repudiation, organizations are investing large sums of money in IS activities. Since security investments are competing for funds that could be used elsewhere, it's not surprising that CFO's are demanding a rational economic approach to such expenditures." [20].

In todays security realm, security managers are forced to make a case for the larger expenditures. A quote from an email of an information security officer posted in the security focus mailing list illustrates the situation; *"I need to begin putting together monthly reports for executive management (CEO) that show the value that the information Security department is providing to the company. The execs know what we do, my senior management feels we need to broadcast the value InfoSec provides."*

2.2 What is the picture in practice?

In researching the question of the security fields perception we find that empirical evidence shows that economic analysis (or cost benefit analysis) is a sound basis for budgeting information security expenditures. In [22], The authors try to find empirical answer to the question - "Do firms use economic analysis in deciding on planned expenditures for information security?" "What are the key factors driving and impeding the use of economic analysis by firms in deciding on information security expenditures?" The survey concluded that senior information security managers apparently do use some form of economic analysis in budgeting for information security. Their analysis shows that some of the participants approach information security expenditures with a formal NPV analysis, whereas other respondents approach these expenditures with a modified economic analysis. The modified approach consists of examining the costs and

benefits of information security activities, but with less emphasis on formally quantifying the benefits. Based on the responses to the open-ended questions, there seems to be a movement toward using more economic analysis in evaluating information security activities.

Another empirical study is the 2005 CSI/FBI Computer Crime and Security Survey. It states "A significant number of organizations conduct some form of economic evaluation of their security expenditures, with 38 percent using Return on Investment (ROI), 19 percent using Internal Rate of Return (IRR) and 18 percent using Net Present Value (NPV)." [24].

2.3 What caused the move?

Security is not a new concept. One might ask what has pushed upper management to require this kind of economic evaluation onto what was previously considered just an operational cost. The importance of effective management of information security has increased in recent years due to increasing frequency and cost of security breaches. The US Treasury Department's Office of Technical Assistance estimates cyber crime proceeds in 2004 were 105 billion dollars, greater than those of illegal drug sales. According to the 2005 CSI/FBI Computer Crime and Security Survey, nearly nine out of ten US businesses suffered from a computer virus, spyware or other online attack in 2004 or 2005 despite widespread use of security software. The total loss reported from 639 respondents of the CSI/FEB survey for 2005 were over 130M dollars (203K dollars per respondent). Public attention about security breaches increased dramatically when companies like Amazon.com, Ebay and Yahoo! were hit by Denial-Of-Service (DOS) attacks in February 2000. A number of high-profile computer worms and viruses, such as *code red, Nimda* and *I love you*, also heightened the awareness.

Another factor is a change in the way companies conduct business. E-commerce has grown tremendously causing security departments to be creative in the methods of securing the organization while keeping in line with tightening budgets and reduced profits. In trying to keep one step ahead of the current vulnerabilities, they have been busy trying to secure new funds. Security is a fundamental enabling technology of the Internet and attacks make it harder to do business on the Internet. Return on Security Investment (ROSI) has become a controversial topic due to immense growth of e-business [10].

Also, the literature sources indicate that, within the past few years, there have been four major drivers setting directions to security decision makers in organizations [17]:

- Government and industry-sector-specific regulations, for example the US Public Company Accounting Reform and Investor Protection Act of 2002 (better known as Sarbanes-Oxley), the Basel II Accord for international banks, and the National Standards to Protect the Privacy of Personal Health Information (HIPAA) for medical privacy.
- Standards, for example the ISO 17799 standard, and best practice models for IT security such as ITIL and COBIT.

– Business risks and security requirements of the business network that an organization has or wants to join. For many companies information security is a qualifier to be in business, for example, big companies like Motorola, Ford and General Motors require their partners or providers have appropriate security practices.
– Urgency to invent opportunities in the midst of security breakdowns that incur monetary damage, corporate liability, and loss of credibility.

When these factors are coupled together it becomes clear why the upper management is requiring detailed explanation of how and why the security department is spending funds.

In the past we have relied on fear, uncertainty, and doubt to qualify the expenditures needed to secure an organization. A method coined as FUD in the information security community. As we can see, these methods are gradually fading into the past while economic measures are rising to the forefront. However, it is rarely possible to use completely rational economic models of cost benefit analysis (for example, the NPV model) in budgeting for information security. Our interviews with the security officers in companies also show that for some companies it is largely driven by such items as best practices in the industry, or a must do approach; *"If the business decides to enter or stay in a certain market, then you have to comply with the rules and regulations of that market. Return on security investment doesn't come into it; it's a business decision to be there, regardless of compliance costs."*

In sum, it is fair to say that in todays security realm, security must make business sense for an organization. Today information security is shifting from what is technically possible to what is economically efficient. Perfect security does not exist, and even if it exists, it may very well be too expensive and not worth it. Likewise, no security causes breaches that are too expensive, and companies can not afford that. Each company should strike an appropriate balance between risk and opportunity to reduce risk through security controls. What is worth is adequate security at a reasonable cost, that provides the companies ability to offer new services, to expand into new markets and to attract and retain customers. Economic evaluation of security activity is needed to justify the budget set for security projects; to assist in project appraisal and selection; and to provide general input for the management of information security.

3 What techniques have been used?

According to the 2005 CSI/FBI Computer Crime and Security Survey, much of the industry has begun to embrace the economic metrics to validate the security department expenditures by expressing them in terms of ROI, NPV and IRR [24]. We will describe them in turn.

3.1 ROSI

Return on security investment states the non-financial and financial benefits of information security or an information security initiative compared to its costs.

Producing the result in financial terms indicates whether the quantifiable benefits offered or delivered outweigh the costs. The main drivers for using ROSI are: to justify the budget set for security projects; to assist in project appraisal and selection; and to provide general input for the management of information security. There are two groups of people driving the use of ROSI. One group, driving use from the top down, includes senior management, academics and finance professionals; the other group, driving use from the bottom up, are security professionals. Both groups wish to have a clear view of the value and benefits of any security investment.

ROSI refers to the calculation of the financial return from an investment in security, such as an initiative or project, based on the financial benefits and costs of that investment. ROSI is expressed as the net gain divided by the investment. In the simplest of terms:

$$(what-I-gained-totally)-(what-I-invested)/(what-I-invested) \quad (1)$$

What a company invest is considered tangible or hard assets. A valid number can be generated relatively easily. The problem lies in determining a number for what is gained. Firewalls simply do not generate revenue, IDS do not generate revenue. The difficulty heres lies in the fact that security is a negative goal. As illustrated by a security office; *"What do you provide to your executives. It is tough to show the value of what you do when that value consists of potentially making something not happen (security incident)."* So how do we decide gain to the avoidance of security incident or controlling the impact of a security incident? Early attempts to measure security risk led to the annual loss expectancy (ALE) model, developed in the late 1970s at the National Institute for Standards and Technology (NIST) [37]. ALE is a dollar figure, produced by multiplying the impact of an incident (in dollars) by the frequency (or probability) of the accident. In other words, ALE considers security breaches from two perspectives: how much damage would such a breach incur, and how likely is it to occur? ALE combines probability and severity of attacks into a single number, which represents the amount a firm actually expect to lose in a given year.

$$ALE = \sum_{i=1}^{n} I(O_i)F_i \quad (2)$$

where:
$\{O_1, \ldots, O_n\}$= Set of harmful outcomes
$I(O_i)$= Impact of outcome in dollars
F_i= Frequency of outcome i

Using ALE, the calculation of risk reduction related to a particular security control, boils down to the calculation of differences of ALE before and after implementing the security control. That difference can be seen as the benefit of implementing the security control in question.

$$what{-}i{-}gained = benefit = \Delta ALE = ALE_{without\_sec\_control} - ALE_{with\_sec\_control} \quad (3)$$

Still the estimation of risk mitigation can be subjective. E.g. how to estimate a security breachs collateral damage, including litigation fees,fines for information disclosure, and harm to the companys overall image and brand [32]. Some in the information community consider this as a problem in examining soft and hard dollars. The soft dollars being the assignment of gain to the above mentioned attributes of risk mitigation, reputation and so forth. "This issue of soft versus hard benefits does not invalidate the security business case, but it does make it unique. While almost all business cases include both hard and soft benefits, most of the important benefits with security business cases are soft."[32].

3.2 NPV

In addition to the subjective downside of ROSI, the time attribute presents a problem and leads managers to use Net Present Value (NPV) along with ROI to justify security expenditures. NPV is very useful in evaluating between alternatives. The methodology behind NPV is to find the cash flows generated by a particular solution and find what those cash flows are worth in todays dollars.

Present Value (NPV) is the most widely accepted criterion for project evaluation in corporate finance [7]. A project with a positive NPV increases the wealth of the firm, that is, the total value generated through the project's lifetime is superior to the cost of financing it. NPV is measured in today's dollars. Its computation is based on the principle of discounting: all projected future cash flows of the project are discounted back to the present time under the assumption that one dollar today is worth $(1+d)^T$ dollars at time T in the future. The cash flows represent the estimated costs, cost savings, and revenues at various points during the useful lifetime of the project. A higher NPV is always preferable to a lower NPV, and a negative NPV represents an unacceptable investment.

3.3 IRR

Internal Rate of Return (IRR) is the final economic metric discussed that a security manager might use to evaluate a project expenditure. The IRR is calculated by using a cash flow like NPV. Unlike the NPV calculation IRR will show a security manager at what rate will we break even.

4 What topics have been addressed?

The largest body of research related to preventing breaches is technical, focusing on such concerns as encryption and access controls. In contrast, the research related to the economic aspects of information security is small but rapidly growing [1, 4, 21, 23, 11, 25, 29, 31, 8]. Researchers have addressed various security issues from an economics perspective, ranging from studies measuring the

cost of security breaches and the benefit of security controls to studies aiming at determining how much to invest in security and how to design an effective security architecture. We will group them in topics and address each group in turn.

4.1 Measuring the cost of security breaches (business impact analysis)

The true cost of a security breach is multi-faceted and difficult to quantify. The loss can be direct or indirect. The business impact of a security breach can be classified into the following categories [27]:

- financial impact
  - a) loss of sales, orders or contracts
  - b) loss of tangible assets
  - c) penalties/legal liabilities
  - d) unforeseen costs
  - e) depressed share price
- Operational impact
  - a) loss of management control
  - b) loss of competitiveness
  - c) new ventures held up
  - d) breach of operating standards
- Customer-related impact
  - a) delayed deliveries to customers or clients
  - b) loss of customers or clients
  - c) loss of confidence by key institutions
  - d) damage to reputation
- Employee-related impact
  - a) reduction in staff morale/productivity
  - b) injury or death

The above impacts can be tangible and intangible. It is possible to estimate some of the above costs such as lost of sales, material and labor costs, and loss of productivity. Other costs such as those related to damage to reputation and loss of confidence are difficult to calculate. Nonetheless these costs are extremely important in measuring the true cost of security for business.

Valuing information assets for security risk management. Firms can't fully quantify the loss if they have not valued the resource. As pointed out by Crume [16] "The first rule of IT security is that you should never spend more to protect something than that thing is actually worth." Consequently, the money you spend on a security control should not exceed the value of the information assets the security control protects. Valuing information for this purpose differs significantly from valuing information for accounting purposes. In most cases,

the organization is not trying to sell its data to others and has not established a marketplace in which the data's value could be tested.

Poore reported that one or more of the following conditions generally forms the basis for valuing information for risk management purposes [33]:

- Exclusive possession. The degree to which information is exclusively possessed directly relates to the value the information has to the organization that possesses it. For example, a trade secret that ceases to be a secret loses value.
- Utility. Information that is useful is at least as valuable as the use to which it can be put. Destruction of information or denial of access to information that results in an enterprise becoming disabled demonstrates the utility of the information b proving that it is essential to the operation of the enterprise.
- Cost of creation or re-creation. One of the easiest and most conservative methods of capturing a value for an entity is to determine how much it cost the enterprise to create or to acquire the information in the first place.
- Liability. When information represents a relationship of trust (e.g. because of its personal or private nature, trade secrecy, or national security implications), then the possessor of the information may assume liability for its protection[2].
- Convertibility. When information represents value intrinsically, (e.g. an electronic funds transfer or an inventory count), or when information has intrinsic value, (e.g., intellectual property, music) potentially convertible to other assets, the information valuation would be at least equal to the conversion value.
- Operational impact. An organization can often assign value on the basis of the impact the absence of the data would have on the organization or the impact that incorrect or untimely date have on the organization. For example, an invalid inventory could cause over or under ordering of materials.

Different valuation methods Different valuation methods have been developed in recent years [31, 34, 9, 25, 19, 12]. These methods produce dissimilar values for the same assets. Some approach look at the costs of creating/re-creating the compromised assets, others examine costs incurred as a result of the security breach, while still others try to capture all effects on both revenues and costs. Further Hoo argues that to value the consequences of security breaches, a comparison could be done between two possible scenarios: one in which a security

[2] Liability is additionally complicated as an element of information valuation because of it is extremely probabilistic in nature. That is, the breach of trust or other actionable tort must occur, a third party must be harmed, and steps must be taken by the third party to extract compensation from the enterprise. Until this process has actually resulted in expenses to the enterprise, the existence of a theoretical liability does not admit to practical quantification. Nonetheless reasonable valuations based on case histories in which data of similar nature resulted in harm and in the award of damage may prove useful in supporting information security risk management decisions.

incident occurs and one in which it does not occur [25]. The differences between the two scenarios would form a basis for valuing the consequences. For example, if a manufacturer's order-taking system suffered a one-week outage, the value lost should not be an entire week's revenues just because the system was unable to take orders. Orders will likely still be taken and processed by some alternative, albeit probably less efficient, method. The cost of the consequences is, therefor, more appropriately computed by comparing the revenues that would have resulted if the system had been operational against the revenues actually realized.

Some organizations have relied on the cost estimates from the CSI/FBI Survey. According to the CSI/FBI Survey 2005, which polled 699 respondents from organizations throughout the United Stated, 639 were able and willing to quantify the losses. Respondents estimates of the losses caused by type of computer security incident are shown in figure 1. The total reported loss was over 130M dollars and the average estimated loss was over 230K dollars per organization across all types of breaches. Figure 1 shows that the top three categories of lossesi.e., from viruses, unauthorized access and theft of proprietary informationswamped the losses from all other categories. The denial of service category is a distant fourth. According to the authors, the reported losses include largely only the direct and tangible costs associated with security breaches. The authors suspect that respondents are more accurate than ever in accounting for their explicit costs (such as the cost of reinstalling software and reconfiguring computer systems). But theyre equally suspicious that implicit losses (such as the lost future sales due to negative media coverage following a breach) are largely not represented in the loss numbers reported here [24].

These implicit costs are difficult to measure, although some researcher propose to capture the implicit costs through the loss of market capitalization a publicly traded company may experience. Cavusoglu proposes a market valuation-based approach to estimate the true cost of security breaches [12]. There approach is based on efficient market hypothesis. In efficient markets, investors are believed to revise their expectations based on new information in announcements. Investors' expectations are reflected in the value of the firm. Security problems may signal to the market a lack of concern for customer privacy or poor security practices within the firm. These signals in turn may lead investors to question the long-term performance of the firm. In investors view a security breach negatively, believing that the transitory and long-term costs resulting from the breach will substantially reduce expected future cash flows, then using the change in market value of the breached firms around security breach announcement days can be a proxy to estimate the rue cost of security breaches. Studies in the same line of research include works from [9].

Difficulty in the valuation of security damage Placing a value on the damage caused by a breach of information security is a highly speculative activity. Some of the costs associated with information assets are readily assessable, such as resources devoted to information recovery, others are not so easily quanti-

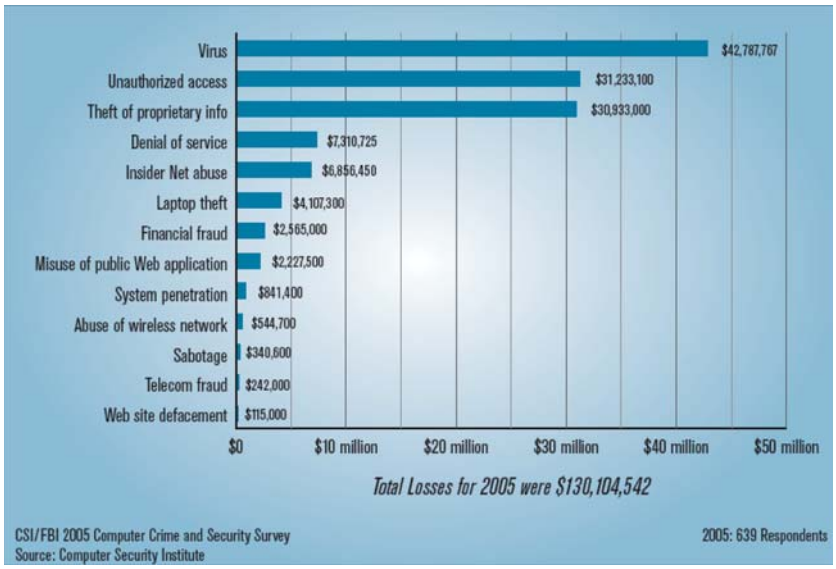

Fig. 1. Financial Losses according to the CSI/FBI Survey.

fied. For example, the value of an information asset is highly dependent on who possesses the information. Time sensitivity can also complicate the valuation problem. For example, a password that expires after ten seconds is worthless after it has expired. Add to the difficulties is the challenge posed by intangible values, such as reputation, trust, embarrassment, etc. and the task of valuation quickly becomes a highly uncertain activity.

4.2 Measuring the value of security controls/safeguards

Ideally, safeguard selection would be based on a balancing of cost and effectiveness. The specific capital, installation, and maintenance costs of safeguards can be readily estimated from a host of vendors. These vendors offer a full range of security services from basic security technology to implementation of security solutions to the complete management of information security [3].

[3] Quantification of the full impact that security controls may have on an organization, especially measures that require changes in worker behavior and in their access to information, is not as easily calculable. Further, security almost always comes at the cost of convenience, hence hampering productivity. The cost of a safeguard

In contrast, the measurement of safeguard efficacy remains primitive in a very few cases and elusive in the rest. Rating processes do exist for some specific technologies, such as firewall, anti-virus software, and intrusion detection systems. However, these ratings are neither comparable across technologies nor applicable in an information security risk assessment context. At present, no formal methodology exists for rating the security of one computer against the security of another. The difficulty of the measurement problem derives from two inherently uncertain quantities: prediction of the attack profile and estimation of security policy compliance. Both factors depend upon humans who have a diverse range of incentives and upon technology that is constantly changing.

The effectiveness of a safeguard is an assessment of how well the safeguard mitigates a risk. A safeguard can mitigate risk in two ways: prevent an attack from occurring or reduce the consequence of a successful attack. Safeguards reduce the consequence of an attack because security managers detect an attack, which gives them an opportunity to either stop an ongoing attack or identify the damage. Security technologies fail for a variety of reasons so security experts recommend using more than one safeguards against expected threats. This security engineering principle is known as *defense-in-depth* [2]. Using the defense-in-depth model, security control can be classified as *protection, detection,* or *recovery* mechanisms. Since prevention mechanisms stop a threat from succeeding, they reduce threat frequencies. Detection and recovery mechanisms reduce the attack outcomes from a compromised system. To assess the effectiveness of safeguards can be difficult and controversial. If available, past incident data should be analyzed to derive the reduction factors. Otherwise, expert judgments would be used to estimate the efficacy rate. In [8], the author uses security manager's subjective judgment to quantify the effectiveness and argues that although security managers recognize that precise effectiveness metrics are unobtainable, they are able to provide rough estimates. Furthermore, the authors reasons that when better estimation are not available, a rational approach is to conduct sensitivity analysis to understand how sensitive the decisions are to the security manager's assumptions and estimates.

Given the fact that a defense-in-depth security architecture is a necessity for a secure environment, the crucial question to answer is how security controls interact with each other. Do they complement each other, for example, is the effectiveness of a security architecture with both a firewall and an IDS greater than the sum of the effectiveness when each controls is applied individually? The point is that firms should carefully evaluate the value of a security mechanism considering already existing controls before concluding on its return instead of isolation from existing controls.

---

should also include the impact of the safeguard on productivity, since this number is sometimes significant enough to make or break the viability of a given solution.

4.3 Determine the optimal level of security investment (the decision framework)

The task of determining the optimal level of security investment utilizes results in the previous two sections. We identify a number of approaches and group them in three groups.

Decision analysis framework This line of work uses the traditional risk or decision analysis framework. The idea is to identify the potential risk of security breaches in terms of their damages and likelihood. Gordon and Loeb provide an economic modeling framework for assessing the optimal amount to invest in information security based on the principle of equating the marginal financial benefits of information security to the marginal financial costs of such security [21]. Hoo provides a decision analytical framework to evaluate different policies for IT security [25]. He develops a risk modeling framework for selection of safeguards which utilizes influence diagrams as a common graphical language that maps relationships between key variables. In stead of comparing security controls on an individual basis, his model groups controls into baskets of safeguards, or policies[4]. Then he makes the cost benefit trade off analysis for each policy. Longstaff et al. proposes Hierarchical Holographic Model (HHM) to assess security risks and provide a model for assessing the efficacy of risk management [30]. Bodin et al. propose to use Analytic Hierarchy Process (AHP) for assisting an organization in making information security investment decisions [4].Their approach offer the advantage of analyzing multi-criteria decision scenarios, where financial and non financial, quantitative and qualitative criteria are compared. Butler proposes a cost benefit analysis method called SAEM to compare alternative security designs [8]. The case study presented in this paper starts with a multi-attribute risk assessment that results in a prioritized list of risks. Security specialists estimate safeguards benefits and how the organizations' risks are reduced. Using SAEM, security design alternatives are compared with organization's current selection of security technologies to see if a more cost-efficient solution is possible. Xie and Mead describe a general framework for hierarchical cost/benefit analysis aimed at providing acceptable estimations for small companies in their information security improvement projects [38]. The framework classifies misuse cases into categories of threats for which nationally surveyed risks and financial data are publicly available. For each category of threats, costs, benefits, baseline risks, and residual risks are estimated. The framework then generates all permutations of possible solutions and analyzes the most optimal approach to maximize the value of security improvement projects.

Game theory Cavusoglu et al. argue that the traditional decision analysis approach for evaluation IT security investment, though intuitive, treats security

[4] He does not consider the interactions between safeguards when grouping them together

technology as a black box and do not take into account that the context of IT security is different from other general IT investment context [11]. They argue that in security, organizations are dealing with strategic adversaries who are looking for opportunities to exploit vulnerabilities in systems. Therefore, IT security can be treated as a kind of game between organizations and attackers. Game theory [35] is used to analyze problems in which the payoffs to players depend on the interaction between players' strategies. In the security investment problem, the firm's payoff from security investment depends on the extent of hacking it is subjected to. The hacker's payoff from hiking depends on the likelihood of being caught. Security investment not only prevent security breaches by reducing the vulnerabilities that attackers can exploit but also act as a deterrent for attackers by making attacks less attractive. Knowing that their attack will not be enough to bypass preventive security mechanisms or will be detected by detective control mechanisms can change the behavior of attachers. Based on the above idea, Cavusoglu et al. use a game theory based approach for determining the optimal IT security investment level. In the same line is the work of Cremonini and Martini. They propose an approach to improve ROI-based evaluation by integrating them with a new index, called Return-On-Attacks (ROA), aimed at measuring the convenience of attacks [15].

Real options theory Real Options Analysis was first developed as a decision support technique in the area of capital investment [13].The concept of real means adapting mathematical models used to evaluate financial options to more tangible investments. This approach reconciles financial and strategic viewpoints to support decision making in the face of uncertainty - in particular, for valuing flexibility. The core of real options analysis for IT assets consists of: i) the identification and the assessment option components in a project and ii)the selection and the application of a mathematical model for valuing financial options that serves to quantify the current value of choosing these components for inclusion at a later time. Real options theory has been applied in several area in information systems and software engineering research, e.g. software reuse [18] and stability of software architecture [3]. In information security, attempts have been made to use real options to explain or guide security investment decisions. Gordon et al. explain why a large portion of security expenditures seem to be made on a wait-and-see basis even though expenditures to prevent information security breaches have been growing rapidly in recent year [23]. They argue that one key driver of actual expenditures on information security activities is the occurrence of actual security breaches. They further explain that this reactive, as opposed to proactive, approach toward a significant portion of information security expenditures is consistent with the real options view of capital investments. Daneva proposes a real options-based decision framework for information security [17]. She identifies a number of options and argues that these options embed flexibility in the decision making process.

4.4 Relevant studies in a broader scope

It is worthwhile to note that even security technology developers have started to incorporate cost and benefit factors in algorithms used by the technology. For example, Lee et al. study the problem of building cost sensitive intrusion detection systems (IDS) [28]. They use the cost model and technical effectiveness of the IDS to determine whether it is worthwhile to employ countermeasures to stop an intrusion. Conrad used Monte-Carlo simulation to capture uncertainty in security modeling parameters (vulnerabilities, frequency of intrusion, damage estimates, etc) and expresses its impact on the model's forcast (e.g. projected benefit) [14]. A Monte-Carlo simulation enables an analyst to quantify the uncertainty in an expert's estimate by defining it as a probability distribution rather than just a single expected value. A highly related topic is software economics, or value-based software engineering . An increasing number of research has been directed to software economics, the study of economic aspects of software. Barry Boehm wrote a comprehensive reference on software engineering economics [6] which, along with the book on cost estimation [5], provides a solid foundation for understanding ROI in the software context.

5 Conclusions and future work

Bruce Schneier, in his book - Beyond Fear: Think Sensibly about Security in an Uncertain World - explains how security really works, *'The key is to think of security not in absolutes, but in terms of sensible trade-offs, whether on a personal or global scale.'* He also adds, *'Economics - not technology - determines what security technologies get used.'* [36]. The overview of literature in this paper echoes his remarks.

In this paper, we gave an overview of the literature on economic approaches to information security management. We discussed a number of issues: i)the need to justify security expenditures, ii)what techniques have been used, and iii) what topics have been addressed in literature. There are several directions for future research on economic aspects of information security management. One prominent line of research is to extend and adapt the current practice into cross-organizational security processes and services, where each unit are profit-loss responsible for itself. It poses challenges both at technical level and organizational level. To make informed decisions on security budgets and resource allocation, at network business level, the partners have to define what shared information responsibilities partners have to each other. They have to determine who pays for security, who suffers in case of failure, who is liable should security be comprised [1]. When multiple organizations or individuals collaborate, they may share risks and revenues, leading to a need for common business cases and an equitable distribution of costs. Networked business will be difficult to function if the organizations involved cannot agree: why security is necessary; the scope it should cover and what each organization expects it to achieve. It will be difficult to manage if failures to achieve agreed security levels are difficult to detect and enforce.

Estimating costs and benefits of security solutions involves a high degree of uncertainty. How to incorporate uncertainty in the decision framework requires further research. Prominent line of work including using Bayesian belief networks (BBN) for cost-benefit trade-off analysis of security treatment strategies [26] and applying Real Options thinking to information security [17].

References

1. R. Anderson. Why information security is hard-an economic perspective. In *ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference*, page 358, Washington, DC, USA, 2001. IEEE Computer Society.
2. R. J. Anderson. *Security Engineering: a Guide to Building Dependable Distributed Systems*. John Wiley and Sons, 2001.
3. R. Bahsoon and W. Emmerich. Evaluating architectural stability with real options theory. In *ICSM '04: Proceedings of the 20th IEEE International Conference on Software Maintenance*, pages 443–447, Washington, DC, USA, 2004. IEEE Computer Society.
4. L. D. Bodin, L. A. Gordon, and M. P. Loeb. Evaluating information security investments using the analytic hierarchy process. *Commun. ACM*, 48(2):78–83, 2005.
5. B. Boehm. *Software Cost Estimation with Cocomo II*. Prentice Hall, 2000.
6. B. W. Boehm and K. J. Sullivan. Software economics: a roadmap. In *ICSE - Future of SE Track*, pages 319–343, 2000.
7. R. A. Brealey, S. C. Myers, and A. J. Marcus. *Fundamentals of Corporate Finance*. ISBN-0-07-255752-4. McGraw-Hill/ Irwin, 2004.
8. S. A. Butler. Security attribute evaluation method: a cost-benefit approach. In *ICSE '02: Proceedings of the 24th International Conference on Software Engineering*, pages 232–240, New York, NY, USA, 2002. ACM Press.
9. K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *J. Comput. Secur.*, 11(3):431–448, 2003.
10. H. Cavusoglu, B. Mishra, and S. Raghunathan. A model for evaluating it security investments. *Commun. ACM*, 47(7):87–92, 2004.
11. H. Cavusoglu, B. Mishra, and S. Raghunathan. A model for evaluating it security investments. *Commun. ACM*, 47(7):87–92, 2004.
12. H. Cavusoglu, B. K. Mishra, and S. Raghunathan. The effect of internet security breach ammouncements on market value of breached firms and internet security developers. *Internal Journal of E-Commerce*, 2004.
13. P. D. Childs, S. H. Ott, and A. J. Triantis. Capital budgeting for interrelated projects: A real options approach. *Journal of Fiancial and Quantitative Analysis*, 33(3):305–335, 1998.
14. J. R. Conrad. Analyzing the risks of information security investmens iwth monte-carlo simulations. In *Proceedings of the Fourth Workshop on the Economics of Information Security (WEIS05)*, June 2005.
15. M. Cremonini and P. Martini. Evaluating information security investments from attackers perspective: the return-on-attack (roa). In *Proceedings of the Fourth Workshop on the Economics of Information Security (WEIS05)*, June 2005.
16. J. Crume. *Inside Internet Security*. Addison Wesley, 2001.

17. M. Daneva. Applying real options thinking to information security. Technical report, CTIT Technical Report TR-CTIT-06-11, Centre for Telematics and Information Technology, University of Twente, Enschede, The Netherlands, 2006.
18. J. M. Favaro, K. R. Favaro, and P. F. Favaro. Value based software reuse investment. *Ann. Softw. Eng.*, 5:5–52, 1998.
19. A. Garg, J. Curtis, and H. Halper. Quantifying the financial impact of it security breaches. *Inf. Manag. Comput. Security*, 11(2):74–83, 2003.
20. L. A. Gordon and M. Loeb. Return on information security investments: Mythis vs. realities. *Journal of Strategic Finance*, 84:26–32, 2002.
21. L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, 5(4):438–457, 2002.
22. L. A. Gordon and M. P. Loeb. Budgeting process for information security expenditures. *Communications of the ACM*, 49(1):121–125, 2006.
23. L. A. Gordon, M. P. Loeb, and W. Lucyshyn. Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal*, 19(2), 2003.
24. L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Rochardson. 2005 CSI/FBI computer crime and security survey. Technical report, Computer Security Institute, 2005.
25. K. J. S. Hoo. *How much is enough? A risk management approach to computer security.* PhD thesis, Stanford University, 2000.
26. S. H. Houmb, G. Georg, R. B. France, J. M. Bieman, and J. Jurjens. Cost-benefit trade-off analysis using BBN for aspect-oriented risk-driven development. In *Proceedings of the 10th International Conference on Engineering of Complex Computer Systems (ICECCS 2005)*, 2005.
27. ISF. The standard of good practice for information security. Technical report, Information Security Forum, 2005.
28. W. Lee, W. Fan, M. Miller, S. J. Stolfo, and E. Zadok. Toward cost-sensitive modeling for intrusion detection and response. *J. Comput. Secur.*, 10(1-2):5–22, 2002.
29. K. D. Loch, H. H. Carr, and M. E. Warkentin. Threats to information systems: Today's reality, yesterday's understanding. *MIS Quart*, 17(2):173–186, 1992.
30. T. A. Longstaff, C. Chittister, R. Pethia, and Y. Y. Haimes. Are we forgetting the risks of information technology? *IEEE Computer*, 33(12):43–51, 2000.
31. R. T. Mercuri. Analyzing security costs. *Commun. ACM*, 46(6):15–18, 2003.
32. T. Pisello. Is there a business case for IT security? *Security Management*, 38(10):140–142, 2004.
33. R. S. Poore. Valuing information assets for security risk management. *Information Systems Security*, pages 13–23, September/October 2000.
34. R. Power. CSI special report: How to quantigy financial losses from inforsec breaches. *Computer Security Alert*, October 1999.
35. E. Rasmusen. *Games and Information.* Blackwell Publishers, 1998.
36. B. Schneier. *Beyond Fear: Think Sensibly about Security in an Uncertain World.* Copernicus Books, September 2003.
37. G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. Technical report, National Institute of Standards and Technology, 2002.
38. N. Xie and N. R. Mead. SQUARE project: Cost/benefit analysis framework for information security improvement projects in small companies. Technical report, CMU/SEI-2004-TN-045, 2004.